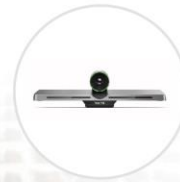


Yealink



Full HD Video Conferencing System Administrator Guide

Version V32.3
May.2018

Copyright

Copyright © 2018 YEALINK(XIAMEN) NETWORK TECHNOLOGY

Copyright © 2018 Yealink (Xiamen) 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 (Xiamen) Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

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

Trademarks

Yealink®, the logo and the name and marks is trademark of Yealink (Xiamen) Network Technology CO., LTD, which are registered legally in China, the United States, EU (European Union) and other countries.

All other trademarks belong to their respective owners. Without Yealink's express written permission, recipient shall not reproduce or transmit any portion hereof in any form or by any means, with any purpose other than personal use.

Warranty

(1) Warranty

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

(2) Disclaimer

YEALINK (XIAMEN) 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 (Xiamen) 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.

(3) Limitation of Liability

Yealink and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Yealink does not provide any

warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Yealink has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

This End User License Agreement ("EULA") is a legal agreement between you and Yealink. By installing, copying or otherwise using the Products, you: (1) agree to be bounded by the terms of this EULA, (2) you are the owner or an authorized user of the device, and (3) you represent and warrant that you have the right, authority and capacity to enter into this agreement and to abide by all its terms and conditions, just as if you had signed it. The EULA for this product is available on the Yealink Support page for the product.

Patent Information

China, the United States, EU (European Union) and other countries are protecting one or more patents of accompanying products and/or patents being applied by Yealink.

Customer Feedback

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

Technical Support

Visit Yealink WIKI (<http://support.yealink.com/>) for the latest firmware, guides, FAQ, Product documents, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (<https://ticket.yealink.com>) to submit all your technical issues.

GNU GPL INFORMATION

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

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

<http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCateId=293&NewsCateId=293&CateId=293>.

Introduction

Yealink administrator guide provides general guidance on configuring, customizing, managing, and troubleshooting video conferencing systems.

This guide is not intended for end users. It is for an administrator who is experienced in system administration.

This guide is applicable to the following Yealink device running firmware version 32 or higher:

- VC880 video conferencing system
- VC800 video conferencing system
- VC500 video conferencing endpoint
- VC500 Pro video conferencing endpoint
- VC200 video conferencing endpoint

The differences between VC500 and VC500 Pro models are as follow:

Features	VC500	VC500 Pro
Work with CP960 conference phone	×	√
H.265 video codec	×	√
60 frame rate	×	√

Tip

If you purchase VC500 model, but you want to use the features supported by VC500 Pro model, you can contact Yealink FAE for help.

Related Documentations

The following related documents are available:

- Video conferencing System Quick Start Guide, which describes how to assemble the system and configure conference room and network.
- Video conferencing System User Guide, which describes how to configure and use basic features available on the systems.
- Video conferencing System Network Deployment Solution, which describes how to deploy network for your systems.
- Yealink VCR11 Remote Control Quick Reference Guide, which describes how to use the VCR11 Remote Control.
- Yealink CPW90 Quick Start Guide, which describes how to connect CPW90 wireless expansion microphones to CP960 conference phone.
- Yealink CPW90 Wireless Microphones Quick Start Guide, which describes how to connect CPW90

wireless microphones to video conference system.

- Yealink CPW90-BT Bluetooth Wireless Microphones Quick Start Guide, which describes how to connect CPW90-BT Bluetooth wireless microphones to video conference system.
- Yealink CP960 HD IP Conference Phone Quick Reference Guide, which describes how to use CP960 conference phone.
- Yealink Wi-Fi USB Dongle WF50 User Guide, which describes how to connect video conference system to Wi-Fi, or how to provide wireless AP.
- Yealink WPP20 Wireless Presentation Pod Quick Start Guide, which describes how to connect WPP20 wireless presentation pod.
- Yealink WPP20 Wireless Presentation Pod User Guide, which describes how to use WPP20 wireless presentation pod.
- Yealink PSTN Box CPN10 Quick Start Guide, which describes how to connect video conference system to PSTN.
- Yealink VCC22 Video Conferencing Camera Quick Start Guide, which describes how to connect the VCC22 video conferencing cameras to the VC800/VC880 video conferencing system.
- Yealink Products Regulatory Notices guide, which describes all regulatory and safety guidance.

You can download these documentations online:

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

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online:

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

Conventions

This topic describes the conventions in the document.

General Conventions

Convention	Description
Bold	Highlights the user interface items such as menus or menu selections when they are involved in a procedure or user action (for example, click Home). Also used to emphasize text.
Blue Text	Used for cross references to other sections within this documentation (for example, refer to Trouble Shooting).
<i>Blue Text in Italics</i>	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (for example, for more information, refer to Yealink Meeting Server User Guide).

GUI Conventions

Convention	Description
->	Indicates the menu path. For example, Network->LAN Configuration indicates the path of entering LAN Configuration page.

What's New in This Guide

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

Changes for Release 32, Guide Version 32.1

This edition adds VC880/VC200 video conferencing system.

The following section is new for this version:

- [Hardware of VC880 Codec](#) on page 15
- [Hardware of VC200 Codec](#) on page 21
- [Hardware of CPW90-BT Bluetooth Wireless Microphone](#) on page 28
- [Hardware of WPP20 Wireless Presentation Pod](#) on page 30
- [LED Instructions of CPW90-BT Bluetooth Wireless Microphones](#) on page 34
- [Wi-Fi](#) on page 63
- [Wireless Access Point](#) on page 65
- [Configuring PSTN](#) on page 80
- [Configuring Local Storage](#) on page 106
- [Configuring Microphone Mute Mode](#) on page 121
- [Accessories with Your System](#) on page 181
- [Resetting the SD Card](#) on page 190

Major updates have occurred to the following sections:

- [Available Audio Output](#) on page 109
- [Available Audio Input](#) on page 111
- [Cloud Directory](#) on page 167

Table of Contents

Introduction..... v

Related Documentations	v
Conventions.....	vi
General Conventions	vi
GUI Conventions	vii
What's New in This Guide	vii
Changes for Release 32, Guide Version 32.1	vii

Table of Contents..... ix

Getting Started..... 15

Hardware Overview	15
Hardware of VC880 Codec	15
Hardware of VC800 Codec	16
Hardware of VC500 Codec	18
Hardware of VC200 Codec	21
Hardware of VCC22 Video Conferencing Camera	23
Hardware of VCH50 Video Conferencing Hub.....	24
Hardware of CP960 Conference Phone.....	26
Hardware of CPE90 Wired Expansion Microphones.....	27
Hardware of CPW90-BT Bluetooth Wireless Microphone.....	28
Hardware of CPW90 Wireless Microphone	29
Hardware of WPP20 Wireless Presentation Pod	30
Hardware of VCR11 Remote Control	30
LED Instructions	32
LED Instructions of VC880/VC800/VC500/VC200.....	33
LED Instructions of VCC22 Video Conferencing Camera.....	33
LED Instructions of CP960 Conference Phone.....	33
LED Instructions of CPE90 Wired Expansion Microphones.....	34
LED Instructions of CPW90-BT Bluetooth Wireless Microphones.....	34
LED Instructions of CPW90 Wireless Microphones	35
LED Instructions of WPP20 Wireless Presentation Pod	36
Powering On and Off.....	37
Powering On the System.....	37
Powering Off the System.....	37
Initialization Process Overview	37
Loading the ROM File	37

Configuring the VLAN	37
Querying the DHCP (Dynamic Host Configuration Protocol) Server	38
Running the Setup Wizard	38
Configuration Methods	39
Using Web User Interface	39
Using Remote Control	40
Using CP960 Conference Phone	41

VCS Deployment Methods 43

Traditional Deployment Methods	43
Public IP Configuration	43
Port Forwarding	43
NAT	44
STUN	47
H.460	49
Intelligent Traversal	49
VPN	51
Cloud Deployment Method	52

Configuring System Settings 55

Configuring Network Settings	55
IPv4 and IPv6 Network Settings	55
DHCP Option	59
VLAN	61
Wi-Fi	63
Wireless Access Point	65
802.1x Authentication	68
Network Speed and Duplex Mode	69
Restricting Reserved Ports	70
Quality of Service (QoS)	71
Adjusting MTU of Data Packets	72
Configuring Account Settings	73
Configuring SIP Settings	74
Configuring H.323 Settings	77
Configuring PSTN	80
Configuring Video Conference Platform	81
Configuring General Settings	93
Setting the Site Name	93
Setting the Language	93
Setting Time and Date	93
Customizing Key Type	100
Allowing Website Snapshot	100
Adjusting Backlight of the CP960 Conference Phone	100

Customizing the Local Interface	101
Configuring Keyboard Input Method.....	105
Configuring USB Storage	106
Configuring Local Storage	106
Screenshot	107
Configuring Video Recording.....	108
Configuring Audio Settings	109
Audio Output Settings.....	109
EQ Self Adaption.....	110
Audio Input Settings	111
Key Tone.....	113
Tones.....	114
Codecs.....	115
DTMF.....	118
Muting Microphone	120
Muting Auto-answered Calls	121
Muting Auto-dialed Calls	122
Configuring Noise Suppression.....	122
Configuring Video Settings.....	123
Changing the Video Input Source	123
Selecting Default Layout for Single Screen.....	123
Selecting Video Frame Rate and Resolution.....	124
Maximizing Monitor Video Display.....	125
Configuring Monitor Resolution	125
Configuring Automatic Sleep Time.....	126
CEC Monitor Controls.....	126
System Integrated with Control Systems	127
Configuring Content Sharing	129
Configuring Dual-Stream Protocol.....	129
Configuring Mix Sending	130
Configuring Shared Content Parameters	131
Configuring Camera Settings.....	131
Adjusting Camera Angle and Focus.....	132
Adjusting Camera Parameters.....	132
Allowing the Far-End System to Control Your Camera	135
Setting Camera Presets.....	137
Configuring Call Settings.....	137
Call Protocol.....	137
Video Call Rate.....	138
Account Polling	138
Search Source List in Dialing.....	139
Call Match	140
Auto Answer	141
Do Not Disturb	142

Configuring Ringback Timeout.....	143
Configuring Auto Refuse Timeout.....	143
SIP IP Call by Proxy.....	143
Configuring Conference Room	144
Conference Type	144
Meeting Password.....	146
Joining the Meeting.....	147
Configuring Voice Activation.....	147
Configuring View Switching.....	148

Securing the System151

User and Administrator	151
Configuring an Administrator Password.....	151
Enabling the User Role	152
Configuring Auto Logout Time	152
Transport Layer Security (TLS)	153
Supported Cipher Suites.....	153
TLS Transport Protocol	154
Managing the Trusted Certificates List.....	154
Managing the Server Certificates.....	157
Secure Real-Time Transport Protocol (SRTP)	158
SRTP Configuration.....	159
H.235	159
H.235 Configuration	160
Defending against Attacks.....	160
Abnormal Call Answering.....	160
Configuring Safe Mode Call	161

Managing the Directory163

Local Directory	163
Adding Local Contacts and Conference Contacts	163
Importing a Local Contact List	165
Exporting Local Contacts List.....	165
Editing Local Contacts	166
Deleting Local Contacts	166
Cloud Directory.....	167
Enterprise Directory	167
Lightweight Directory Access Protocol (LDAP).....	168
LDAP Attributes	168
Configuring LDAP	169
Searching for Contacts.....	171
Placing Calls to Contacts.....	171
Meeting Whitelist.....	171

Configuring Meeting Whitelist.....	172
Deleting Meeting Whitelist.....	172
Meeting Blacklist	172
Adding Meeting Blacklist	172
Deleting Meeting Blacklist	173
Managing the Call Log	175
Saving History Record.....	175
Adding a History Record to Local Directory.....	175
Deleting History Records.....	176
Deleting a History Record.....	176
Deleting Multiple History Records.....	176
Deleting All History Records.....	176
Placing Calls to History Records.....	177
Placing a Call	179
Placing a Call by Entering a Number.....	179
Placing a Call from the Search Result.....	180
Editing Numbers before Calling.....	180
Accessories with Your System.....	181
Using the VCC22 Video Conferencing Cameras.....	181
Controlling VCC22 Camera.....	181
Adjusting Camera Layout.....	181
Using the CPW90 Wireless Microphones with VCS.....	182
Registering CPW90 with VCS.....	182
Deregistering CPW90 from VCS.....	183
Viewing CPW90 Information.....	183
Finding the Registered CPW90.....	183
Using the CPW90 Wireless Microphones with CP960.....	184
Registering CPW90 with the CP960.....	184
Deregistering CPW90 from the CP960 Conference Phone.....	184
Viewing CPW90 Information.....	185
Finding the Registered CPW90.....	185
Using the CPW90-BT Bluetooth Wireless Microphones with VCS.....	185
Registering CPW90-BT with VCS.....	185
Deregistering CPW90-BT from VCS.....	186
Viewing CPW90-BT Information.....	186
Finding the Registered CPW90-BT.....	187
System Maintenance.....	189

Exporting or Importing Configuration Files	189
Exporting BIN Files from the System	189
Importing BIN Files to the System	189
Rebooting the System	190
Resetting the SD Card	190
Resetting the System	190
Resetting the System using Configuration Methods	190
Resetting the System using Reset Button	190
System Log Files	191
Configure System Log Level	191
Local Logging	192
Syslog Logging	193
Packets Capture	193
Capturing the Packets via Web User Interface	193
Capturing the Packets via Remote Control	196
Capturing the Packets via Ethernet Software	197
System Firmware	197
Upgrading Firmware	197
License	198
Importing Device Type License	198
Viewing Device Type	198
Multipoint License	199
Viewing Multipoint License Status	200

Trouble Shooting201

General Issues	201
Call Issues	202
Audio Issues	203
Video Issues	204
Placing a Test Call	206
System Diagnostics	206
Diagnosing the Audio	206
Diagnosing the Camera	206
Diagnosing the Network	206
System Status	207
System Status List	208
Viewing System Status	209
Viewing Call Statistics	210

Getting Started

Topics:

[Hardware Overview](#)

[LED Instructions](#)

[Powering On and Off](#)

[Initialization Process Overview](#)

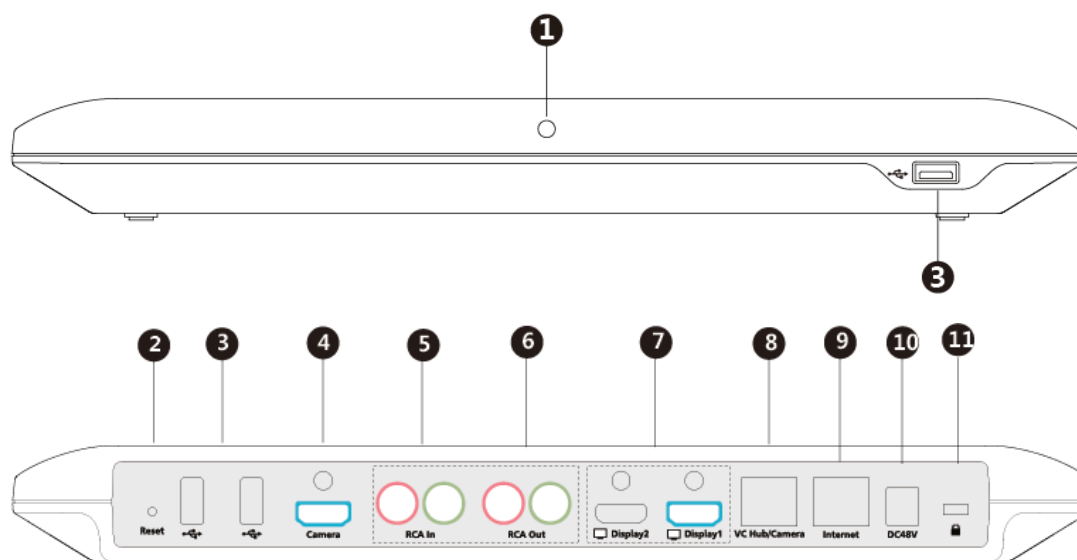
[Configuration Methods](#)

Hardware Overview

This chapter provides hardware overview.

Hardware of VC880 Codec

Owning rich physical interfaces for audio and video connection, VC880 can be connected to the 3rd-party camera or access to the video matrix. In addition, it comes with the professional RCA-in/out interface that integrates the mixer with the gooseneck microphone. Its split-type structure can meet the deploy requirement of the control room which separates from a large conference room.



	Port Name	Description
①	LED Indicator	Indicates different statuses of the system.
②	Reset Key	Resets the system to factory defaults.
③	USB	<ul style="list-style-type: none"> Inserts a USB flash drive to one of the two USB ports for storing

	Port Name	Description
		<p>screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified.</p> <ul style="list-style-type: none"> • Inserts a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. • Inserts a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Inserts a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Inserts a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
④	Camera	Connects to a third-party camera.
⑤	RCA In	Connects to an audio input device using a RCA cable.
⑥	RCA Out	Connects to an audio output device using a RCA cable.
⑦	Display	Connects to a monitor.
⑧	VC Hub/Phone	<ul style="list-style-type: none"> • If you want to use wired sharing, connect this port to the Codec port on the VCH50 video conferencing hub. • Connect this port to the Camera port on the VCC22 video conferencing cameras.
⑨	Security Slot	Allows you to connect a universal security cable to VCC22, so you can lock it down. The camera cannot be removed when locked.
⑩	Internet	Connects to the network device.
⑪	DC48V	Connects to the power source via a power adapter.
⑫	Security Slot	Allows you to connect a universal security cable to VC880 codec, so you can lock it down. The system cannot be removed when locked.

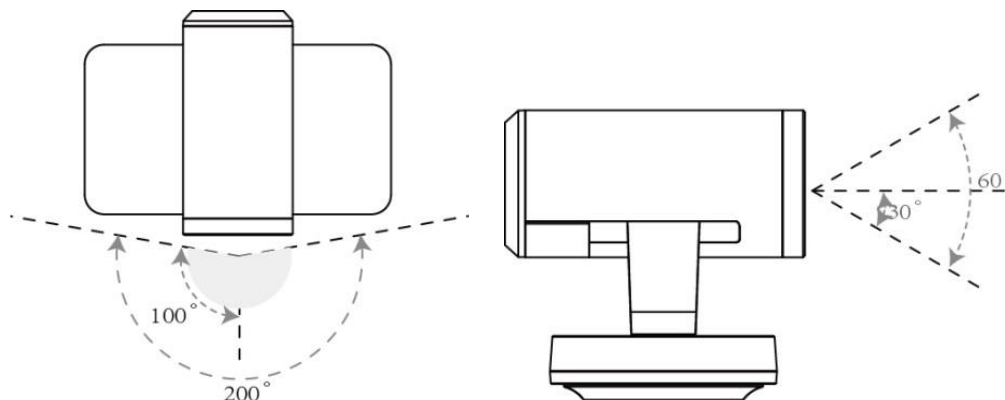
Related Topic:

[LED Instructions of VC880/VC800/VC500/VC200](#)

Hardware of VC800 Codec

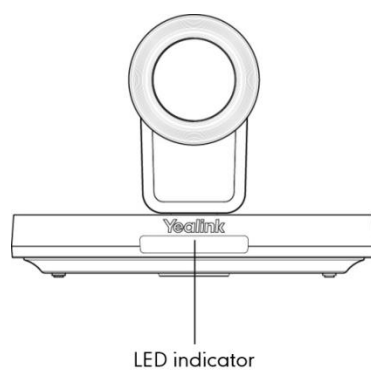
VC800 codec compresses outgoing video and audio data, transmits this information to the far site, and decompresses incoming data.

VC800 supports 16:9 and 4:3 aspect ratios. It can be compatible with different audio devices, and can adapt to the monitors automatically. The VC800 camera can be panned (± 100 degrees range), tilted (± 30 degrees range) and supports 12 x optical zoom, white balance and automatic gain.



Front Panel of VC800 Codec

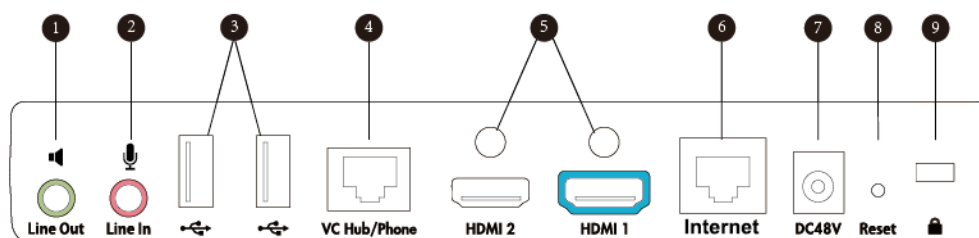
The LED indicator in front of the camera indicates different statuses of the system.



Related Topic:

[LED Instructions of VC880/VC800/VC500/VC200](#)

Rear Panel of VC800 Codec



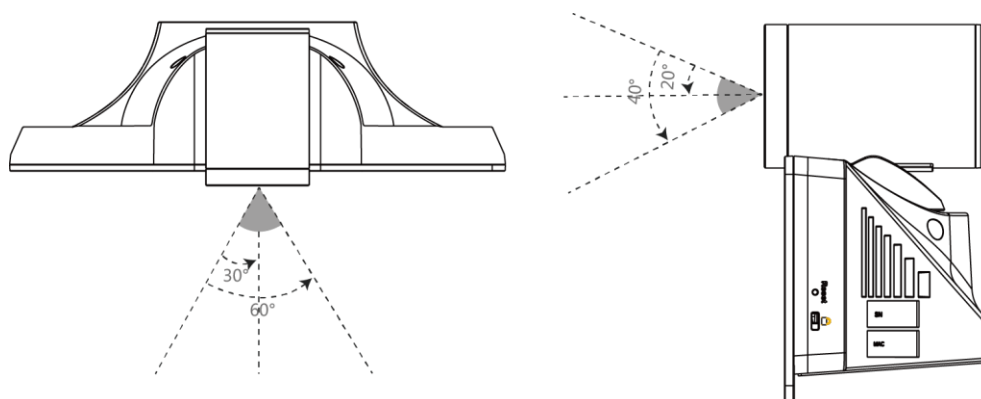
	Port Name	Description
①	Line Out	Connects to an audio output device using an audio cable (3.5mm).

	Port Name	Description
②	Line In	Connects to an audio input device using an audio cable (3.5mm).
③	USB	<ul style="list-style-type: none"> • Inserts a USB flash drive to one of the two USB ports for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. • Inserts a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. • Inserts a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Inserts a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
④	VC Hub/Phone	<ul style="list-style-type: none"> • If you want to share contents, connect this port to the Codec port on the VCH50 video conferencing hub. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone.
⑤	HDMI	Connects to a monitor
⑥	Internet	Connects to the network device.
⑦	DC48V	Connects to the power source via a power adapter.
⑧	Reset Key	Resets the system to factory defaults.
⑨	Security Slot	Allows you to connect a universal security cable to VC800 codec, so you can lock it down. The system cannot be removed when locked.

Hardware of VC500 Codec

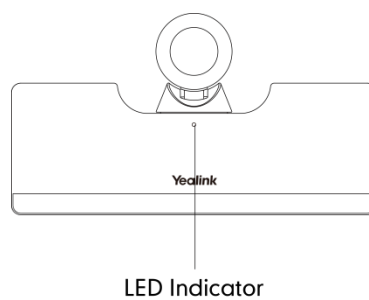
VC500 codec compresses outgoing video and audio data, transmits this information to the far site, and decompresses incoming data.

VC500 supports 16:9 and 4:3 aspect ratios. It can be compatible with different audio devices, and can adapt to the monitors automatically. The VC500 camera can be panned (± 60 degrees range), tilted (± 40 degrees range) and supports 5 x optical zoom, white balance and automatic gain.



Front Panel of VC500 Codec

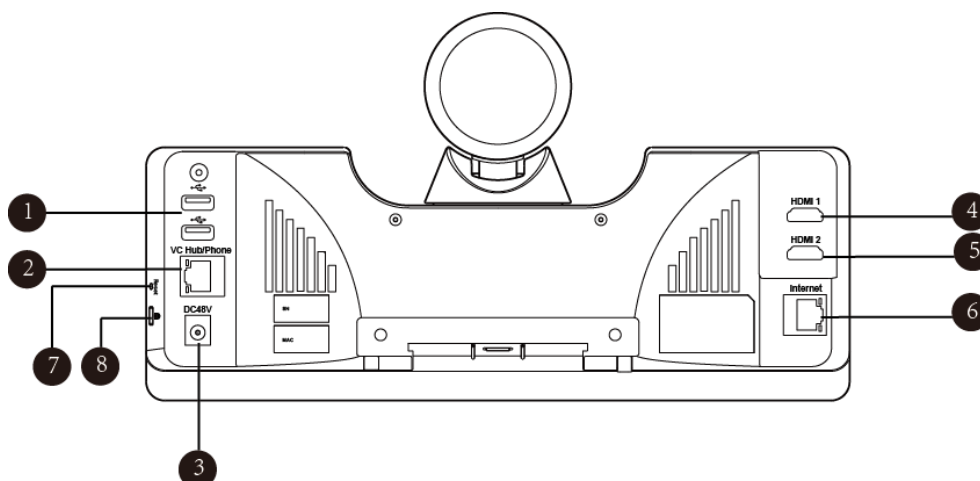
The LED indicator in front of the camera indicates different statuses of the endpoint.



Related Topic:

[LED Instructions of VC880/VC800/VC500/VC200](#)

Rear Panel of VC500 Codec



	Port Name	Description
①	USB	<ul style="list-style-type: none"> Connects to an audio input device using a USB to Line-in adapter. Connects to an audio output device using a USB to Line-out adapter Inserts a DD10 dongle to one of the two USB ports for connecting the CPW90 wireless microphones. Inserts a USB flash drive to one of the two USB ports for storing screenshots, recording videos or capturing packets. Inserts a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. Inserts a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. Inserts a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network). <p>Note:</p> <ul style="list-style-type: none"> The DD10 dongle and USB flash drive can work at the same time. If multiple USB flash drives are connected, only the latter one can be identified.
②	VC Hub/Phone	<ul style="list-style-type: none"> If you want to share contents, connect this port to the Codec port on the VCH50 video conferencing hub. If you need an audio device, connect this port to the Internet port on the CP960 Conference phone.
③	DC48V	Connects to the power source via a power adapter.
④	HDMI 1	Connects to a monitor for displaying video images.

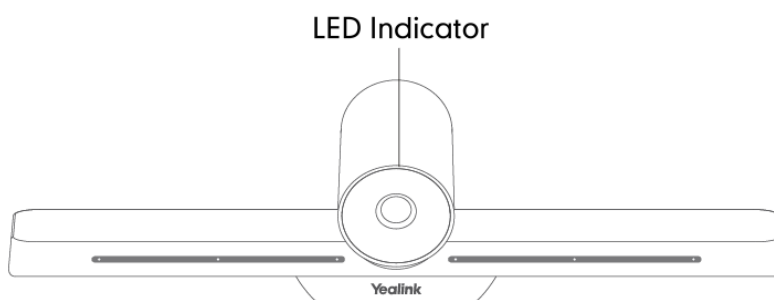
	Port Name	Description
⑤	HDMI 2	Connects to secondary monitor for displaying video images.
⑥	Internet	Connects to the network device.
⑦	Reset Key	Resets the system to factory defaults.
⑧	Security Slot	Allows you to connect a universal security cable to VC800/VC500 codec, so you can lock it down. The system cannot be removed when locked.

Hardware of VC200 Codec

Yealink VC200 is an entry-level smart video conferencing endpoint designed for small and huddle room. Its Ultra HD 4K and 4 x digital zoom camera and 103° super-wide angle lens deliver outstanding video quality and additional boost face-to-face collaboration. With 6 beamforming microphone arrays for direct voice pickup and Yealink Noise Proof Technology, VC200 brings excellent sound in small rooms and ensures that everyone can be heard as well as seen.

Front Panel of VC200 Codec

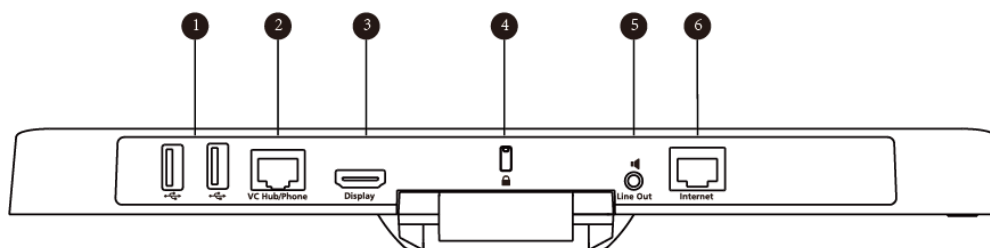
The LED indicator in front of the camera indicates different statuses of the endpoint.



Related Topic:

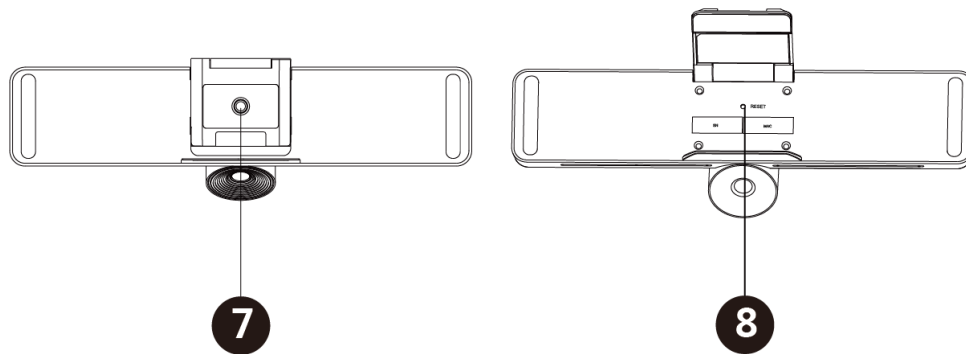
[LED Instructions of VC880/VC800/VC500/VC200](#)

Rear Panel of VC200 Codec



	Port Name	Description
①	USB	<ul style="list-style-type: none"> Inserts a USB flash drive to one of the two USB ports for storing screenshots, recording videos or capturing packets. Inserts a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network). <p>Note: If multiple USB flash drives are connected, only the latter one can be identified.</p>
②	VC Hub/Phone	<ul style="list-style-type: none"> If you want to share contents, connect this port to the Codec port on the VCH50 video conferencing hub. If you need an audio device, connect this port to the Internet port on the CP960 Conference phone.
③	Display	Connects to a monitor.
④	Security Slot	Allows you to connect a universal security cable to VC800/VC500 codec, so you can lock it down. The system cannot be removed when locked.
⑤	Line Out	Connects to an audio output device using an audio cable (3.5mm).
⑥	Internet	Connects to the network device.

Bottom of VC200 Codec

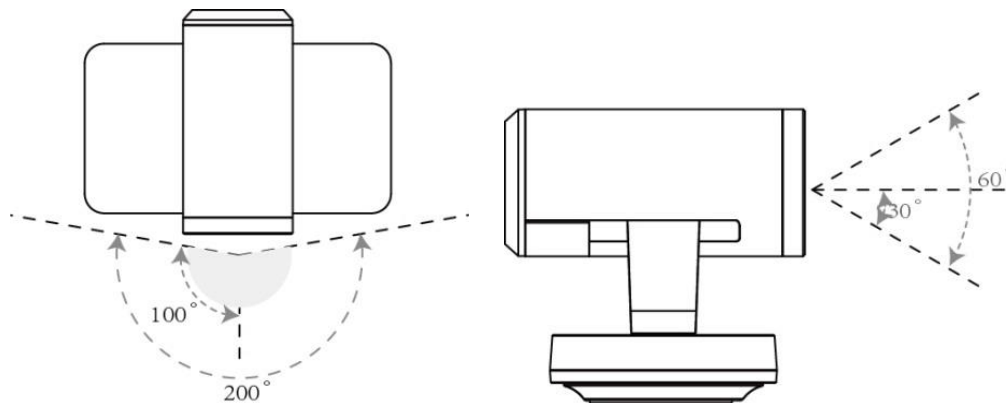


	Port Name	Description
⑦	VESA	Secures the endpoint to the TV stand or a tripod using a 1/4"-20 UNC screw
⑧	Reset Key	Resets the system to factory defaults.

Hardware of VCC22 Video Conferencing Camera

Yealink VC800 can connect up to 8 VCC22 cameras, and Yealink VC880 can connect up to 9 VCC22 cameras, developing a typical multi-camera solution. This dead-zone-free solution is suitable for every large meeting room and auditorium.

The camera can be panned (± 100 degrees range), tilted (± 30 degrees range) and supports 12 x optical zoom, white balance and automatic gain.

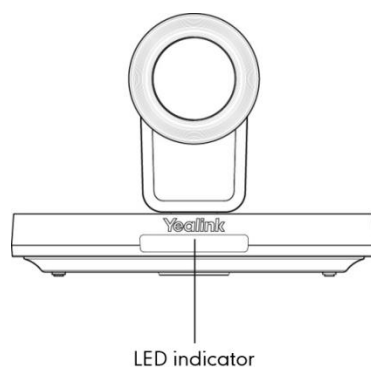


Note

VCC22 video conferencing cameras are not applicable to VC500/VC200 video conferencing endpoints.

Front Panel of VCC22 Video Conferencing Camera

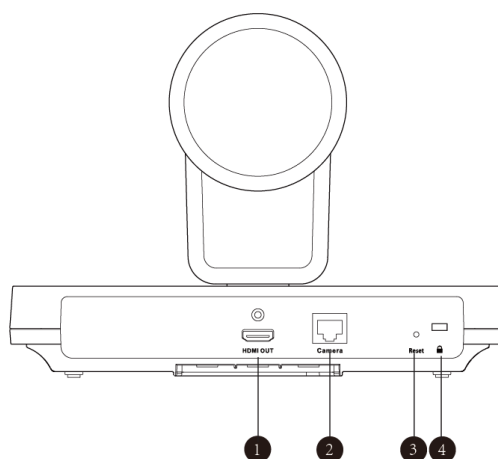
The LED indicator in front of the camera indicates different statuses of the camera.



Related Topic:

[LED Instructions of VCC22 Video Conferencing Camera](#)

Rear Panel of VCC22 Video Conferencing Camera



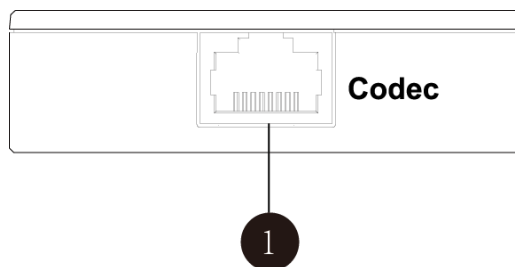
	Port Name	Description
①	HDMI Out	Connects to a monitor for displaying shared content.
②	Camera	Connects to a PoE switch.
③	Reset Key	Resets the camera to factory defaults.
④	Security Slot	Allows you to connect a universal security cable to VCC22, so you can lock it down. The camera cannot be removed when locked.

Hardware of VCH50 Video Conferencing Hub

If you want to connect a PC to your system using Ethernet cable, you need to connect the VCH50 video

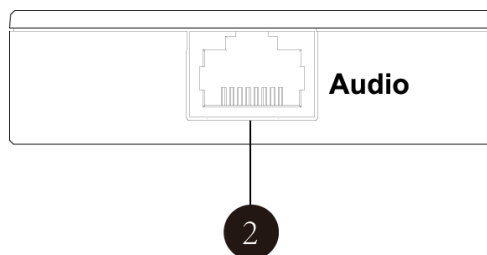
conferencing hub to your system.

Left Side of VCH50 Cable Hub



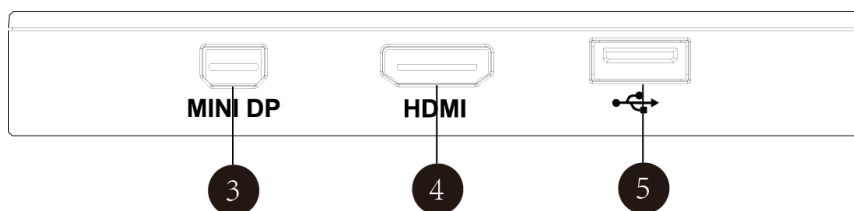
	Port Name	Description
①	Codec	Connects to the video conferencing system using the provided 7.5m network cable.

Right Side of VCH50 Cable Hub



	Port Name	Description
②	Audio	Connects to the CP960 Conference phone using the provided 0.5m network cable.

Rear Panel of VCH50 Cable Hub



	Port Name	Description
③	MINI DP	Connects to a PC using Mini-DP cable for sharing contents.
④	HDMI	Connects to a PC using HDMI cable for sharing contents.
⑤	USB	Inserts a USB flash drive to the USB port for storing screenshots, recording videos or capturing packets.

Hardware of CP960 Conference Phone

The CP960 conference phone can work as an audio device for the system. You can also place calls, answer calls or view directory and history on the CP960 conference phone.

Hardware component instructions of the phone are:

CP960 Conference Phone	NO.	Item	Description
	①	Three Internal Microphones	Supports 360-degree audio pickup at a radius of up to 6 meters.
	②	Mute Button	<ul style="list-style-type: none"> Indicates call statuses. Toggles mute feature.
	③	Speaker	Provides audio output.
	④	Touch Screen	5 inch (720 x 1280) capacitive (5-point) touch screen with two idle screens.
	⑤	Volume Touch Keys	Adjust the volume of the speaker, ringer or media.
	⑥	HOME Touch Key	Returns to the idle screen.
	⑦	Wired Mic Ports	Allow you to connect CPE90 to your phone (optional).
	⑧	Internet Port	<ul style="list-style-type: none"> Connect to the VC Hub/Phone port on the video conferencing system. Connect to the Audio port on the VCH50 video conferencing hub.
	⑨	Security Slot	Allows you to connect a universal security cable to your phone so you can lock down your phone. The phone will not be removed after locked.
	⑩	3.5mm Audio-out Port	This port is unavailable when CP960 conference phone works with the video conferencing system.
	⑪	Micro USB	This port is unavailable when

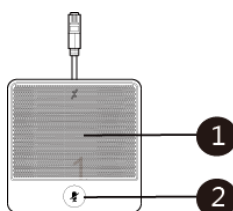
CP960 Conference Phone	NO.	Item	Description
		Port	CP960 conference phone works with the video conferencing system.
	⑫	USB Port	<ul style="list-style-type: none"> • Connects a USB flash drive to store screenshots, recording videos or captured packets. • Connects to the mini USB port on the charge cradle to charge the CPW90 wireless expansion microphones. <p>Note: If multiple USB flash drives are connected, only the latter one can be identified.</p>

Related Topic:

[LED Instructions of CP960 Conference Phone](#)

Hardware of CPE90 Wired Expansion Microphones

The CPE90 can work as expansion microphones of the CP960 conference phone. It supports 360-degree audio pickup at a radius of up to 3 meters. There is a mute button on its top. You can mute or unmute the CPE90 by tapping the mute button.



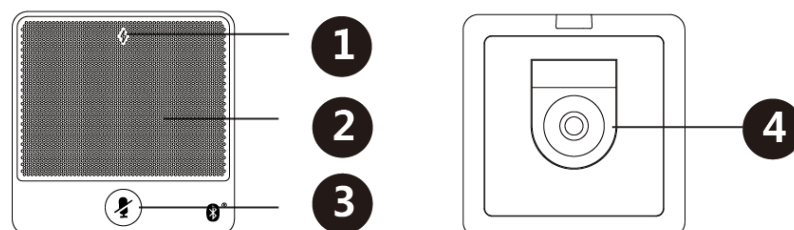
	Name	Description
①	Built-in Microphones	Support 360-degree audio pickup at a radius of up to 3 meters.
②	Mute Button	<ul style="list-style-type: none"> • Indicates call statuses. • Toggles mute feature.

Related Topic:

[LED Instructions of CPE90 Wired Expansion Microphones](#)

Hardware of CPW90-BT Bluetooth Wireless Microphone

The CPW90-BT is a Bluetooth wireless microphone, which can work as the audio input device of the video conferencing system. It supports 360-degree audio pickup at a radius of up to 3 meters. There are a mute button and a battery indicator LED on its top. You can mute or unmute the CPW90-BT by tapping the mute button.



	Name	Description
①	Battery Indicator LED	Indicates the battery information.
②	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 3 meters.
③	Mute Button	<ul style="list-style-type: none"> • Indicates statuses. • Toggles mute feature.
④	Charging Slot	Put the CPW90-BT on the charging cradle to charge.

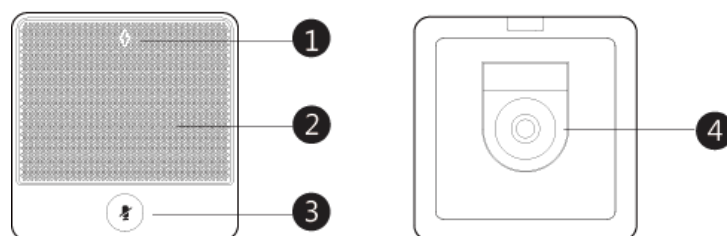
Related Topic:

[Using the CPW90-BT Bluetooth Wireless Microphones with VCS](#)

[LED Instructions of CPW90-BT Bluetooth Wireless Microphones](#)

Hardware of CPW90 Wireless Microphone

The CPW90 is a wireless microphone, which can work as the audio input device. It supports 360-degree audio pickup at a radius of up to 3 meters. There are a mute button and a battery indicator LED on its top. You can mute or unmute the CPW90 by tapping the mute button.



	Name	Description
①	Battery Indicator LED	Indicates the battery information.
②	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 3 meters.
③	Mute Button	<ul style="list-style-type: none"> Indicates statuses. Toggles mute feature.
④	Charging Slot	Put the CPW90 on the charging cradle to charge.

Related Topic:

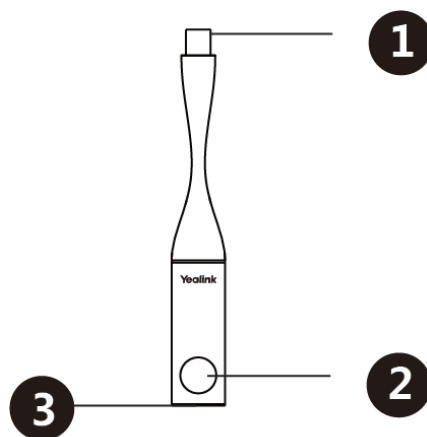
[LED Instructions of CPW90 Wireless Microphones](#)

[Using the CPW90 Wireless Microphones with VCS](#)

[Using the CPW90 Wireless Microphones with CP960](#)

Hardware of WPP20 Wireless Presentation Pod

Combining a self-built 5G Wi-Fi, WPP20, the wireless presentation pod, partners up with Yealink new-generation video conferencing system to offer high-quality wireless content sharing with just one tap.



	Name	Description
①	USB	<ul style="list-style-type: none"> • Connects to the video conferencing system to obtain Wi-Fi profile. • Connects to the PC for sharing content.
②	Presentation button	<ul style="list-style-type: none"> • Press it to start or stop sharing full screen of the PC. • Long press it for 3 seconds and then release it, choose the window you want to share.
③	Indicator LED	Indicates the status.

Related Topic:

[LED Instructions of WPP20 Wireless Presentation Pod](#)

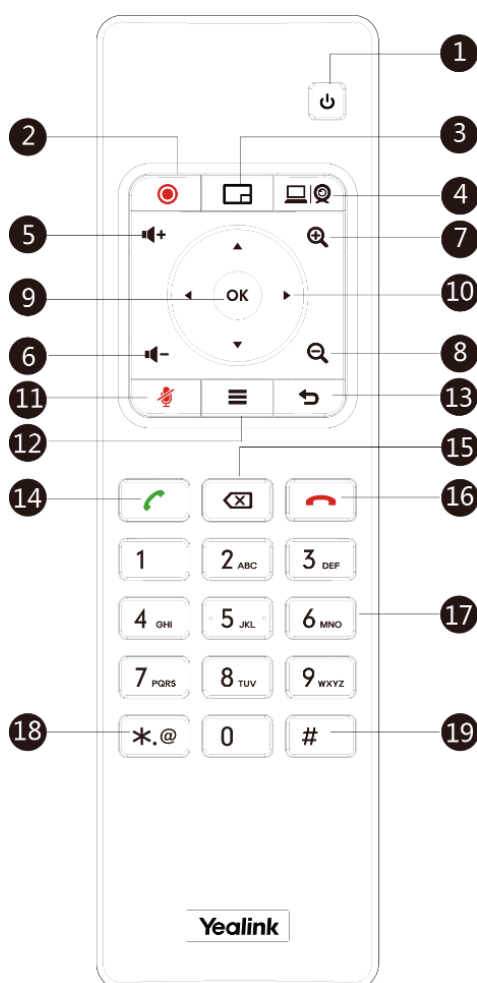
Hardware of VCR11 Remote Control

The VCR11 remote control enables you to operate a video conferencing system. This includes placing calls, adjusting the volume, controlling the camera, navigating screens, and more.

Tip

The infrared sensor locates within the LED indicator of camera. Aim the remote control at the infrared sensor to operate the camera.

The following table shows the parts of the remote control and includes descriptions for each part.



Description	
①	<ul style="list-style-type: none"> Power the System On and Off. Puts the system to sleep or wakes the system.
②	Starts or stops recording video and audio.
③	Adjust layout during a video call.
④	Use the predefined function. This key can be configured as a Presentation key (default), Input key, ScreenShot key or Mute Speaker key.
⑤	Increases the system volume.
⑥	Decreases the system volume.
⑦	<ul style="list-style-type: none"> Increases the camera zoom. Increases the captured image magnifications. Behaves as page up in a multiple page list.
⑧	<ul style="list-style-type: none"> Decreases the camera zoom.

Description	
	<ul style="list-style-type: none"> Decreases the captured image magnifications. Behaves as page down in a multiple page list.
⑨	Confirms actions or answers incoming calls.
⑩	<ul style="list-style-type: none"> Navigate through menu items. Pan and tilt the camera to adjust the viewing angle.
⑪	Toggles mute feature.
⑫	<ul style="list-style-type: none"> Returns to the idle screen when in the menu. Opens Talk Menu during a call.
⑬	Returns to the previous menu.
⑭	<ul style="list-style-type: none"> Enters the pre-dialing screen. Places a call. Answers a call.
⑮	<ul style="list-style-type: none"> Deletes one character at a time. Long press to delete all characters in the input field. Long press it for 2 seconds to start capturing packets and long press it for 2 seconds again to stop capturing packets.
⑯	<ul style="list-style-type: none"> Ends a call or exits from a conference call. Returns to the idle screen.
⑰	<ul style="list-style-type: none"> Enters digits. Enters the pre-dialing screen.
⑱	Generates special characters: .@*.
⑲	Generates a pound key (#).

Related Topic

[Remote Control](#)

LED Instructions

You can know the system status by viewing the LED light.

LED Instructions of VC880/VC800/VC500/VC200

LED Status	Description
Solid green	The system is powered on.
	The system is upgrading firmware.
Solid red	The system is in sleep mode.
Flashing red	The system codec is upgrading firmware.
Solid orange	System exception (for example: network unavailable, update failure).
Off	The system is powered off, or is not connected to the power adapter.

LED Instructions of VCC22 Video Conferencing Camera

LED Status	Description
Solid green	The VC880/VC800 system is powered on.
	The VC880/VC800 system is upgrading firmware.
	The VCC22 video conferencing camera is working.
Solid red	The VC880/VC800 system is in sleep mode.
	The VCC22 video conferencing camera is disabled.
Flashing red	The VCC22 video conferencing camera is upgrading firmware.
Solid orange	The VCC22 video conferencing camera is not selected.
Off	The VCC22 video conferencing camera is not connected to the PoE switch.

LED Instructions of CP960 Conference Phone

LED Status	Description
Solid red	The CP960 conference phone is initializing.
	The CP960 conference phone is muted.
Flashing red	The CP960 conference phone is ringing.
Solid green	The CP960 conference phone is placing a call.
	The CP960 conference phone is in a call and unmuted.
Off	The CP960 conference phone is idle.
	The CP960 conference phone is not connected to the video conferencing

LED Status	Description
	system correctly.

LED Instructions of CPE90 Wired Expansion Microphones

LED Status	Description
Solid red	The CP960 conference phone is muted.
Flashing red	The CP960 conference phone is ringing.
Solid green	The CP960 conference phone is placing a call.
	The CP960 conference phone is in a call and unmuted.
Off	The CPE90 is not connected to the CP960 conference phone.
	The CPE90 is idle.

LED Instructions of CPW90-BT Bluetooth Wireless Microphones

Battery Indicator LED

LED Status	Description
Solid green for one second and then off	The CPW90-BT is turned on.
Solid green for 3 seconds and then off	The CPW90-BT is in the idle mode.
Solid green	The CPW90-BT is fully charged.
Solid red	The CPW90-BT is being charged.
Fast flashing red 3 times and then off	The battery capacity is too low to turn on the CPW90-BT.
Slowly flashing red	The battery capacity is less than 10%.
Off	If you tap the mute button, the battery indicator LED on the CPW90-BT is still off, it means the CPW90-BT is turned off.

Mute Indicator LED

LED Status	Description
Solid green	The system is in a call and unmuted.
Slowly flashing red	The system is receiving an incoming call.

LED Status	Description
Solid red	The system is muted.
Fast flashing yellow	The CPW90-BT is in the registration mode.
Slowly flashing yellow	The CPW90-BT has registered with the VCS, but the VCS is out of range. The CPW90-BT has registered with the VCS, but the VCS is turned off.
Flashing red and green alternately	The VCS is searching for the CPW90-BT which has registered with it.
Off	The CPW90-BT is in the idle mode.

LED Instructions of CPW90 Wireless Microphones

Battery Indicator LED

LED Status	Description
Solid green for one second and then off	The CPW90 is turned on.
Solid green for 3 seconds and then off	The CPW90 is in the idle mode.
Solid green	The CPW90 is fully charged.
Solid red	The CPW90 is being charged.
Fast flashing red 3 times and then off	The battery capacity is too low to turn on the CPW90.
Slowly flashing red	The battery capacity is less than 10%.
Off	If you tap the mute button, the battery indicator LED on the CPW90 is still off, it means the CPW90 is turned off.

Mute Indicator LED

LED Status	Description
Solid green	The CP960 enters the pre-dialing screen.
	The system is in a call and unmuted.
Slowly flashing red	The system is receiving an incoming call.
Solid red	The system is muted.
Fast flashing yellow	The CPW90 is in the registration mode.

LED Status	Description
Slowly flashing yellow	The CPW90 has registered with the CP960/VCS, but the CP960/VCS is out of range. The CPW90 has registered with the CP960/VCS, but the CP960/VCS is turned off.
Flashing red and green alternately	The CP960/VCS is searching for the CPW90 which has registered with it.
Off	The CPW90 is in the idle mode.

LED Instructions of WPP20 Wireless Presentation Pod


LED Status	Description
Fast flashing green	The WPP20 is starting up.
	The WPP20 is trying to pair to the video conferencing system.
	The WPP20 is plugged into the video conferencing system, and firmware update is in progress.
	The WPP20 is plugged into the video conferencing system, and the WPP20 is updating Wi-Fi profile.
Slowly flashing green	The WPP20 pairs to the video conferencing system successfully, but you are not sharing content.
Solid green	The WPP20 pairs to the video conferencing system successfully, and you are sharing content.
	Firmware update is done.
	Wi-Fi profile update is done.
Slowly flashing red	The WPP20 cannot find or connect to the video conferencing system in 10 seconds after start-up.
	The WPP20 pairs to the video conferencing system successfully, but it does not detect the Yealink Wireless Presentation Pod software is running on your PC.
	Yealink Wireless Presentation Pod software is turned off.
	Firmware update fails.
	Wi-Fi profile update fails.

Powering On and Off

Powering On the System

Your system starts up automatically after you connect an electrical supply. If you power off the system using the remote control, do the following to power it up.

Procedure

1. Press  to power on your system.


Your system is powered on successfully, and the LED indicator illuminates solid green.

Related Topic:

[Powering Off the System](#)

Powering Off the System

Procedure

1. On your remote control, press .
2. Select **Shut down** and then press **OK** key.

The system shuts down immediately, and the LED indicator turns off.

Related Topic:

[Powering On the System](#)

Initialization Process Overview

The initialization process of the system is responsible for network connectivity and operation of the system in your local network. Once connect your system to the network and to an electrical supply, the system begins its initialization process.

Loading the ROM File

The ROM file resides in the flash memory of the system. The system comes from the factory with a ROM file preloaded. During initialization, the system runs a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If you connect the system to a switch, the switch notifies the system of the VLAN information defined on the switch. The system can then proceed with the DHCP request for its network settings (if using DHCP).

Querying the DHCP (Dynamic Host Configuration Protocol)

Server

The system is capable of querying a DHCP server.

After establishing network connectivity, the system can obtain the following network parameters from the DHCP server during initialization:

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

By default, the system obtains these parameters from a DHCPv4. You can configure network parameters of the system manually if any of them are not supplied by the DHCP server.

Running the Setup Wizard

The setup wizard appears during initial setup or factory reset, navigate the screens and perform the required steps to configure the system.

Tip

You can run the setup wizard using your remote control.

You can also tap **Exit Boot Wizard** on your CP960 conference phone to skip the setup wizard.

You can configure following features during setup wizard.

Menu	Description
Language	Set the language displayed on the monitor.
Date&Time	The system obtains the time and date from the NTP server automatically by default. You can also configure the time and date manually.
Site Name	Edit the site name.
Password	Change the administrator password.
Firewall Port forwarding	Displays firewall Port forwarding information.
Wired Network	Your system can obtain the network settings from a Dynamic Host Configuration Protocol (DHCP) server. You can also configure network settings manually.
Wi-Fi (only applicable to VC200)	Connects to Wi-Fi.
Account	(Optional) Log into the video conferencing platform. Your system supports Yealink VC Cloud Management Service/Yealink Meeting Server/StarLeaf/Zoom/Pexip/BlueJeans/Custom platform.

After you complete the setup wizard, the system starts up properly and is ready for use.

Configuration Methods

You can configure your system using web user interface, VCR11 remote control or CP960 conference phone.

Using Web User Interface

A web-based interface is especially useful for remote configuration. You can use the web user interface to perform most of the calling and configuration tasks.

Logging on to Web User Interface

To log on to your system's web user interface, you must open a web browser and enter the system's IP address. Login credentials are required for accessing the web user interface. The default administrator user name is "admin" and password is "0000" (case-sensitive).

Before you begin

Make sure the system is power on.

Procedure

1. On your computer, enter the system's IP address into your web browser.
2. Enter the administrator user name and password.
3. Click **Login**.

Caution:

The web user interface will be locked after 3 failed login attempts. Please contact your support team or try again 3 minutes later.

Related Topic

[Web Server Type Configuration](#)

[User and Administrator](#)

Web Server Type Configuration

Web server type determines the access protocol of the system's web user interface. The web user interface supports both HTTP and HTTPS protocols. The HTTPS protocol ensures that the configuration of all login information (such as user names and passwords) is transmitted using an encrypted channel. If you disable the desired protocol, you cannot access the web user interface using this protocol.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Advanced->Web Server**.

- For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->Web Server Type.**
- For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->Web Server Type.**

2. Configure and save the following settings:

Parameter	Description	Configuration Method
HTTP	Enables or disables the user to access the system web user interface using the HTTP protocol. Default: Enabled	Web User Interface Remote Control
HTTP Port	Specifies the HTTP port for the user to access the system's the web user interface. Valid Values: 1-65535 Default: 80 Note: Ensure that the configured port is not used.	Web User Interface
HTTPS	Enables or disables the user to access the system web user interface using the HTTPS protocol. Default: Enabled	Web User Interface Remote Control
HTTPS Port	Specifies the HTTPS port for the user to access the system's the web user interface. Valid Values: 1-65535 Default: 443 Note: Ensure that the configured port is not used.	Web User Interface

Using Remote Control

You can use the real remote control or virtual remote control to configure and use the system. If you do not use remote control, you can disable it.

Using Virtual Remote Control

You can use virtual remote control on your web user interface to control your system.

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500: on your web user interface, go to **Home->Remote Control** to show

or hide the virtual remote control.

- For VC200: on your web user interface, go to **VC200->Remote Control** to show or hide the virtual remote control.

Configuring Remote Control

Remote control feature is enabled by default. If your environment does not use remote control to control the system, you can disable remote control feature.

Procedure

1. On your web user interface, go to **Setting->General**.
2. Select the desired value from the pull-down list of **Remote Control Enabled**.

Using CP960 Conference Phone

You can use the CP960 conference phone to perform calling and partial configuration tasks. For more information, refer to [Yealink CP960 HD IP Conference Phone Quick Reference Guide](#).

VCS Deployment Methods

Topics:

[Traditional Deployment Methods](#)

[Cloud Deployment Method](#)

Traditional Deployment Methods

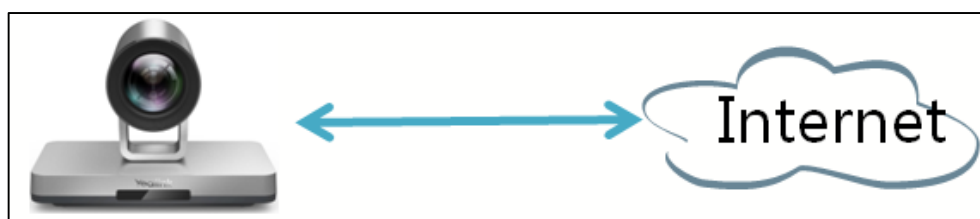
If you do not use cloud-based service, you can choose traditional deployment method to deploy your VCS, and dial IP addresses or SIP/H.323 account of other devices to make a call.

Use one of the following methods to deploy your VCS:

- Public IP Configuration (Outside of Firewall)
- Port forwarding with ALG feature
- Port forwarding with static NAT feature
- STUN
- H.460
- Intelligent traversal
- VPN

Public IP Configuration

Your video conferencing system is connected to the Internet directly.



This deployment method involves a simple setup process and creates a stable network environment. However, it is more expensive due to leased line costs. This method is often used in the head office.

Port Forwarding

The most common deployment scenario is deploying the VCS in an intranet (behind a firewall). You must assign a static private IP address to the VCS. In the meantime, do port forwarding on the firewall.

Port forwarding is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a

network gateway, such as a router or firewall.

To receive a public-to-private call, you must forward the following ports to the public network on your router or firewall.

Description	Port Range	Port Type
Gatekeeper	1719	UDP
H.323 Call setup	1720	TCP
Control and media for audio, video, content, and data/FECC	50000-51000	TCP/UDP
Web management port (optional)	443	TCP
SIP (optional)	5060-5061	TCP/UDP

Related Topic

[NAT](#)

NAT

Many application-layer protocols, such as multimedia protocols (H.323/SIP) have address or port information. The address and port information included in the H.323/SIP protocol cannot be translated via the traditional NAT method, which leads to communication problems.

ALG (application layer gateway) feature on the router/firewall can help translate address and port of application-layer protocols. If your router does not support ALG feature, you should configure port forwarding on your router first, and then enable static NAT feature on your system to help address and port in the H.323/SIP protocol traverse the firewall.

Note

If H.460 firewall traversal is enabled on the system, the system will automatically ignore the static NAT settings for H.323 calls. For more information, refer to [Configuring H.460 for H.323 Calls](#) on page 49.

Related Topic:

[Port Forwarding](#)

[Selecting Static NAT for SIP Calls](#)

Configuring NAT

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->NAT/Firewall->NAT Configuration**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->NAT/Firewall->NAT**.

- For VC200: on your remote control, go to **More->Network->Wired Network->NAT/Firewall->NAT**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static NAT/ Type	<p>Specifies the static NAT type.</p> <ul style="list-style-type: none"> • Disabled—the system does not use the NAT feature. • Manual—the system uses the manually configured NAT public address. • Auto—the system obtains the NAT public address from the Yealink-supplied server. <p>Default: Disabled</p>	<p>Web User Interface Remote Control</p>
NAT Public IP Address/ Public IP Address	<ul style="list-style-type: none"> • Displays the NAT public address automatically obtained from the Yealink-supplied server if the static NAT is set to Auto. • Configures the NAT public address for the system if the static NAT is set to Manual. 	<p>Web User Interface Remote Control</p>

Related Topic:

[Selecting Static NAT for SIP Calls](#)

[Port Forwarding](#)

Selecting Static NAT for SIP Calls

You can use H.233 protocol to make a private-to-public call directly after you configure the port forwarding settings and enable the static NAT feature. If you want to use SIP account or SIP IP address to make a private-to-public call, you need another step: apply the static NAT settings to the SIP protocol.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->SIP Account->NAT Traversal**.
 - On your web user interface, go to **Account->SIP IP Call->NAT Traversal**.
 - On your remote control, go to **More->Setting->Advanced->SIP IP Call->NAT Traversal**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select StaticNat.	Web User Interface Remote Control

Related Topic:

[Port Forwarding](#)

[Configuring NAT](#)

Route Traversal

If your environment has a secondary router connected to the first router, the VCS connected to each router may not be able to communicate properly. In this situation, you can configure static NAT and enable route traversal feature forcibly on the VCS that is connected to the secondary router, so that the NAT works even though both devices are in the Intranet.

Caution:

If you enable route traversal forcibly, the risk is that the VCS may fail to call the other VCS connected to the same router, because the NAT address replaces the private address.

Procedure

1. On your web user interface, go to **Network->NAT/Firewall->NAT Configuration**.
2. Configure and save the following settings:

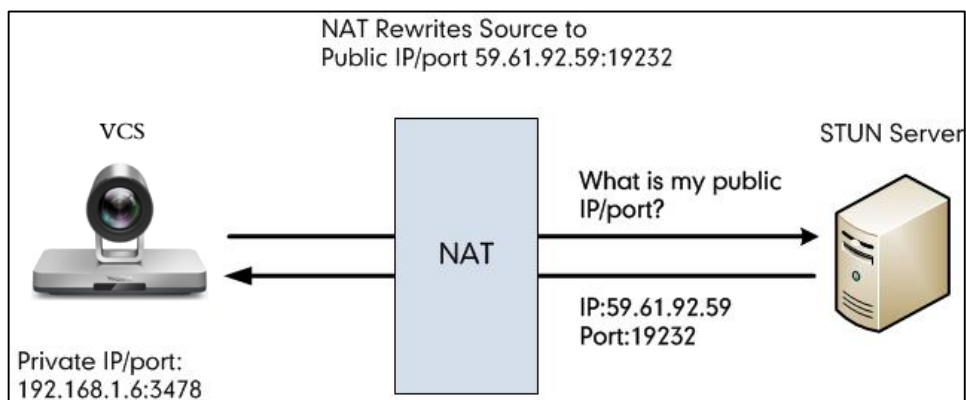
Parameter	Description	Configuration Method
Static NAT/ NAT	Select Manual , and then configure the NAT address manually.	Web User Interface Remote Control
NAT Public IP Address/ Public IP Address	Configures the NAT address for the system manually.	Web User Interface Remote Control
Route Traversal	Configures the route traversal type. <ul style="list-style-type: none"> • Auto–NAT works only when making a call to a public address. NAT does not work when making a call to a private address. • Compulsory–NAT works no matter you are making a call to a public address or private address. Default: Auto	Web User Interface

3. Apply the route traversal settings to the SIP protocol.

For more information, refer to [Selecting Static NAT for SIP Calls](#) on page 45.

STUN

You can use the Simple Traversal of UDP through NAT (STUN) function besides ALG or static NAT. If STUN is enabled, the system can perform private-to-public network traversal using the STUN server. STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows the system behind a NAT to first discover the presence of a NAT and the type of NAT, and then allows the system to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The system can be configured to work as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client. For more information, refer to [RFC3489](#).



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

No.	Time	Source	Destination	Protocol	Length	Info
444	18.587848	192.168.1.6	218.107.220.74	STUN	62	Binding Request
447	18.711349	218.107.220.74	192.168.1.6	STUN	98	Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232

The system will send SIP message using the mapped IP address and port.

Note

STUN does not enable incoming TCP connections through NAT or incoming UDP packets through symmetric NATs.

Configuring STUN

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->NAT/Firewall->STUN Config**.
 - For VC880/VC800/VC500: on your remote control, go to

More->Setting->Advanced->NAT/Firewall->STUN Config.

- For VC200: on your remote control, go to **More->Network->Wired Network->NAT/Firewall->STUN Config.**

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active/ STUN Active	Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the system. Default: Disabled	Web User Interface Remote Control
STUN Server	Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. Default: Blank	Web User Interface Remote Control
STUN Port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. Default: 3478	Web User Interface Remote Control

Selecting STUN for SIP Calls

To make a private-to-public call, you can enable STUN feature for SIP account or SIP IP address.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->SIP Account.**
 - On your web user interface, go to **Account->SIP IP Call.**
 - On your remote control, go to **More->Setting->Advanced >SIP IP Call.**
2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select STUN.	Web User Interface

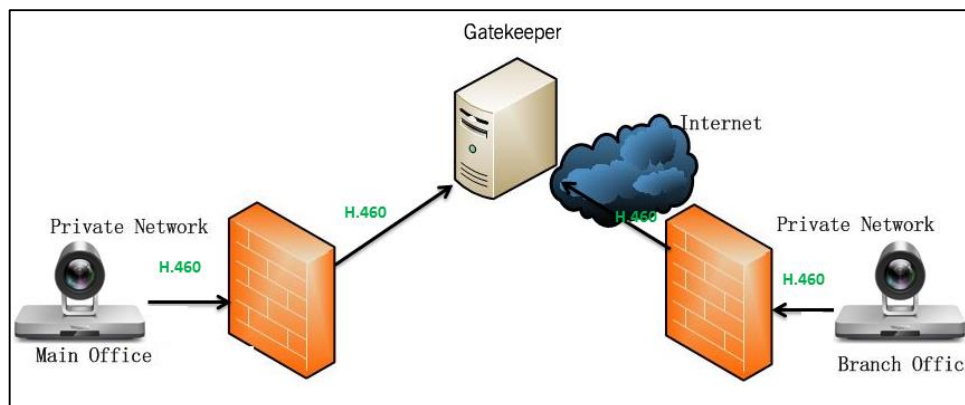
Related Topic:

[Configuring SIP Settings](#)

[STUN](#)

H.460

Yealink video conferencing systems support firewall traversal of H.323 calls using H.460 protocols. To use this feature, make sure your gatekeeper supports H.460 feature.



Note

If you configure H.323 settings and enable H.460 support, the system ignores static NAT settings.

Configuring H.460 for H.323 Calls

To make a private-to-public call, you can enable H.460 feature for H.323 protocol.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->H.323->H.460 Active**.
 - On your remote control, go to **More->Setting->Advanced->H.323->H.460**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
H.460 Active/ H.460	Enables or disables firewall traversal of H.323 calls using H.460 protocols. Default: Disabled	Web User Interface Remote Control

Related Topic:

[Configuring H.323 Settings](#)

Intelligent Traversal

Some branch offices lack IT professionals, which means that professional network configuration (for example: port forwarding) is impossible. You can deploy the VCS in an intranet, and assign a private IP address to it, make sure the private IP address can access the public network.

To make a private-to-public call, you only need to enable the intelligent traversal feature. But using this

method, inbound calls are unavailable.

Audio & Video Intelligent Traversal

When VCS in the Intranet calls the VCS in the public network, the audio & video streams may carry private addresses, resulting that the VCS in the public network cannot send the audio& video streams to the correct addresses, and VCS in the Intranet experiences one-way audio or video.

The intelligent traversal feature allows the VCS in the public network to check the media source address and port of incoming RTP packets, and then send back RTP packets to the address where incoming RTP packet comes from, instead of the address provided in the Session Description Protocol (SDP).

The following example illustrates a scenario about using audio & video intelligent traversal:

The VCS A locates in the Intranet and the router does not support the ALG feature. The VCS B locates in the public network. A calls B, and then A sends the RTP packets to the B.

- If B disables the audio & video intelligent traversal feature, B sends RTP data to the negotiated IP address of A (private IP address provided in the Session Description Protocol), causing the device display of A appears black screen.
- If B enables the audio & video intelligent traversal feature, B sends back RTP packets to the address where incoming RTP packet comes from. A and B can communicate normally.

Configuring Audio & Video Intelligent Traversal

Procedure

1. On your web user interface, go to **Network->NAT/Firewall->Intelligent Firewall Traversal->Audio&Video Intelligent Traversal**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Audio&Video Intelligent Traversal	Enables or disables the audio & video media stream to traverse firewall. Default: On	Web User Interface

Data Intelligent Traversal

When VCS in the Intranet calls the VCS in the public network, the VCS in the Intranet may fail to receive data (for example: PC content and FECC protocol) from the public network. You can use data intelligent traversal to solve these problems.

The following example illustrates a scenario about using data intelligent traversal:

The VCS A locates in the Intranet and the router supports the ALG feature. The VCS B locates in the public network.

The ALG feature on the router can temporarily map the port to a public port, which lasts 30 seconds by default. If the VCS B in the public network does not share content within 30 seconds, the mapped port will change, so that the VCS B may fail to share content to VCS A later. To solve this problem, enable the

data intelligent traversal on VCS A, the VCS A will send keep-alive messages at regular intervals to keep the port open, so that the VCS B can share content normally.

Configuring Data Intelligent Traversal

Procedure

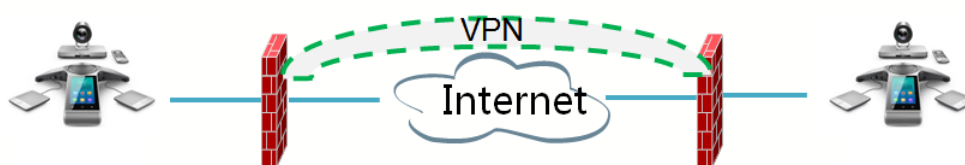
1. On your web user interface, go to **Network->NAT/Firewall->Intelligent Firewall Traversal ->Data Intelligent Traversal**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Data Intelligent Traversal	Enables or disables the PC content and FECC protocol to traverse firewall. Default: On	Web User Interface

VPN

Yealink video conferencing system uses OpenVPN to achieve VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After you configure VPN feature on the system, the system will act as a VPN client and uses the certificates to authenticate the VPN server.

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



VPN Related Files

To use VPN, you should upload the compressed package of VPN-related files to the system in advance. The file format of the compressed package must be *.tar. The related VPN files are certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client.

The following table lists the unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for your system:

VPN files	Description	Unified Directories
ca.crt	CA certificate	/config/openvpn/keys/ca.crt
client.crt	Client certificate	/config/openvpn/keys/client.crt

VPN files	Description	Unified Directories
client.key	Private key of the client	/config/openvpn/keys/client.key

VPN Configuration

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Advanced->VPN**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advance Network->VPN**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->NAT/Firewall->VPN**.
- Configure and save the following setting:

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

Cloud Deployment Method

When holding a video conference, customers often encounter several problems, such as no public IP address, weak network infrastructure, complicated firewall configuration, inefficient deployment and no traversal server.

Cloud-based technology drives positive change in the way organizations communicate. With video conference platform, organizations can communicate easily. Public IP address and complex network settings are unnecessary.

Challenges such as infrastructure costs and interoperability are eliminated. Both the head office and the branch offices can use the cloud deployment method. Both inbound and outbound calls are available.

Related Topic:

[Registering a Yealink Cloud Account](#)

Configuring System Settings

Topics:

[Configuring Network Settings](#)

[Configuring Account Settings](#)

[Configuring General Settings](#)

[Configuring Audio Settings](#)

[Configuring Video Settings](#)

[Configuring Content Sharing](#)

[Configuring Camera Settings](#)

[Configuring Call Settings](#)

[Configuring Conference Room](#)

This chapter provides information for configuring system settings, such as account, network, audio and video settings.

Configuring Network Settings

The following introduces how to configure network settings.

IPv4 and IPv6 Network Settings

Yealink video conferencing system support IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack-addressing mode.

Note

Yealink video conferencing systems comply with the DHCPv4 specifications documented in [RFC 2131](#), and DHCPv6 specifications documented in [RFC 3315](#).

IP Addressing Mode Configuration

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->LAN Configuration->Internet Port->IPv4/IPv6**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wired Network->IP Mode**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->IP Mode**.

2. Configure and save the following setting:

Parameter	Description	Configuration Method
IPv4/IPv6 /IP Mode	Configures the IP address mode. Default: IPv4 Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control

IPv4 Configuration

After connected to the wired network, the system can obtain the IPv4 network settings from a Dynamic Host Configuration Protocol (DHCP) server if your network supports it.

You can also configure IPv4 network settings manually.

Before you begin

Make sure the IP address mode is set to IPv4 or IPv4&IPv6.

Procedure

1. Do one of the following:

- On your web user interface, go to **Network->LAN Configuration->IPv4 Config**.
- On your remote control, go to **More->Setting->Advanced->Wired Network->IPv4**.
- For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wired Network->IPv4**.
- For VC200: on your remote control, go to **More->Network->Wired Network->IPv4**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
DHCP	Enables or disables the system to obtain network settings from the DHCP server. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Static IP	Enables or disables the system to use manually configured network settings. Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
IP Address	Configures the IPv4 address assigned to the system. Default: Blank Note: If you change this parameter, the system will	Web User Interface Remote Control

Parameter	Description	Configuration Method
	reboot to make the change take effect.	
Subnet Mask	Configures the subnet mask assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Gateway	Configures the gateway assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Static DNS	Triggers the static DNS feature to on or off. Default: Off Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Primary DNS/ DNS primary Server	Configures the primary DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Secondary DNS/ DNS Secondary Server	Configures the secondary DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control

IPv6 Configuration

You can set up an IPv6 address for the system either by using DHCPv6 or by manually configuring an IPv6 address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

Before you begin

Make sure the IP address mode is set to IPv6 or IPv4&IPv6.

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->LAN Configuration->IPv6 Config**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wired Network->IPv6**.

- For VC200: on your remote control, go to **More->Network->Wired Network->IPv6**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
DHCP	<p>Enables or disables the system to obtain network settings from the DHCP server.</p> <p>Default: Enabled/On</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Static IP	<p>Enables or disables the system to use manually configured IPv6 network settings.</p> <p>Default: Disabled</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p>
IP Address	<p>Configures the IPv6 address assigned to the system.</p> <p>Default: Blank</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>
IPv6 prefix((0~128)/ IPv6 prefix	<p>Configures the IPv6 prefix.</p> <p>Default: Blank</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Gateway	<p>Configures the IPv6 default gateway.</p> <p>Default: Blank</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Static IPv6 DNS/Static DNS	<p>Triggers the static IPv6 DNS feature to on or off.</p> <p>Default: Off</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
Primary DNS/ DNS primary Server	Configures the primary IPv6 DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Secondary DNS/ DNS Secondary Server	Configures the secondary IPv6 DNS server assigned to the system. Default: Blank Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control

DHCP Option

DHCP options are added network and other control information that a DHCP server can hand out to the systems.

Note

For more information on DHCP options, refer to [RFC 2131](#) or [RFC 2132](#).

Supported DHCP Option for IPv4

The following table lists common DHCP options for IPv4 supported by Yealink video conferencing system.

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

Parameters	DHCP Option	Description
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identify the vendor-specific information.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

DHCP Option 42, Option 2

Your system supports using the NTP server address offered by DHCP.

DHCP option 42 is used to specify a list of NTP servers available to the client by IP address. NTP servers should be listed in order of preference.

DHCP option 2 is used to specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

Related Topic:

[NTP Settings](#)

DHCP Option 12

You can specify a hostname for the system when using DHCP. The DHCP client uses option 12 to send a predefined hostname to the DHCP registration server. The name may or may not be qualified with the local domain name (based on [RFC 2132](#)). See [RFC 1035](#) for character restrictions.

Related Topic:

[Host Name Configuration](#)

Host Name Configuration

Procedure

1. On your web user interface, go to **Network->LAN Configuration->Host Name**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Host Name	Configures the host name of the system. Default: Blank	Web User Interface

Parameter	Description	Configuration Method
	<p>Note: When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	

Related Topic:

[DHCP Option 12](#)

VLAN

The purpose of VLAN configurations on the system is to insert tag with VLAN information to the packets generated by the system. When VLAN is properly configured for the Internet port on the system, the system will tag all packets from the Internet port with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

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

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

Configuring LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows systems 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.

When LLDP feature is enabled on systems, the systems periodically advertise their own information to the directly connected LLDP-enabled switch. The systems can also receive LLDP packets from the connected switch and obtain their VLAN IDs, and then start communications with the call control.

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Advanced->LLDP**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->LLDP**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->LLDP**.
- Configure and save the following settings:

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

Configuring VLAN Manually

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

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Advanced->VLAN->Internet Port**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->VLAN**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->VLAN**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Active	Enables or disables VLAN for the Internet port. Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
VID(1-4094)	Specifies the identification of the Virtual LAN. Default: 1 Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Priority	Configures VLAN priority for the Internet port. Valid values: 0-7	Web User Interface Remote Control

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 make the change take effect.</p>	

Configuring DHCP VLAN

Your system supports VLAN discovery via DHCP. When the VLAN discovery method is set to DHCP, the system will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Procedure

1. On your web user interface, go to **Network->Advanced->VLAN->DHCP VLAN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
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 make the change take effect.</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 make the change take effect.</p>	Web User Interface

Wi-Fi

Wi-Fi feature enables you to connect the system to the organization's wireless network.


For VC880/VC800/VC500, you need to connect a WF50 Wi-Fi USB Dongle to the system for connecting to the wireless network.

For VC200, you can connect to the wireless network directly.

Connecting to the Wireless Network

There are two ways to connect to the wireless network:

- Manually connect to an available wireless network
- Manually connect to hidden wireless network

When the system connects to a wireless network, the Wi-Fi icon  will display on the status bar. The Wi-Fi icon indicates the signal strength. The more arcs you see, the stronger the signal strength is.

Manually Connect to an Available Wireless Network

You can manually connect your phone to a wireless network.

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wi-Fi**.
 - For VC200: on your remote control, go to **More->Network->Wi-Fi**.
2. Check the checkbox of **Wi-Fi**
3. If you already enabled wireless AP, select **OK** to turn it off. The system will automatically search for available wireless networks in your area.
4. Select the desired wireless network (SSID) to connect to it.
5. If the network is secure, enter its password in the **Password** field.
6. Select **Join to Network**.

Manually Connect to hidden Wireless Network

For security, there are some wireless networks that do not broadcast their SSID or name. This makes the wireless network is not displayed when you are browsing the list of available networks. In order to connect to one of these types of networks you will need to create a manual wireless connection.

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wi-Fi**.
 - For VC200: on your remote control, go to **More->Network->Wi-Fi**.
2. Check the checkbox of **Wi-Fi**.
3. If you already enabled wireless AP, select **OK** to turn it off. The system will automatically search for available wireless networks in your area.
4. Select **Other**.
5. Select the desired value from the pull-down list of **Security Mode**.
6. Configure the corresponding fields.
7. If the network is secure, enter its password in the **Password** field.
8. Select **Join to Network**.

Viewing the Wireless Network Status

You can view the wireless network status.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Wi-Fi->Wi-Fi Status->Connection Status**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wi-Fi->Wi-Fi State**.
 - For VC200: on your remote control, go to **More->Network->Wi-Fi->Wi-Fi State**.
2. View the detailed wireless network information (e.g., SSID or signal strength).

Forgetting a Wi-Fi Connection Profile

If you are connected to a wireless network and would no longer like to connect to it automatically, you can choose to forget it.

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wi-Fi**.
 - For VC200: on your remote control, go to **More->Network->Wi-Fi**.
2. Select the saved wireless network (SSID), and then select **Forget the Network**.

Disabling Wi-Fi Feature

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Wi-Fi->Wi-Fi Config->Wi-Fi Switch**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wi-Fi**.
 - For VC200: on your remote control, go to **More->Network->Wi-Fi**.
2. Disable Wi-Fi.

Wireless Access Point

Video conferencing system can provide wireless access point (AP) for other device.

For VC880/VC800/VC500, you need to connect a WF50 Wi-Fi USB Dongle to the system for providing wireless AP.

For VC200, you can provide wireless AP directly.

Enabling Wireless Access Point

- Do one of the following:
 - On your web user interface, go to **Network->Wireless AP->AP Config**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wireless AP**.
 - For VC200: on your remote control, go to **More->Network->Wireless AP**.
- Enable **Wireless AP**
- If you already enabled Wi-Fi, select **OK** to turn it off.

Configuring Wireless Access Point


Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Wireless AP**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wireless AP**.
 - For VC200: on your remote control, go to **More->Network->Wireless AP**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
AP Name	Configures the name of wireless AP.	Web User Interface Remote Control
Security Mode	Configures the security mode of the wireless AP. <ul style="list-style-type: none"> None WPA2-PSK Default: WPA2-PSK	Web User Interface Remote Control
Password	Configures the password of the wireless AP.	Web User Interface Remote Control
Network Sharing	Enables or disables the system to share its wired network to the connected devices. <ul style="list-style-type: none"> Enabled—The connected devices can use an Internet connection. Disabled—The connected devices cannot use an Internet connection. Default: Disabled	Web User Interface Remote Control
Frequency	Configures the frequency of the wireless AP.	Web User Interface Remote Control

Parameter	Description	Configuration Method
	<ul style="list-style-type: none"> • 2.4G • 5G Default: 5G	
Channel	Configures the channel of the wireless AP. Default: Auto	Web User Interface Remote Control
AP ID Address	Configures the generation type of wireless AP address. <ul style="list-style-type: none"> • Auto—generates the wireless AP address automatically. The default network segment is 192.168.144.X. • Manual—If automatically generated network segment conflict with your used one, you can change the network segment manually. Default: Disabled	Web User Interface Remote Control
IP Address	Configures the IP address of the wireless AP. Note: It only works if the value of AP ID Address is set to Manual .	Web User Interface Remote Control

Viewing the Connected Devices

If other devices connect to your wireless AP, the number of connections appears beside the  icon. You can view the details of the connected devices.

Procedure

- Do one of the following:
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wireless AP->AP Device List**
 - For VC200: on your remote control, go to **More->Network->Wireless AP->AP Device List**.
- View the names and MAC addresses of the connected devices.

Disabling Wireless Access Point

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Wireless AP**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Wireless AP**.

- For VC200: on your remote control, go to **More->Network->Wireless AP**.
2. Disable wireless AP.

802.1x Authentication

The system supports the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)

For more information on 802.1X authentication, refer to [Yealink 802.1X Authentication](#).

802.1x Authentication Configuration

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Advanced->802.1x**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->802.1x Mode**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->802.1x Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
802.1x Mode	Specifies the 802.1x authentication mode. <ul style="list-style-type: none"> • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 Default: Disabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Identity	Configures the user name for 802.1x authentication. Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

Parameter	Description	Configuration Method
MD5 Password	Configures the password for 802.1x authentication. Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the access URL of the CA certificate when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPV2 or EAP-TTLS/EAP-MSCHAPV2. Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Device Certificates	Configures the access URL of the server certificate when the 802.1x authentication mode is configured as EAP-TLS. Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

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.

Supported Transmission Methods

Supported transmission methods for VC880/VC800/VC500 system's Internet port:

- Auto-negotiate
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)

Supported transmission methods for VC200 endpoint's Internet port:

- Auto-negotiate
- Half-duplex (transmit in 10Mbps or 100Mbps)
- Full-duplex (transmit in 10Mbps or 100Mbps)

Configuring Transmission Methods

Procedure

1. On your web user interface, go to **Network->Advanced->Speed->Network Speed**.
2. Configure and save the following setting:

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

Restricting Reserved Ports

By default, the system communicates through TCP and UDP ports in the 50000 - 51000 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.

To minimize the number of UDP and TCP ports that are available for communication, you can restrict the ports range

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->NAT/Firewall->Reserved Port**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->NAT/Firewall->Reserved Port**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->NAT/Firewall->Reserved Port**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
UDP Port Scope	<p>Configures the range of the UDP ports.</p> <p>Valid values: 1024-65000</p> <p>Default range: 50000-51000</p> <p>Note: SIP and H.323 calls share the</p>	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
	configured ports. If you change this parameter, the system will reboot to make the change take effect.	
TCP Port Scope	Configures the range of the TCP ports. Valid values: 1024-65000 Default range: 50000-51000 Note: SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control

Quality of Service (QoS)

Video conferencing system is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. Your system supports the DiffServ model of QoS.

Audio QoS

In order to make VoIP transmissions intelligible to receivers, audio packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the audio 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 better presentation, data packets (PC content) emanated from the system should be configured with a high transmission priority.

DSCPs for audio, video and data packets can be specified respectively.

QoS Configuration

Procedure

- Do one of the following:
 - On your web user interface, go to **Network->Advanced->QoS**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->QoS**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->QoS**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
QoS Enable	Enables or disables QoS feature. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Audio Priority	Configures the DSCP (Differentiated Services Code Point) for audio packets. Valid Values: 0 to 63 Default: 63 Note: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Video Priority	Configures the DSCP (Differentiated Services Code Point) for video packets. Valid Values: 0 to 63 Default: 34 Note: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface Remote Control
Data Priority	Configures the DSCP (Differentiated Services Code Point) for data packets. Valid Values: 0 to 63 Default: 63 Note: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

Adjusting MTU of Data Packets

Data 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 data 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.

Procedure

1. Do one of the following during a call:
 - On your web user interface, go to **Network->Advanced->MTU->Network MTU(1000-1500)**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Advanced->Advanced Network->Network MTU(1000-1500)**.
 - For VC200: on your remote control, go to **More->Network->Wired Network->Advanced Network->Network MTU(1000-1500)**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Network MTU(1000-1500)	<p>Specifies the maximum MTU size (in bytes) of data packets sent by the system.</p> <p>Valid Values: Integer from 1000 to 1500</p> <p>Default: 1500</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Restricted Single Packet Mode	<p>Enables or disables the restricted single packet mode.</p> <ul style="list-style-type: none"> • Disabled—sends data packets using multiple packets mode. • Enabled—sends data packets using single packet mode. <p>Default: Disabled</p> <p>Note: Some devices of other vendors only accept the data packets sent by single packet mode. If local system sends data packets using multiple packets mode, the video call may appear the mosaic phenomenon. To avoid this situation, enable this configuration.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	<p>Web User Interface</p>

Configuring Account Settings

This chapter provides information on how to configure account settings.

Configuring SIP Settings

Yealink video conferencing system supports Session Initiation Protocol (SIP). If your server supports SIP, you can use SIP to establish calls.

Registering a SIP Account

You can register a SIP account for making calls.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->SIP Account**.
 - On your remote control, go to **More->Setting->Advanced->SIP Account**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Account Active/SIP Account	Enables or disables the SIP account. Default: Enabled	Web User Interface Remote Control
User Name	Specifies the user name to use for authentication when registering with a SIP server. Default: Blank	Web User Interface Remote Control
Register Name	Configures the user name of the SIP account for register authentication. Default: Blank	Web User Interface Remote Control
Password	Specifies the password associated with the user name used to authenticate the system to the SIP server. Default: Blank	Web User Interface Remote Control
Server Host/Server	Configures the IP address or domain name of the SIP server for the SIP account. Default: Blank	Web User Interface Remote Control
Port/SIP Server Port	Configures the port of the SIP server. Valid values: Integer from 0 to 65535. Default: 5060	Web User Interface Remote Control
Enable Outbound Proxy Server/Outbound	Enables or disables the system to send requests of the SIP account to the outbound proxy server.	Web User Interface Remote Control

Parameter	Description	Configuration Method
	Default: Disabled	
Outbound Server/ Outbound	Configures the IP address or domain name of the outbound proxy server for the SIP account. Note: it is configurable only when the Outbound Proxy Server is enabled.	Web User Interface Remote Control
Port/ Outbound Port	Configures the port of the outbound proxy server. Valid values: Integer from 0 to 65535. Default: 5060	Web User Interface Remote Control
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. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: UDP Note: TLS is available only when the system is registered with a SIP server that supports TLS.	Web User Interface Remote Control
Server Expires	Configures the registration expiration time (in seconds) of the SIP server. Default: 3600	Web User Interface Remote Control
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. Default: 30	Web User Interface
Rport	Enables or disables the Rport feature. When the VCS locates behind a NAT	Web User Interface

Parameter	Description	Configuration Method
	<p>device, you can enable Rport to solve the port traversal with the SIP sever.</p> <p>Note: Rport feature depends on support from a SIP server.</p> <p>For more information, refer to RFC 3581.</p> <p>Default: Disabled</p>	

Configuring SIP IP Call

IP call means you dial the IP address of the far site instead of the account. you can use SIP protocol to establish IP calls.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->SIP IP Call**.
 - On your remote control, go to **More->Setting->Advanced->SIP IP Call**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
SIP IP Call	<p>Enables or disables the SIP IP Call.</p> <p>Default: Enabled.</p> <p>Note: When it is set to Enabled on both sites, the system can call the far site by dialing an IP address directly.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Transport	<p>Configures the type of transport protocol for the SIP IP call.</p> <ul style="list-style-type: none"> UDP—provides best-effort transport via UDP for SIP signaling. TCP—provides reliable transport via TCP for SIP signaling. DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. <p>Default: TCP</p>	<p>Web User Interface</p> <p>Remote Control</p>
Rport	<p>Enables or disables the Rport feature.</p> <p>When the VCS locates behind a NAT device, you can enable Rport to solve the port traversal with the SIP sever.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
	<p>Note: Rport feature depends on support from a SIP server.</p> <p>For more information, refer to RFC 3581.</p> <p>Default: Disabled</p>	

Configuring H.323 Settings

Your system supports H.323 protocol. Others can dial the IP address of your system directly using 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 dial your H.323 name or extension instead of the IP address.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->H.323**.
 - On your remote control, go to **More->Setting->Advanced->H.323**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
H.323 Protocol	<p>Enables or disables the H.323 protocol.</p> <p>Default: Enabled.</p> <p>Note: Only when it is set to Enabled, can H.323 account be registered. When it is set to Enabled on both sites, the system can call the far site by dialing an IP address directly.</p>	<p>Web User Interface</p> <p>Remote Control</p>
H.323 Account	<p>Enables or disables the H.323 account.</p> <p>Default: Enabled</p> <p>If it is set to disabled, the system cannot place or receive calls using the H.323 protocol.</p>	<p>Web User Interface</p> <p>Remote Control</p>
H.323 Name	<p>Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper.</p> <p>Default: blank</p>	<p>Web User Interface</p> <p>Remote Control</p>
H.323 Extension	<p>Specifies the extension that gatekeepers and gateways use to identify this system.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
	<p>Default: blank</p> <p>Note: Users can place point-to-point calls using the extension if both systems are registered with a gatekeeper.</p>	
<p>Gatekeeper Mode/ Gatekeeper Type</p>	<p>Configures the gatekeeper 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>	<p>Web User Interface Remote Control</p>
<p>Gatekeeper IP Address 1/ Gatekeeper Server1</p>	<p>Configures the IP address of the primary gatekeeper.</p>	<p>Web User Interface Remote Control</p>
<p>Port/ Gatekeeper Port 1</p>	<p>Configures the port of the primary gatekeeper.</p> <p>Valid values: Integer from 0 to 65535.</p> <p>Default: 1719</p>	<p>Web User Interface Remote Control</p>
<p>Gatekeeper IP Address 2/ Gatekeeper Server2</p>	<p>Configures the IP address of the secondary gatekeeper.</p> <p>Note: If communication with the primary gatekeeper is lost, the system registers with the alternate gatekeeper.</p>	<p>Web User Interface Remote Control</p>
<p>Port/ Gatekeeper Port 2</p>	<p>Configures the port of the secondary gatekeeper.</p> <p>Valid values: Integer from 0 to 65535.</p> <p>Default: 1719</p>	<p>Web User Interface Remote Control</p>
<p>Gatekeeper Authentication/ Gatekeeper Verify</p>	<p>Enables or disables support for gatekeeper authentication.</p> <p>Default: Disabled</p> <p>Note: When Gatekeeper Authentication is enabled, the gatekeeper ensures that only trusted H.323 systems are allowed to access the gatekeeper.</p>	<p>Web User Interface Remote Control</p>
<p>Gatekeeper Username</p>	<p>Specifies the user name for authentication with gatekeeper.</p> <p>Default: blank</p>	<p>Web User Interface Remote Control</p>

Parameter	Description	Configuration Method
Gatekeeper Password	Specifies the password for authentication with gatekeeper. Default: blank	Web User Interface Remote Control
Protocol Monitor Port	Specifies the port for the H.323 call setup. If the ISP limits the 1720 port, you should modify the port, and dial the far site using h323:ip:port format. Default: 1720 Note: It is only applicable to IP call for H.323.	Web User Interface
Local Early Media	Enables or disables local early media feature on the system. <ul style="list-style-type: none"> • Disabled—the local system sends an Open Logical Channel (OLC) message and receives an acknowledgement message from the far site. After receiving the acknowledgement message, the system may then transmit RTP streams to the far site. • Enabled—the system sends an Open Logical Channel (OLC) message to the far site and then transmits RTP streams to the far site directly before receiving the acknowledgement message of OLC. For some gatekeepers, you need to enable this feature to avoid black screen during a call. Default: Disabled.	Web User Interface

H.323 Tunneling

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

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->StarLeaf.**
 - On your web user interface, go to **Account->H.323.**
 - On your remote control, go to **More->Setting->Advanced->H.323.**
2. Configure and save the following setting:

Parameter	Description	Configuration Method
H.323 Tunneling	Enables or disables the system to send all signaling and media through the HTTP tunnel. Default: Disabled	Web User Interface

Configuring PSTN

PSTN box CPN10 is used to connect video conferencing system to the PSTN (Public Switched Telephone Network). It is a cost-effective solution for PSTN office. Up to 2 cascaded PSTN Boxes can be installed to video conferencing systems, which allow you to experience the conference conveniently in excellent speech quality with PSTN. For more information, refer to [Yealink PSTN Box CPN10 Quick Start Guide](#).

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->PSTN Account.**
 - On your remote control, go to **More->Setting->Advanced->PSTN Account.**
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Account Active/PSTN Account	Enables or disables the H.323 protocol. Default: Enabled. Note: Only when it is set to Enabled, can H.323 account be registered. When it is set to Enabled on both sites, the system can call the far site by dialing an IP address directly.	Web User Interface Remote Control
Label/PSTN Account Label	Enables or disables the H.323 account. Default: Enabled If it is set to disabled, the system cannot place or receive calls using the H.323 protocol.	Web User Interface Remote Control

Configuring Video Conference Platform

You can log into the following video conference platform:

- Yealink VC Cloud Management Service
- Yealink Meeting Server
- StarLeaf
- Zoom
- BlueJeans
- Pexip
- Custom

Yealink VC Cloud Management Service

The Yealink VC Cloud Management Service is a value-added cloud-based service platform for Cloud systems. It offers significant convenience and cost-savings to integrators and business customers in terms of deployment, configuration and usage.

The cloud enterprise administrator uses the Yealink VC Cloud management service to assign each user an individual Yealink Cloud account. For more information, refer to [Yealink VC Cloud Management Service Administrator Guide](#).

When you log into the Yealink Meeting Server, you can:

- Dial other Yealink Cloud accounts to establish a conversation.
- View and join scheduled conferences.
- Initiate and join meet now conferences.
- Join the permanent VMR.
- Manage Yealink Cloud video conferences.

For detailed introduction, refer to [Yealink Full HD Video Conferencing System User Guide](#).

Registering a Yealink Cloud Account

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Note: If it is disabled, you cannot register a Yealink Cloud account.	Web User Interface Remote Control
Platform Type	Select Yealink VC Cloud Management Service.	Web User Interface Remote Control

Parameter	Description	Configuration Method
Login Type	<p>Specifies the method for logging into the Yealink VC Cloud Management Service platform.</p> <ul style="list-style-type: none"> • PIN Code Login: This method uses the user's PIN code to log into the Yealink VC Cloud Management Service platform. The PIN code consists of 9 digits. You can only use the PIN code once and it will expire if unused for 7 days. Contact Cloud administrator when it expires. • user/password: This method uses the user's Yealink Cloud number and password to log into the Yealink VC Cloud Management Service platform. <p>Default: PIN Code Login</p>	<p>Web User Interface Remote Control</p>
Pincode/Pin Code	<p>Specifies the PIN code for logging into the Yealink VC Cloud Management Service platform.</p> <p>Default: Blank</p> <p>Note: It only works if the value of Login Type is set to PIN Code Login.</p>	<p>Web User Interface Remote Control</p>
Username	<p>Specifies the user name to log into the Yealink VC Cloud Management Service platform.</p> <p>Default: Blank</p> <p>Note: It only works if the value of Login Type is set to user/password.</p>	<p>Web User Interface Remote Control</p>
Password	<p>Specifies the password associated with the user name when signing into the Yealink VC Cloud Management Service platform.</p> <p>Default: Blank</p> <p>Note: It only works if the value of Login Type is set to user/password.</p>	<p>Web User Interface Remote Control</p>
Server	<p>Configures the IP address or domain name of the Yealink VC Cloud Management Service platform.</p> <p>Default: yealinkvc.com</p>	<p>Web User Interface Remote Control</p>

Parameter	Description	Configuration Method
Remember Me	<p>Enables or disables the system to remember the registration information.</p> <p>Default: ON</p> <p>Note: If it is on, user name and password will be filled automatically next time.</p> <p>It only works if the value of Login Type is set to Username/Password.</p>	Remote Control

Note

A Yealink Cloud account can be used to log into five Cloud systems at most simultaneously.

Yealink Meeting Server

The enterprise administrator uses the Yealink Meeting Server (YMS) to assign each user an individual YMS account. For more information on how to add YMS accounts, refer to [Yealink Meeting Server Administrator Guide](#).

When you log into the Yealink Meeting Server, you can:

- Dial other YMS accounts to establish a conversation.
- View and join scheduled conferences.
- Initiate and join meet now conferences.
- Join the permanent VMR.
- Manage YMS video conferences.

For detailed introduction, refer to [Yealink Full HD Video Conferencing System User Guide](#).

Registering a YMS Account

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	<p>Enables the Cloud feature.</p> <p>Default: Enabled</p> <p>Note: If it is disabled, the system cannot register the YMS account.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
Platform Type	Select Yealink Meeting Server.	Web User Interface Remote Control
ID	Specifies the ID when registering a YMS account. Default: Blank	Web User Interface Remote Control
Password	Specifies the password associated with the ID when registering a YMS account. Default: Blank	Web User Interface Remote Control
Server Host	Configures the IP address or domain name of the Yealink Meeting Server. Default: Blank	Web User Interface Remote Control
Port	Configures the port of the Yealink Meeting Server. Default: 0	Web User Interface Remote Control
Outbound Proxy Server/ Outbound Server	Configures the IP address or domain name of the outbound proxy server. Default: Blank	Web User Interface Remote Control
Remember Password	Enables or disables the system to remember the registration information. Default: ON Note: If it is on, other registration information will be filled automatically when you enter the ID next time.	Remote Control

Note

A YMS account can be used to log into five devices at most simultaneously.

If enterprise administrator enables the **Device upgrade** feature on Yealink Meeting Server, video conferencing systems that log into the Yealink Meeting Server will upgrade firmware automatically once the current firmware version is different from the one on Yealink Meeting Server.

StarLeaf Cloud Platform

You can log into the StarLeaf Cloud platform.

When you place a call using the StarLeaf Cloud account, you can:

- Call the other StarLeaf Cloud account to establish a point to point call.

- Call the Meeting ID to join the Virtual Meeting Rooms.
- Call between StarLeaf Cloud account and Microsoft Skype for Business/Lync account.

Logging into the StarLeaf Cloud Platform

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Default: Enabled Note: If it is disabled, the system cannot log into the StarLeaf Cloud platform.	Web User Interface Remote Control
Platform Type	Select StarLeaf.	Web User Interface Remote Control
QCP Code	Specifies the quick access code to log into the StarLeaf Cloud platform. Default: Blank	Web User Interface Remote Control

Note

System that logs into the StarLeaf Cloud platform will upgrade firmware automatically once the current firmware version is different from the one on StarLeaf Server.

Logging into the Zoom Cloud Platform

You can log into the Zoom Cloud platform and join the virtual meeting room.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Default: Enabled	Web User Interface Remote Control

Parameter	Description	Configuration Method
	Note: If it is disabled, the system cannot log into the Zoom Cloud platform.	
Platform Type	Select Zoom.	Web User Interface Remote Control
Server/ Host Server	Configures the IP address or domain name of the Zoom Cloud server. Default: zoomcrc.com	Web User Interface Remote Control
Transport	Configures the type of transport protocol for the Zoom Cloud platform. <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. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. Default: 3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. Default: 30	Web User Interface

Registering a Pexip Account

You can register the Pexip account.

When you place a call using the Pexip account, you can:

- Call the device alias to establish a point to point call.
- Call the aliases to join the Virtual Meeting Rooms, Virtual Auditoriums or Virtual Receptions.
- Call between Pexip account and Microsoft Skype for Business/Lync account.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Note: If it is disabled, you cannot register a Pexip account.	Remote Control Web User Interface
Platform Type	Select Pexip.	Remote Control Web User Interface
Alias	Specifies the alias when registering a Pexip account. Default: Blank	Remote Control Web User Interface
Username	Specifies the user name when registering a Pexip account. Default: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the user name when registering a Pexip account. Default: Blank	Web User Interface Remote Control
Server/ Host Server	Configures the IP address or domain name of the Pexip server. Default: Blank	Web User Interface Remote Control
Port	Configures the port of the Pexip server. Default: 0	Web User Interface
Transport	Configures the type of transport protocol for the Pexip platform. <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. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: TCP	Web User Interface

Parameter	Description	Configuration Method
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. Default: 3600	Web User Interface
Remember Password	Enables or disables the system to remember the registration information. Default: ON Note: If it is on, other registration information will be filled automatically when you enter the alias next time.	Remote Control
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. Default: 30	Web User Interface

Note

You can also register the Pexip account using SIP or H.323 protocol. For more information, refer to [Configuring SIP Settings](#) and [Configuring H.323 Settings](#).

Logging into the BlueJeans Cloud Platform

You can log into the BlueJeans Cloud platform and join the virtual meeting room.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->BlueJeans**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform->Platform Type->BlueJeans**.
 - Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Default: Enabled Note: If it is disabled, the system cannot log into the BlueJeans Cloud platform.	Web User Interface Remote Control
Platform Type	Select BlueJeans.	Web User Interface Remote Control

Parameter	Description	Configuration Method
Server Host/ Server	Configures the IP address or domain name of the BlueJeans server. Default: bjn.vc	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the BlueJeans Cloud platform. <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. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. Default: 3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. Default: 30	Web User Interface

Registering a Custom Account

You can register a custom account.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. Note: If it is disabled, you cannot register a custom account.	Web User Interface Remote Control

Parameter	Description	Configuration Method
Platform Type	Select Custom.	Web User Interface Remote Control
Label	Configures the account label displayed on the monitor when registering a custom account. Default: Blank	Web User Interface Remote Control
Username	Specifies the user name when registering a custom account. Default: Blank	Web User Interface Remote Control
Register Name	Configures the register name when registering a custom account. Default: Blank	Web User Interface Remote Control
Password	Specifies the password associated with the user name when registering a custom account. Default: Blank	Web User Interface Remote Control
Server Host/ Server	Configures the IP address or domain name of the custom server. Default: Blank	Web User Interface Remote Control
Port	Configures the port of the custom server. Default: 0	Web User Interface
Transport	Configures the type of transport protocol for the custom platform. <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. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. Default: TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the custom server. Default: 3600	Web User Interface

Parameter	Description	Configuration Method
Remember password	Enables or disables the system to remember the registration information. Default: ON Note: If it is on, other registration information will be filled automatically when you enter the user name next time.	Remote Control
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. Default: 30	Web User Interface

Logging out of the Video Conference Platform

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Advanced Setting->Log Out**.
 - On your remote control, go to **More->Setting->Advanced->Video Conference Platform->Log Out**.

Configuring the Third-party Virtual Meeting Room

A Virtual Meeting Room (VMR) is an online space, typically hosted by a Cloud-service provider, where multiple participants can join. Participants usually join by dialing a specific number or an address with a simple name like zoomcrc.com.

If you do not register a Cloud account, or you only register a Yealink Cloud account or YMS account, you can configure a third-party VMR (StarLeaf/Zoom/BlueJeans/Pexip) in advance, so that you can quickly join a VMR without registering a third-party Cloud account. Up to 5 third-party VMRs can be configured.

Procedure

- On your web user interface, go to **Setting->3rd-Party VMR**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
VMR Name 1	Configures the virtual meeting room name. Default: Zoom Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface

Parameter	Description	Configuration Method
VMR Server1	Configures the virtual meeting room server address. Default: zoomcrc.com Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 2	Configures the virtual meeting room name. Default: Blue Jeans Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 2	Configures the virtual meeting room server address. Default: bjn.vc Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 3 to 5	Configures the virtual meeting room name. Default: Blank Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 3 to 5	Configures the virtual meeting room server address. Default: Blank Note: It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface

Dialing screen of your web user interface and monitor will appear the configured VMR.

You can select the desired VMR from the pull-down list, and then enter conference ID to call the corresponding VMR.

Configuring General Settings

Setting the Site Name

You can set the site name.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->General->General Information->Site Name**
 - On your remote control, go to **More->Setting->Basic->Site Name**.
- Configure and save the following setting:

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

Setting the Language

You can specify a language to display in the monitor and web user interface respectively. The CP960 conference phone will detect and use the same language as the monitor.

Procedure

- Do one of the following:
 - On your web user interface, click **Language** at the top of the web page.
 - On your remote control, go to **More->Setting->Basic->Language**.
- Select the desired language.

Setting Time and Date

Your system can obtain the time and date from SNTP (Simple Network Time Protocol) time server automatically, or you can set the time and date manually.

Time Zone

The following table lists the available time zone on video conferencing system.

Time	Time Zone Name	Time	Time Zone Name
-11:00	Samoa	+01:00	Poland (Warsaw)
-10:00	United States-Hawaii-Aleutian	+02:00	Estonia(Tallinn)

Time	Time Zone Name	Time	Time Zone Name
-10:00	United States-Alaska-Aleutian	+02:00	Finland(Helsinki)
-09:30	French Polynesia	+02:00	Gaza Strip(Gaza)
-09:00	United States-Alaska Time	+02:00	Greece(Athens)
-08:00	Canada(Vancouver, Whitehorse)	+02:00	Israel(Tel Aviv)
-08:00	Mexico(Tijuana, Mexicali)	+02:00	Jordan(Amman)
-08:00	United States-Pacific Time	+02:00	Latvia(Riga)
-07:00	Canada(Edmonton, Calgary)	+02:00	Lebanon(Beirut)
-07:00	Mexico(Mazatlan, Chihuahua)	+02:00	Moldova(Kishinev)
-07:00	United States-Mountain Time	+02:00	Russia(Kaliningrad)
-07:00	United States-MST no DST	+02:00	Romania(Bucharest)
-06:00	Canada-Manitoba(Winnipeg)	+02:00	Syria(Damascus)
-06:00	Chile(Easter Islands)	+02:00	Turkey(Ankara)
-06:00	Mexico(Mexico City, Acapulco)	+02:00	Ukraine(Kyiv, Odessa)
-06:00	United States-Central Time	+03:00	East Africa Time
-05:00	Bahamas(Nassau)	+03:00	Iraq(Baghdad)
-05:00	Canada(Montreal, Ottawa, Quebec)	+03:00	Russia(Moscow)
-05:00	Cuba(Havana)	+03:30	Iran(Teheran)
-05:00	United States-Eastern Time	+04:00	Armenia(Yerevan)
-04:30	Venezuela(Caracas)	+04:00	Azerbaijan(Baku)
-04:00	Canada(Halifax, Saint John)	+04:00	Georgia(Tbilisi)
-04:00	Chile(Santiago)	+04:00	Kazakhstan(Aktau)
-04:00	Paraguay(Asuncion)	+04:00	Russia(Samara)
-04:00	United Kingdom-Bermuda(Bermuda)	+04:30	Afghanistan(Kabul)
-04:00	United Kingdom(Falkland Islands)	+05:00	Kazakhstan(Aqtobe)
-04:00	Trinidad&Tobago	+05:00	Kyrgyzstan(Bishkek)
-03:30	Canada-New Foundland(St.Johns)	+05:00	Pakistan(Islamabad)
-03:00	Denmark-Greenland(Nuuk)	+05:00	Russia(Chelyabinsk)
-03:00	Argentina(Buenos Aires)	+05:30	India(Calcutta)
-03:00	Brazil(no DST)	+05:45	Nepal(Katmandu)

Time	Time Zone Name	Time	Time Zone Name
-03:00	Brazil(DST)	+06:00	Kazakhstan(Astana, Almaty)
-02:30	Newfoundland and Labrador	+06:00	Russia(Novosibirsk, Omsk)
-02:00	Brazil(no DST)	+06:30	Myanmar(Naypyitaw)
-01:00	Portugal(Azores)	+07:00	Russia(Krasnoyarsk)
0	GMT	+07:00	Thailand(Bangkok)
0	Greenland	+08:00	China(Beijing)
0	Denmark-Faroe Islands(Torshavn)	+08:00	Singapore(Singapore)
0	Ireland(Dublin)	+08:00	Australia(Perth)
0	Portugal(Lisboa, Porto, Funchal)	+08:00	Russia(Irkutsk, Ulan-Ude)
0	Spain-Canary Islands(Las Palmas)	+08:45	Eucla
0	United Kingdom(London)	+09:00	Korea(Seoul)
0	Morocco	+09:00	Japan(Tokyo)
+01:00	Albania(Tirane)	+09:00	Russia(Yakutsk, Chita)
+01:00	Austria(Vienna)	+09:30	Australia(Adelaide)
+01:00	Belgium(Brussels)	+09:30	Australia(Darwin)
+01:00	Caicos	+10:00	Australia(Sydney, Melbourne, Canberra)
+01:00	Chad	+10:00	Australia(Brisbane)
+01:00	Spain(Madrid)	+10:00	Australia(Hobart)
+01:00	Croatia(Zagreb)	+10:00	Russia(Vladivostok)
+01:00	Czech Republic(Prague)	+10:30	Australia(Lord Howe Islands)
+01:00	Denmark(Kopenhagen)	+11:00	New Caledonia(Noumea)
+01:00	France(Paris)	+11:00	Russia(Srednekolymsk Time)
+01:00	Germany(Berlin)	+11:30	Norfolk Island
+01:00	Hungary(Budapest)	+12:00	New Zealand(Wellington, Auckland)
+01:00	Italy(Rome)	+12:00	Russia(Kamchatka Time)
+01:00	Luxembourg(Luxembourg)	+12:45	New Zealand(Chatham Islands)
+01:00	Macedonia(Skopje)	+13:00	Tonga(Nukualofa)
+01:00	Netherlands(Amsterdam)	+13:30	Chatham Islands
+01:00	Namibia(Windhoek)	+14:00	Kiribati

NTP Settings

You can set a NTP time server for the desired area as required. The NTP time server address can be offered by the DHCP server or configured manually.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Date& Time**.
 - On your remote control, go to **More->Setting->Basic->Date & Time**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Time Type	Select SNTP to obtain the time and date from the NTP server automatically.	Web User Interface Remote Control
DHCP Time	Enables or disables the system to update time with the offset time offered by 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) For more information on available time zone, refer to Time Zone on page 93.	Web User Interface Remote Control
NTP Primary Server/ Primary Server	Specifies the address of the primary time server to use when Time Type is set to Manual Time . Default: cn.pool.ntp.org	Web User Interface Remote Control
NTP Secondary Server/ Secondary Server	Specifies the address of the secondary time server to use when Time Type is set to Manual Time . Default: cn.pool.ntp.org	Web User Interface Remote Control
Synchronism (15~86400s)	Configures the interval (in seconds) to update time and date from the NTP server. Default: 1000.	Web User Interface

DST Settings

You can set DST for the desired area as required. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Date & Time**.
 - On your remote control, go to **More->Setting->Basic->Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
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. <ul style="list-style-type: none"> • Automatic-use DST. DST will be configured automatically. Default: Automatic	Web User Interface Remote Control
Fixed Type	Configures the DST calculation methods. <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. Note: It only works if the value of Daylight Saving Time is set to Enabled.	Web User Interface
Start Date	When the DST calculation method is set to By Date . Configures the time to start DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
End Date	When the DST calculation method is set to By Date . Configures the time to end DST. Note: It only works if the value of the	Web User Interface

Parameter	Description	Configuration Method
	Daylight Saving Time is set to Enabled.	
DST Start Month	When the DST calculation method is set to By Week . Configures the time to start DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Start Day of Week		
DST Start Day of Week Last in Month		
Start Hour of Day		
DST Stop Month	When the DST calculation method is set to By Week , Configures the time to end DST. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Stop Day of Week		
DST Stop Day of Week Last in Month		
End Hour of Day		
Offset(minutes)	Configures the DST offset time (in minutes). Valid values: -300 to +300. Note: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface

Configuring Time and Date Manually

You can set the time and date manually when the system cannot obtain the time and date from the NTP time server.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Date & Time**, and Select **Manual Time** from the pull-down list of **Time Type**.
 - On your remote control, go to **More->Setting->Basic->Date & Time**, and Select **Manual Settings** from the pull-down list of **Time Type**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Time Type	Select Manual Time to configure the time and date manually.	Web User Interface Remote Control

3. Configure the time and date manually:

Configuring Time and Date Format


You can customize the time and date by choosing between a variety of time and date formats.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Date & Time**.
 - On your remote control, go to **More->Setting->Basic->Date & Time**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Time Format	Configures the time format. <ul style="list-style-type: none"> Hour12 Hour24 Default: Hour 24	Web User Interface Remote Control
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 DD MMM YYYY WWW DD MMM Default: YYYY-MM-DD Note: "WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.	Web User Interface Remote Control

Customizing Key Type

You can configure a custom type for the custom key () on the remote control.

Procedure

1. On your web user interface, go to **Setting->Remote Control->Custom Key Type**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Custom Key Type	<p>Specify a feature to the custom key on the remote control.</p> <ul style="list-style-type: none"> • Input: press to select the video input source • Screenshot: press to capture screen. • Mute Speaker: press to mute or unmute the speaker. • Presentation: press to start or stop presentation. <p>Default: Presentation</p>	Web User Interface

Allowing Website Snapshot

You can choose whether to allow the web to show the same content that displayed on your monitor. If you want to prevent content on your monitor from being viewed remotely, you can disable this feature.

Procedure

1. On your remote control, navigate to **More->Setting->Basic**.
2. Select the **Website Snapshot** checkbox.

Adjusting Backlight of the CP960 Conference Phone

You can change the backlight brightness of the CP960 conference phone. Backlight time specifies the delay time to turn off the backlight when the phone has been idle for a specified time.

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

- **Always On:** Backlight is turned on permanently.
- **Specific time:** Backlight is turned off when the phone has been idle for a specified time.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->General->General Information->Backlight Time**.
 - On your CP960 conference phone, go to **Settings->Display->Backlight**.
 - On your CP960 conference phone, swipe down from the top of the screen to enter the control center, and drag the backlight slider.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active Level	Configures the brightness of the CP960 conference phone.	CP960 conference phone
Backlight Time	Configures the backlight time of the CP960 conference phone. Default: Always On	Web User Interface CP960 conference phone

Customizing the Local Interface

You can configure the time before the system starts screen saver, and customize the screen to show or hide some information.

Screen Saver

The screen saver automatically starts when the system or CP960 conference phone has been idle for the preset waiting time. You can set screen saver for the monitor and CP960 conference phone respectively.

The screen saver stops when:

- Press any key.
- There is an incoming call.
- A new prompt (for example, USB device available now).

Setting Screen Saver for Monitor

You can configure the waiting time before the monitor starts the screen saver.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->General->General Information->Screen Saver Wait Time**.
 - On your remote control, go to **More->Setting->Basic->Screensaver**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Screen Saver Wait Time	Configures the inactive time (in minutes) before the system starts screen saver. Default: 1 Min	Web User Interface Remote Control

Four pictures are displayed like a slide show when screen saver starts.

Setting Screen Saver for CP960 Conference Phone

The CP960 conference phone supports four types of screen savers: Clock, Colors, Photo Frame and Photo Table. You can choose anyone you like. And you can configure the waiting time before the CP960 conference phone starts the screen saver.

Procedure

1. On your CP960 conference phone, go to **Settings->Display->Screen Saver**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Wait Time	Configures the inactive time (in minutes) before the CP960 conference phone starts screen saver. Default: 10min	CP960 Conference Phone

3. Tap the desired screen saver.

Showing or Hiding IP Address

You can choose to hide IP address on the status bar of your monitor.

Procedure

1. On your web user interface, go to **Setting->General->General Information->Hide IP Address**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Hide IP address	Enables or disables the monitor to hide IP address on the status bar. Default: Disabled	Web User Interface

Showing or Hiding Heading Time

You can choose to hide time and date on the status bar of your monitor.

Procedure

1. On your web user interface, go to **Setting->General->General Information->Hide Heading Time**.
2. Configure and save the following setting:


Parameter	Description	Configuration Method
Hide Heading Time	Enables or disables the monitor to hide time and date on the status bar. Default: Disabled	Web User Interface




Showing or Hiding Icons in a Call




During a call, the system will show some information and icons (such as call time, mute icon and recording icon) by default, so that you can know the call status from these icons. You can also hide these icons as needed to achieve the best video effects.

Procedure

1. On your web user interface, go to **Setting->General->Hide Icon in Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Time Icon	Enables or disables the system to hide call time during a call. <ul style="list-style-type: none"> • Disabled- the system does not display call time during a call. • Hide with UI- the system displays call time during a call, but the call time will disappear when the status bar hides automatically. • Enabled- the system displays call time during a call. Default: Hide with UI	Web User Interface
Mute Icon	Enables or disables the system to hide mute icon () during a call. <ul style="list-style-type: none"> • Disabled- the system does not display mute icon during a call. • Hide with UI- the system displays mute icon during a call, but the mute icon will disappear when the status bar hides automatically. • Enabled- the system displays mute icon during a call. Default: Disabled	Web User Interface
Camera Icon	Enables or disables the system to hide camera icon	Web User Interface

Parameter	Description	Configuration Method
	<p>() during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display camera icon during a call. • Hide with UI- the system displays camera icon during a call, but the camera icon will disappear when the status bar hides automatically. • Enabled- the system displays camera icon during a call. <p>Default: Disabled</p>	
Recording Icon	<p>Enables or disables the system to hide recording icon () during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display recording icon during a call. • Hide with UI- the system displays recording icon will disappear when the status bar hides automatically. • Enabled- the system displays recording icon during a call. <p>Default: Disabled</p>	Web User Interface
Sitename Icon	<p>Enables or disables the system to hide site name icon during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display site name icon during a call. • Hide with UI- the system displays site name icon during a call, but the site name will disappear when the status bar hides automatically. • Enabled- the system displays site name icon during a call. <p>Default: Disabled</p>	Web User Interface
Hold Icon	<p>Enables or disables the system to hide hold icon () during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display hold icon during a call. • Hide with UI- the system displays hold icon during a call, but the hold icon will disappear when the status bar hides automatically. • Enabled- the system displays hold icon during a call. <p>Default: Disabled</p>	Web User Interface





Parameter	Description	Configuration Method
Encrypt Icon	<p>Enables or disables the system to hide encrypt icon () during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display encrypt icon during a call. • Hide with UI- the system displays encrypt icon during a call, but the encrypt icon will disappear when the status bar hides automatically. • Enabled- the system displays encrypt icon during a call. <p>Default: Disabled</p>	Web User Interface
OutPut Mute Icon	<p>Enables or disables the system to hide output mute icon (output volume is set to 0: ) during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display output mute icon during a call. • Hide with UI- the system displays output mute icon during a call, but the output mute icon will disappear when the status bar hides automatically. • Enabled- the system displays output mute icon during a call. <p>Default: Disabled</p>	Web User Interface
SecondScreen Icon	<p>Enables or disables the system to hide second screen icon () during a call.</p> <ul style="list-style-type: none"> • Disabled- the system does not display second screen icon during a call. • Hide with UI- the system displays second screen icon during a call, but the second screen icon will disappear when the status bar hides automatically. • Enabled- the system displays second screen icon during a call. <p>Default: Disabled</p>	Web User Interface

Configuring Keyboard Input Method

You can enter characters using the enabled input method. On-screen keyboard on the monitor supports English and Russian input methods.

Procedure

1. On your web user interface, go to **Setting->General->General Information->Keyboard IME**.

2. Select the desired list from the **Disabled** column and click  .
The selected input method appears in the **Enabled** column.
3. Repeat step 2 to add more input methods to the **Enabled** column.
4. (Optional.) To remove a input method from the **Enabled** column, select the desired input method and then click  .
5. To adjust the display order of the enabled input methods, select the desired input method, and click  or  .

Configuring USB Storage

If you have high requirement for data security, you can disable the USB storage. So that you cannot use USB flash driver to store recorded videos, screenshots or captured packets.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->USB Enable**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
USB Enable	Enables or disables the USB feature. Default: Enabled Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

Configuring Local Storage

VC200 supports local storage in addition to USB storage.

Note:

The priority of local storage is lower than USB storage. When user disables USB storage, the captured screenshot and recorded files are saved on local storage automatically.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->Local Storage Enable**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Local Storage Enable	Enables or disables the local storage feature. Default: Enabled Note: If you change this parameter, the	Web User Interface

Parameter	Description	Configuration Method
	system will reboot to make the change take effect.	

Screenshot

You can capture screenshot.

Before You Begin

If you want to save screenshot to USB flash driver, make sure a USB flash drive is connected, and the USB feature is enabled.

If you want to save screenshot to local storage (only applicable to VC200), make sure local storage is enabled.

Configuring Screenshot



Procedure

1. On your web user interface, go to **Setting->Video & Audio->Screenshot**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Screenshot	<p>Enables or disables capture screenshot using the remote control.</p> <ul style="list-style-type: none"> • Enabled • Disabled- you cannot capture screenshot using your remote control. <p>Default: Enabled</p>	Web User Interface

Capturing Screenshot

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500: on your web user interface, go to **Home->Screenshot**.
 - For VC200: on your web user interface, go to **VC200->Screenshot**.
 - On your remote control, if  is set to Screenshot key, press  to capture screenshot.
 - On your CP960 conference, tap **More->Screenshot** during a call.

Related Topic:[Configuring USB Storage](#)[Configuring Local Storage](#)

Configuring Video Recording

Before You Begin

If you want to record video to USB flash driver, make sure a USB flash drive is connected, and the USB feature is enabled.

If you want to record video to local storage (only applicable to VC200), make sure local storage is enabled.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->USB Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Recording	<p>Enables or disables the video recording feature on the system.</p> <p>Default: Enabled</p> <p>If it is set to disabled, you cannot record video.</p>	Web User Interface
Auto Recording	<p>Enables or disables the system to start recording automatically once a call is established.</p> <p>Default: Disabled.</p> <p>Note: The auto recording feature is available only when the recording feature is enabled.</p>	Web User Interface
Dual Screen Recording Setting	<p>Select the desired screen. You can record the video on the selected screen when you are using dual screen.</p> <ul style="list-style-type: none"> • Screen 1+2: record video on dual screen • Screen 1 Only • Screen 2 Only <p>Default: Screen 1+2</p> <p>Note: This is not applicable to VC200.</p>	Web User Interface

Related Topic:[Configuring USB Storage](#)[Configuring Local Storage](#)

Configuring Audio Settings

Audio Output Settings

Available Audio Output

Model	Audio Output
VC880/VC800/VC200	<ul style="list-style-type: none"> • Auto- selects the audio output with the highest priority. If the audio output with the highest priority is removed, the system will select the next highest priority device. The priority is VCS Phone>HDMI>Line Output. • VCS Phone • HDMI • Line Output
VC500	<ul style="list-style-type: none"> • Auto- selects the audio output with the highest priority. The priority is VCS Phone>HDMI> USB Line out. • VCS Phone • HDMI • USB Line out

Specifying an Available Audio Output

You can specify an available audio output if you do not want to use the default audio output device.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Video & Audio->Audio Output**.
 - On your remote control, go to **More->Setting->Video & Audio->Audio Settings->Audio Output**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Video & Audio->Audio Settings->Audio Output**.
 - For VC200: on your remote control, go to **More->Setting->Video & Audio->Audio Output**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Audio Output	Specifies the audio output device for the system. Valid values: <ul style="list-style-type: none"> • Auto - selects the audio output 	Web User Interface Remote Control

Parameter	Description	Configuration Method
	<p>device with highest priority.</p> <ul style="list-style-type: none"> • VCS Phone - selects the CP960 conference phone. • HDMI - selects the built-in speakerphone of the monitor. • Line Output -Speakerphone connected to VC880/VC800/VC200 codec. • USB Line out - Speakerphone connected to the USB port on the VC500 codec using a USB to Line-out adapter. <p>Default: Auto.</p> <p>If VCS Phone is selected as the audio output device manually or automatically, the audio input device must be VCS Phone or VCS Phone+ Wireless Microphone.</p>	

The system will start EQ self-adaption to optimize the acoustic effect automatically when the audio output switches to **HDMI** or **Line Output/USB Line out**.

Related Topic:

[EQ Self Adaption](#)

EQ Self Adaption

The system supports EQ self adaption to optimize the acoustic effect.

For VC880/VC800/VC500: the EQ self-adaption starts when one of the following situations occurs:

- The audio output device manually or automatically switches to **HDMI** or **Line Output/USB Line out**.
- When the system is powered on, the system finds that the **HDMI** or **Line Output/USB Line out** is current audio output.
- The EQ self-adaption feature changes from disabled to enabled.

For VC200: the EQ self-adaption starts when one of the following situations occurs:

- First time you connect a display device to VC200.
- Reset the VC200.
- Click **EQ Self Adaption**.

Configuring EQ Self Adaption

Procedure

1. On your web user interface, go to **Setting->Video & Audio->Audio Settings**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
EQ Self Adaption	Enables or disables the EQ self adaption feature on the system. Default: Enabled	Web User Interface
Start EQ Self Adaption	Starts the EQ self adaption feature. Note: This configuration is only applicable to VC200 and appears only if EQ Self Adaption is set to On .	Web User Interface

Audio Input Settings

You can configure audio input settings for your system.

Available Audio Input

Model	Audio Output
VC880/VC800	<ul style="list-style-type: none"> • Auto—the system automatically selects the audio input with the highest priority. The audio input priority is shown as below: • VCS Phone • Bluetooth Micpod • Line Input
VC200	<ul style="list-style-type: none"> • Auto • VCS Phone • Built-in Micphone • Bluetooth Micpod • Line Input
VC500	<ul style="list-style-type: none"> • Auto • VCS Phone • Bluetooth Micpod • USB Line in

Specifying an Available Audio Input

You can specify an available audio input if you do not want to use the default audio input device.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Video & Audio->Audio Settings->Audio Input**.
 - For VC880/VC800/VC500: on your remote control, go to **More->Setting->Video & Audio->Audio Settings->Audio Input**.
 - For VC200: on your remote control, go to **More->Setting->Video & Audio->Audio Input**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio Input	<p>Specifies the audio input for the system.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • Auto- selects the audio input device with the highest priority. • VCS Phone- selects the CP960 conference phone. • VCS Phone + Wireless Microphone- selects the CP960 conference phone and CPW90 wireless expansion microphones • Built-in Micphone - selects the VC200 built-in microphone. • Bluetooth Micpod - selects the CPW90-BT Bluetooth wireless microphones. • Wireless Microphone - selects the CPW90 wireless microphones. • Line Input- audio input device connected to the Line In port on the VC800 codec • USB Line in - audio input device connected to the USB port on the VC500 codec using a USB to Line-in adapter <p>Default: Auto.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Line AEC	<p>Enables or disables echo cancellation for line input device.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • On- If you select an acoustic device (for example: a microphone) to be the line input, you can enable this 	<p>Web User Interface</p>

Parameter	Description	Configuration Method
	<p>configuration to eliminate echo.</p> <ul style="list-style-type: none"> • Off- If you select a non-acoustic device (for example: a mobile phone) to be the line input, you should disable this configuration. <p>Default: Off</p> <p>Note: This configuration appears only if Audio Input is set to Line Input/USB Line in.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	
Audio Line In	<p>Configures the volume of line input device.</p> <p>Valid Values: Integer from -50 to 50dB</p> <p>Default: 0</p> <p>Note:</p> <ul style="list-style-type: none"> • 0 means default volume. Positive number means increasing volume. Negative number means decreasing volume. • This configuration appears only if Audio Input is set to Line Input/USB Line in. • If you change this parameter, the system will reboot to make the change take effect. • This configuration is not applicable to VC200. 	Web User Interface

Note

If **VCS Phone** is selected as the audio output manually or automatically, the audio input must be **VCS Phone** or **VCS Phone+Wireless Microphone**.

Key Tone

You can enable the key tone feature to produce a sound when you press any key on the remote control or tap the onscreen dial pad on the CP960 conference phone.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->General->General Information->Key Tone**.
 - On your remote control, go to **More->Setting->Basic->Key Tone**.
2. Configure and save the following setting:

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

Tones

When receiving a message, 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.

Supported Tones

Available tone sets for the system:

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

Custom Tones Formats

You can customize tones beside the existed tones.

tone = element1[,element2] [,element3]...[,element8]

Where

- **element** = [!]**Freq1**[+**Freq2**][+**Freq3**][+**Freq4**] /**Duration**
- **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.
- **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.
- You can configure at most eight different tones for one condition, and separate them by commas. (for example: 250/200, 0/1000, 200+300/500, 600+700+800+1000/2000).
- An exclamation mark "!" before tones (for example: !250/200, 0/1000, 200+300/500, 600+700+800+1000/2000) means playing tones once.

Customizing Tones

Procedure

1. On your web user interface, go to **Setting->Tones**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Select Country	Select Custom.	Web User Interface
Ring Back	Customizes the ring-back tone for the system. Default: Blank Note: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Busy	Customizes the busy tone for the system. Default: Blank Note: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Call Waiting	Customizes the call waiting tone for the system. Default: Blank Note: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Auto Answer	Customizes the auto answer tone for the system. Default: Blank Note: It only works if the parameter "Select Country" is set to Custom.	Web User Interface

Codecs

CODEC is an abbreviation of COmpress-DECompress, and is capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio/video signal with a minimum number of bits while retaining quality. This can effectively reduce the frame size and the bandwidth required for audio/video transmission.

Audio Codecs

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

Supported Audio Codecs

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

Codec	Algorithm	Bit Rate	Sample Rate	Reference
ARES	ARES	8-64kpbs	48 Ksps	None
Opus	opus	8-12 Kbps	8 Ksps	RFC 6716
		16-20 Kbps	12 Ksps	
		28-40 Kbps	16 Ksps	
		48-64 Kbps	24 Ksps	
		64-128 Kbps	48 Ksps	
G.722.1c	G.722.1	48 Kbps	32 Ksps	RFC 5577
G.722.1c		32 Kbps	32 Ksps	RFC 5577
G.722.1c		24 Kbps	32 Ksps	RFC 5577
G.722.1		24 Kbps	16 or 32 Ksps	RFC 5577
G722	G.722	64 Kbps	16 Ksps	RFC 3551
PCMU	G.711 u-law	64 Kbps	8 Ksps	RFC 3551
PCMA	G.711 a-law	64 Kbps	8 Ksps	RFC 3551

The Opus codec supports various audio bandwidths, defined as follows:

Abbreviation	Audio Bandwidth	Sample Rate (Effective)
NB (narrowband)	4 kHz	8 kHz
MB (medium-band)	6 kHz	12 kHz
WB (wideband)	8 kHz	16 kHz
SWB (super-wideband)	12 kHz	24 kHz
FB (fullband)	20 kHz	48 kHz

Configuring Audio Codecs

Procedure

1. On your web user interface, go to **Account->Codec->Audio Codec**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the audio codecs to be used. Note: You can move disabled codec to	Web User Interface

Parameter	Description	Configuration Method
	this field.	
Disable Codecs	Specifies the audio codecs that are not used. Note: You can move enabled codec to this field.	Web User Interface
Opus Sample Rate	Configures the sample rate of the opus audio codec. <ul style="list-style-type: none"> Opus-FB(48KHZ) Opus-SWB(24KHZ) Opus-WB(16KHZ) Opus-MB(12KHZ) Opus-NB(8KHZ) Default: Opus-FB(48KHZ)	Web User Interface
Special audio codec byte sequence	Enables or disables the special audio codec byte sequence. Note: Different devices have different definition about how some codecs are stored (Big-endian or little-endian), which may lead to the audio incompatibility problems between Yealink and certain devices. You can enable the special audio codec byte sequence feature to solve these incompatibility problems.	Web User Interface

Video Codecs

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

Supported Video Codecs

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

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

Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H265	H265/90000			Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P

Note

If you are using H.265 video codec during a two-way video calls, the system will negotiate with the other party to use H264 High profile video codec automatically when placing a new call.

Configuring Video Codecs

Procedure

1. On your web user interface, go to **Account->Codec->Video Codec**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the enabled video codecs for the system to use. Note: You can move disabled codec to this field.	Web User Interface
Disable Codecs	Specifies the disabled video codecs for the system that are not used. Note: You can move enabled codec to this field.	Web User Interface

DTMF

DTMF is the signal sent from the system to the network, which is generated when pressing the keypad during a call. Each key pressed generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

DTMF Keypad

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

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Transmission Ways of DTMF Digits

Three ways to transmit DTMF digits during SIP calls:

- **RFC 2833** -- DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.
- **INBAND** -- DTMF digits are transmitted in the voice band. It uses the same codec as your voice and is audible to conversation partners.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages. DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

Configuring DTMF for SIP Protocol

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->Zoom/Pexip/BlueJeans/Custom**.
 - On your web user interface, go to **Account->SIP Account**.
 - On your web user interface, go to **Account->SIP IP Call**.
 - On your remote control, go to **More->Setting->Advanced->SIP IP Call**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
DTMF Type	<p>Configures the DTMF type.</p> <p>INBAND—DTMF digits are transmitted in the voice band.</p> <ul style="list-style-type: none"> • RFC2833—DTMF digits are transmitted by RTP Events compliant to RFC2833. • SIP INFO—DTMF digits are transmitted by the SIP INFO 	<p>Web User Interface</p> <p>Remote Control</p>

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

Configuring DTMF for H.323 Protocol

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->StarLeaf.**
 - On your web user interface, go to **Account->H.323.**
2. Configure and save the following setting:








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

Muting Microphone

You can mute the local microphone during a call, so that other parties cannot hear you.

Procedure

Do one of the following during a call:

- For VC880/VC800/VC500: on your web user interface, go to **Home->Mute**.
 - For V200: on your web user interface, go to **VC200->Mute**.
 - On your remote control, press  .
 - On your CP960 conference phone, tap  .
 - On your CP960 conference phone's touch screen, tap  .
 - On your CPW90 wireless microphones, tap  .
 - On your CPW90-BT Bluetooth wireless microphones, tap  .
 - On your CPE90 wired expansion microphones, tap  .
- If video conferencing system is muted, the  icon will appear on the local video.

Configuring Microphone Mute Mode

By default, mute a single microphone (CPE90/CPW90/CPW90-BT) will mute other microphones synchronously. To avoid picking up unwanted sounds from other microphones, you can choose to mute a single microphone only, and other microphones keep unmuted.

Procedure

1. On your web user interface, go to **Setting->Video & Audio**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Microphone Mute Mode	Configures the microphone mute mode. <ul style="list-style-type: none"> • Synchronized- mute/unmute a single microphone will mute/unmute other microphones synchronously. • Separated- mute/unmute a single microphone will not mute/unmute other microphones synchronously. Default: Synchronized	Web User Interface

Note:

If you use remote control or CP960 conference phone to mute or unmute a microphone, all microphone will be muted/unmuted synchronously.

Muting Auto-answered Calls

The auto answer mute feature allows the system to turn off the microphone when an incoming call is answered automatically. This avoids the caller hearing local conversation freely.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Auto Answer Mute**.
 - On your remote control, go to **More->Setting->Call Features->Auto Answer Mute**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
Auto Answer Mute	<p>Enables or disables the local microphone to be muted when an incoming call is answered automatically.</p> <p>Default: Enabled</p> <p>Auto answer mute feature is configurable only when the auto answer is enabled.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Related Topic:

[Auto Answer](#)

Muting Auto-dialed Calls

The auto dialout mute feature allows the system to turn off the microphone after the other party answers your call, so that the other party cannot hear you.

Note

The system is still muted after you hang up.

Procedure

- On your web user interface, go to **Setting->Call Features->Auto Dialout Mute**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
Auto Dialout Mute	<p>Enables or disables the system to turn off the microphone after the other party answers your call.</p> <p>Default: Disabled</p>	<p>Web User Interface</p>

Configuring Noise Suppression

The impact noises in the room are picked-up, including paper rustling, coffee mugs, coughing, typing and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting.

You can enable the Transient Noise Suppressor (TNS) to suppress these noises. You can also enable the Noise Barrier feature to block these noises when there is no speech in a call.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->Noise Suppression**.
2. Configure and save the following settings:


Parameter	Description	Configuration Method
TNS	Enables or disabled the Transient Noise Suppressor (TNS). Default: Enabled	Web User Interface
Noise Barrier	Enables or disabled the noise barrier feature. Default: Disabled	Web User Interface

Configuring Video Settings

Changing the Video Input Source

Your system supports camera and PC video input source. Video input source is camera by default, if you want to view the PC content, you can switch video input source to PC.

Procedure

1. Do one of the following during a call:
 - On your web user interface, go to **Home->Input Choose**.
 - On your remote control, press  or OK key to open Talk Menu, and select **Input Choose**.
 - If you select **PC**, the remote video image is shown in big size, and the PC content is shown in small size (Picture-in-Picture).
 - If you select **Camera+PC**, the PC content is shown in big size, and other video images are shown in small size.
 - If you select **Camera**, the remote video image is shown in big size, and the local video image is shown in small size (Picture-in-Picture).

Selecting Default Layout for Single Screen

When only one monitor is connected to the system, you can configure the default layout when a call is established.

Procedure

1. On your web user interface, go to **Setting->Call Features->Default Layout of Single Screen**.

2. Configure and save the following setting:

Parameter	Description	Configuration Method
Default Layout of Single Screen	<p>Configures the default layout of single screen when a call is established.</p> <ul style="list-style-type: none"> • Remote big Local small—the remote video image is shown in big size, and the local video image below is shown in small size. • Remote Full screen—the remote video image is shown in full size. • Equal—the remote and local video images are shown in the same size. • Picture In Picture—the remote video image is shown in full screen, and local video image is shown in the PIP (Picture-in-Picture) <p>Default: Picture In Picture</p>	Web User Interface

Selecting Video Frame Rate and Resolution

To transfer a clear and smooth video, you can specify the maximum frame and resolution for local video according to the network environment.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->Main**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable 60fps	<p>Enables or disables 60fps for a video call.</p> <p>Default: Enabled</p> <p>Note: It is not applicable to VC200.</p>	Web User Interface
Main->Frame	<p>Specifies the maximum frame rate of the video.</p> <ul style="list-style-type: none"> • 60fps—this option appears only if Enable 60fps is set to Enabled. 60fps is not applicable to VC200. • 30fps • 15fps • 5fps 	Web User Interface

Parameter	Description	Configuration Method
	Default: 30fps	
Main->Resolution	Specifies the maximum resolution of the video. <ul style="list-style-type: none"> 1080P 720P Default: 1080P	Web User Interface

Maximizing Monitor Video Display

Your monitor may not display the entire HD image. To solve this problem, you can adjust the monitor to display the entire HD image manually.

Procedure

1. On your remote control, go to **More->Setting->Basic->Display**.
2. Use left or right navigation key to adjust the **Display(90%-100%)** slider.

Configuring Monitor Resolution

You can specify the resolution for the monitor.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Video & Audio->Output Resolution**.
 - On your CP960 conference phone, go to **Settings->Display->Output Resolution**.

Parameter	Description	Configuration Method
Display1	Configures the output resolution of primary monitor. <ul style="list-style-type: none"> Auto-select the highest output resolution automatically Available output resolutions (The available resolutions depend on the monitor you are using) Default: Auto	Web User Interface CP960 conference phone
Display2	Configures the output resolution of secondary monitor. <ul style="list-style-type: none"> Auto-select the highest output resolution 	Web User Interface CP960 conference phone

Parameter	Description	Configuration Method
	automatically <ul style="list-style-type: none"> Available output resolutions (The available resolutions depend on the monitor you are using) Default: Auto	

Configuring Automatic Sleep Time

Static images displayed for long periods may lead to monitor burn-in. You can configure the inactive time before your system goes to sleep.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->General->General Information->Automatic Sleep Time**.
 - On your remote control, go to **More->Setting->Basic->Automatic Sleep Time**.
- Configure and save the following setting:

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

CEC Monitor Controls

Consumer Electronics Control (CEC) is a feature of HDMI designed to allow users to command and control devices connected through HDMI by using only one remote control.

CEC feature is enabled by default on Yealink video conferencing system. Ensure that all monitors connected to the system supports and enables CEC feature.

The following CEC features are available:

- One Touch Play**-Use the system remote control to wake up the monitors. All connected CEC-capable monitors are powered on, and their displays are switched to VCS input.
- System Standby**-When the VCS enters sleep mode, all connected CEC-capable monitors are

switched to standby mode for power saving.

Note

The VCS does not respond to CEC commands issued by a television remote control.

Configuring CEC Monitor Controls

Procedure

1. On your web user interface, go to **Setting->General->General Information->CEC Enable**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
CEC Enable	Enables or disables the CEC feature. Default: Enabled	Web User Interface

System Integrated with Control Systems

You can connect an AMX or Crestron control system to your video conferencing system, so that you can control your video conferencing system via the control system.

Connection Settings for Control Systems

You need to finish following settings before you connect the video conferencing system to the control system.

Procedure

1. On your web user interface, go to **Security->Security Control**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Current Control TCP Port	Control TCP port (read-only). Default: 6024	Web User Interface
Control Security Enabled	Enables or disables an authentication password when the control system tries to connect to the video conferencing system. Default: Enabled	Web User Interface
Control Security Password	Configures the authentication password when the control system tries to connect to the video conferencing system. Note: it is configurable only when the Control Security Enabled is on.	Web User Interface

Parameter	Description	Configuration Method
Baud Rate	Configures the baud rate. Available values are: <ul style="list-style-type: none"> • 2400 • 4800 • 9600 • 19200 • 38400 • 115200 Default: 115200 Note: It must be the same rate for control system and Yealink video conferencing system.	Web User Interface
Data Bits	Configures the data bits. Available values are: <ul style="list-style-type: none"> • 7 • 8 Default: 8 Note: It must be the same data bits for control system and Yealink video conferencing system.	Web User Interface
Parity	Configures the parity. Available values are: <ul style="list-style-type: none"> • None • Odd • Even • Space Default: Space Note: It must be the same parity for control system and Yealink video conferencing system.	Web User Interface
Stop Bits	Configures the stop bits. Available values are: <ul style="list-style-type: none"> • 1 • 2 Default: 1 Note: It must be the same stop bits for control system and Yealink video conferencing system.	Web User Interface

Connection Methods of Control Systems

You can connect Yealink video conferencing system to the control system via LAN connection or Serial connection.

- **LAN Connection:** Make sure the Yealink video conferencing system and the control system are in the same network segment. To establish a connection, the control system needs to know the IP address and TCP port of the Yealink video conferencing system.
- **Serial Connection:** The USB port on the Yealink video conferencing system can be connected to the serial port on the control system through a USB to RS-232 cable.

For more information, refer to [Yealink VC Deployment and User Manual for Control Systems](#) and [API Commands Introduction for Yealink Video Conferencing System](#).

Configuring Content Sharing

You can select dual-stream protocol or mix sending method to share content, and you can configure mode, frame rate and resolution for shared content.

Note

If the far site does not support the dual-stream protocol, you can select mix sending feature to mix the video and content, and then send them to the far site in one stream.

Configuring Dual-Stream Protocol

The dual-stream protocol allows video and PC content to 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).

Configuring H.239 protocol

H.239 protocol is used when sharing content with the far site in H.323 calls.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->StarLeaf**.
 - On your web user interface, go to **Account->H.323**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
H.239	Enables or disables the standards-based	Web User Interface

Parameter	Description	Configuration Method
	People+Content data collaboration in H.323 calls. Default: Enabled Note: Enable this setting if you know that H.239 is supported by the far-end sites you call.	

Enabling BFCP (Binary Floor Control Protocol)

BFCP protocol is used when sharing content with the far site in SIP calls.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->Zoom/Pexip/BlueJeans/Custom.**
 - On your web user interface, go to **Account->SIP Account.**
 - On your web user interface, go to **Account->SIP IP Call.**
- Configure and save the following setting:

Parameter	Description	Configuration Method
BFCP	Enables or disables the BFCP protocol for sharing content in SIP calls. Default: For Zoom/Pexip/BlueJeans/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled. Note: Enable this setting if you know that BFCP is supported by the far-end sites you call.	Web User Interface

Related Topic:

[Configuring Mix Sending](#)

Configuring Mix Sending

During a video call, the far site may not support H.239 protocol and BFCP. In this case, you can enable mix sending feature to mix the video and content to one stream, and then sent it to the far site.

Procedure

- On your web user interface, go to **Setting->Video & Audio.**

2. Configure and save the following setting:

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

Configuring Shared Content Parameters

You can specify the mode, maximum frame and resolution for the shared content.

Procedure

1. On your web user interface, go to **Setting->Video & Audio->Content Sharing**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Content Sharing Mode	Configures the content sharing mode. <ul style="list-style-type: none"> • Sharing Document- select this value to save bandwidth when you are sharing a document. • Sharing Video- select this value to play video fluently when you are sharing a video. Default: Sharing Document	Web User Interface
Frame	Specifies the maximum frame rate of the shared content. <ul style="list-style-type: none"> • 30fps • 15fps • 5fps Default: 15fps	Web User Interface
Resolution	Specifies the maximum resolution of the shared content. <ul style="list-style-type: none"> • 1080P • 720P Default: 1080P	Web User Interface



Configuring Camera Settings

You can configure camera settings on the system.

Adjusting Camera Angle and Focus

You can pan, tilt and zoom your own camera.

Procedure

- Do one of the following:
 - For VC880/VC800/VC500, on your web user interface, go to **Home->Yourself->**  .
 - For VC200, on your web user interface, go to **VC200->Yourself->**  .
 - On your remote control, select local video.
 - On your CP960 conference phone, tap **Camera**.
- Use the navigation buttons to move the camera up, down, left, or right.
- Use the zoom out/in key to zoom out or zoom in.

Adjusting Camera Parameters

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

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Camera**.
 - For VC880/VC800/VC500, on your remote control, go to **More-> Setting->Camera Setting**.
 - For VC200, on your remote control, go to **More-> Setting->Video & Audio**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Camera	Configures the desired camera.	Web User Interface
Status	Enables or disables the camera. Default: Enabled Note: It is not applicable to VC200.	Web User Interface
Multi-camera Default Layout	Configures the default camera layout when you connect multiple cameras. <ul style="list-style-type: none"> 1+N Selected Speaker Equal N×N Default: 1+N Note: It is not applicable to VC500/VC200.	Web User Interface

Parameter	Description	Configuration Method
Select a camera	<p>Select the camera you want to highlight.</p> <p>Default: The first connecting camera.</p> <p>This configuration appears only if Multi-camera Default Layout is set to 1+N or Selected Speaker.</p> <p>Note: It is not applicable to VC500/VC200.</p>	Web User Interface
Camera Name	<p>Configures a name for the camera.</p> <p>Note: It is not applicable to VC200.</p>	Web User Interface
Exposure Compensation	<p>Configures exposure compensation.</p> <ul style="list-style-type: none"> • Off • 1 to 12 <p>Exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlight environment. If the environment light is dark, you can increase the compensation value.</p> <p>Default: 1</p>	Web User Interface Remote Control
Flicker	<p>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 that the light is powered by.</p>	Web User Interface Remote Control
White Balance Mode	<p>Configures the white balance mode of the camera.</p> <p>Auto–Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room.</p> <ul style="list-style-type: none"> • InDoor • OutDoor • OnePush • ATW • Manual–Manually set red and blue gain. <p>Default: ATW</p>	Web User Interface Remote Control
Red Gain/Blue Gain	<p>Configures the red gain/blue gain of the camera.</p> <p>Valid Values: 0-100</p> <p>Default: 50</p>	Web User Interface Remote Control

Parameter	Description	Configuration Method
	<p>Note: You can set this parameter only when the white balance mode is configured to Manual.</p>	
Display Mode	<p>Configures the display mode of the camera.</p> <ul style="list-style-type: none"> High Definition Standard Mild Custom Definition <p>Default: Standard</p>	<p>Web User Interface</p> <p>Remote Control</p>
Saturation	<p>Configures the saturation of the camera's image.</p> <p>Valid Values: 0-100</p> <p>Default: 50</p>	<p>Web User Interface</p> <p>Remote Control</p>
Sharpness	<p>Configures the sharpness of the camera's image.</p> <p>Valid Values: 0-100</p> <p>Default: 15</p> <p>Note: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.</p>	<p>Web User Interface</p> <p>Remote Control</p>
Brightness	<p>Configures the brightness of the camera's image.</p> <p>Valid Values: 0-100</p> <p>Default: 50</p>	<p>Web User Interface</p> <p>Remote Control</p>
Contrast	<p>Configures the contrast of the camera's image.</p> <p>Valid Values: 0-100</p> <p>Default: 49</p>	<p>Web User Interface</p> <p>Remote Control</p>
Noise Reduction (2D)	<p>Specifies the noise reduction (2D) mode.</p> <ul style="list-style-type: none"> Off Low Middle High <p>Default: Middle</p>	<p>Web User Interface</p> <p>Remote Control</p>
Noise Reduction (3D)	<p>Specifies the noise reduction (3D) mode.</p> <p>Valid Values: 0-22</p> <p>Default: 3</p>	<p>Web User Interface</p> <p>Remote Control</p>
WDR	<p>Specifies the wide dynamic range.</p> <ul style="list-style-type: none"> Off-do not use WDR 1-5 	<p>Web User Interface</p> <p>Remote Control</p>

Parameter	Description	Configuration Method
	<p>Default: 2</p> <p>Note: Wide Dynamic Range (WDR) technology improves a camera's image quality under high-contrast lighting conditions where both dimly and brightly lit areas are present in the field of view. It enables the camera to capture details clearly in both the poorly and strongly illuminated areas of the video.</p>	
Hangup Mode	<p>Enables or disables the camera to flip the image view when camera is handed at up-side-down position</p> <p>Default: Off</p>	Web User Interface
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>	Web User Interface
Reset Camera	<p>Reset the camera settings to factory defaults.</p> <p>Note: The camera presets will also be cleared.</p>	Web User Interface

Allowing the Far-End System to Control Your Camera

You can allow the far-end system to control your camera, so that the far end obtain the best effect for viewing.

To allow the far-end system to control your camera, complete these two main tasks:

- Enable the camera control protocol.
- Enable the Far Control of Near Camera feature.

Camera Control Protocol

If far site wants to control your camera, both the far site and near site should enable the camera control protocol simultaneously. Your system supports FECC (Far End Camera Control) protocol. You can enable the FECC(H.323) protocol for H.323 call and enable FECC(SIP) protocol for SIP call.

Configuring FECC(H.323) Protocol

FECC(H.323) protocol is used when controlling the far-site camera in H.323 calls.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->StarLeaf.**
 - On your web user interface, go to **Account->H.323.**
- Configure and save the following setting:

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

Configuring FECC(SIP) Protocol

FECC(SIP) protocol is used when controlling the far-site camera in SIP calls.

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->Zoom/Pexip/BlueJeans/Custom.**
 - On your web user interface, go to **Account->SIP Account.**
 - On your web user interface, go to **Account->SIP IP Call.**
- Configure and save the following setting:

Parameter	Description	Configuration Method
FECC(SIP)	Enables or disables the FECC (SIP) protocol for far site to control near camera. Default: For Zoom/Pexip/BlueJeans/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled.	Web User Interface

Note

If FECC (SIP) protocol and FECC (H.323) protocol are both enabled, the system will select the appropriate camera control protocol according to the protocol (SIP or H.323) the call uses.

Configuring Far Control of Near Camera

You can allow the far site to pan, tilt, or zoom the near-site camera.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Video & Audio->Far Control of Near Camera**.
 - On your remote control, go to **More->Setting->Video & Audio->Far Control of Near Camera**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Not FECC in call(0~300s)	Configures the duration time (in seconds) that far site cannot control the near-site camera after the call establishes. Default: 15 If it is set to 15, the far site is not allowed to control the near-site camera in the first 15 seconds of the call.	Web User Interface
Far Control Near Camera	Enables or disables the far site to control the near-site camera. Default: Enabled	Web User Interface Remote Control

Setting Camera Presets

Camera presets store camera pan, tilt, and zoom settings. Camera presets help you quickly point a camera at pre-defined locations. Camera presets remain in effect until you change them. For more information about creating and using presets, refer to the [Yealink Full HD Video Conferencing System User Guide](#).

Configuring Call Settings

Call Protocol

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

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Call Protocol**.
 - On your remote control, go to **More->Call Features->Call Protocol**.

2. Configure and save the following settings:

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

Video Call Rate

You can specify the maximum video call rate. The configurable video call rates on the system are: 64kb/s, 128kb/s, 256kb/s, 384kb/s, 512kb/s, 768kb/s, 1024kb/s, 1280kb/s, 1500kb/s, 2000kb/s, 3000kb/s, 4000kb/s, 5000kb/s, 6000kb/s.

Note

The call rate of audio and PC content are also affected by this configuration.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Video Call Rate**.
 - On your remote control, go to **More->Call Features->Video Call Rate**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
Video Call Rate	<p>Specifies the maximum video call rate.</p> <p>Default: 2000kb/s</p>	<p>Web User Interface</p> <p>Remote Control</p>

Account Polling

Account polling feature allows the system to use different call types (Cloud platform/H.323 account/SIP account/PSTN account/H.323 IP Call/SIP IP Call) to dial a number when more than one account is registered.

Priority of Call Types

In the dialing screen, if you select the call type automatically, the system will select a call type according to the following priority:

- If you dial an account, the priority is: **Cloud platform>H.323 account>SIP account>PSTN account.**
- If you dial an IP address, the priority is: **H.323 IP Call>SIP IP Call.**

Procedure

1. On your web user interface, go to **Setting->Call Features->Account Polling.**
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Account Polling	<p>Enables or disables the account polling on the system.</p> <ul style="list-style-type: none"> • Disabled—the system dials a number using the call type with the highest priority. In this situation, once the dialed number differs from the call type you are using, the call will fail. • Enabled—the system tries each call type in order to dial a number. <p>Default: Enabled</p>	Web User Interface

Example;

1. System A is registered with a Yealink Cloud account and a SIP account.
2. Select the call type automatically.
3. Dial the number.
 - If account polling is disabled, system A can only use its Cloud account (highest priority) to call system B.
 - If account polling is enabled, system A will use its Cloud account (highest priority) to call system B first. If this call fails, system A continues to use its SIP account (next priority) to call system B.

Related Topic:

[Placing a Call by Entering a Number](#)

Search Source List in Dialing

Search source list in dialing allows you to search entries from the source list when the system is in the

dialing screen.





The source list includes History, Local Directory, Cloud Contacts, Enterprise Directory and LDAP.

Note

Cloud Contacts and Enterprise Directory appear in the search source list only when you log into the corresponding platform. If you want to match the LADP list, make sure LDAP is already configured.

Configuring Search Source List in Dialing

Procedure

1. On your web user interface, go to **Directory->Setting->Search Source List In Dialing**.
2. Select the desired list from the **Disabled** column and click  .
The selected search source list appears in the **Enabled** column.
3. Repeat step 2 to add more search source 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 search priority of the enabled search source lists, select the desired list, and click  or  .
The system will search the list with higher priority preferentially.

Related Topic:

[Call Match](#)

Call Match

Call match feature allows the dialing screen to display the search result after you enter the search criteria.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Call Match**.
 - On your remote control, go to **More->Setting->Call Features->Call Match**.
2. Configure and save the following setting:

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

Related Topic:

[Search Source List in Dialing](#)

Auto Answer

You can allow the system to answer incoming calls automatically.

Answering a Call Automatically

You can specify whether to answer a call automatically when the system is not in a call.

Caution:

Auto answer feature may create security issues. An unexpected caller can view your video conference room randomly.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Auto Answer**.
 - On your remote control, go to **More->Call Features->Call Features->Auto Answer**.
 - On your CP960 conference phone, swipe down from the top of the screen.
- Configure and save the following setting:

Parameter	Description	Configuration Method
Auto Answer	Enables or disables the auto answer feature on the system. Default: Enabled	Web User Interface Remote Control CP960 conference phone

Related Topic

[Muting Auto-answered Calls](#)

Answering Multiple Calls Automatically

You can specify whether to answer a call automatically when the system is already in a call.

Caution:

Auto answer multiway feature may create security issues. An unexpected caller may interrupt your ongoing conference call.

Before you begin

Make sure auto answer is enabled.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->Auto Answer Multiway**.
 - On your remote control, go to **More->Call Features->Call Features->Auto Answer Multiway**.

2. Configure and save the following setting:

Parameter	Description	Configuration Method
Auto Answer Multiway	Enables or disables the system to answer a call automatically when the system is already in a call. Default: Disabled	Web User Interface Remote Control

Do Not Disturb

You can enable do not disturb feature to reject incoming calls automatically. All calls you reject will be logged to Missed Calls list.

Enabling DND when Not in a Call

If you do not want to accept conference call, you can enable DND when the system is idle.


Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->DND**.
 - On your remote control, go to **More->Call Features->Call Features->DND**.
 - On your CP960 conference phone, swipe down from the top of the screen.
- Configure and save the following setting:

Parameter	Description	Configuration Method
DND	Enables or disables DND mode on the system. Default: Disabled	Remote Control Web User Interface CP960 conference phone

Enabling DND during an Active Call

To prevent callers from interrupting the active call, you can enable DND during an active call. The DND feature will be disabled automatically after the call ends.

- Do one of the following during a call:
 - For VC880/VC800/VC500, on your web user interface, go to **Home->DND**.
 - For VC200, on your web user interface, go to **VC200->DND**.
 - On your remote control, press  or OK key to open **Talk Menu**, and select **DND**.
 - On your CP960 conference phone, go to **More->DND**.

Configuring Ringback Timeout

Ringback timeout defines a specific period of time after which the system will cancel the dialing if the call is not answered by far site.

Procedure

1. On your web user interface, go to **Setting->Call Features->Ringback Timeout(30-240)**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Ringback Timeout (30-240)	Configures the duration time (in seconds) in the ringback state. Default: 180 If it is set to 180, the system will cancel dialing if the call is not answered within 180s.	Web User Interface

Configuring Auto Refuse Timeout

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

Procedure

1. On your web user interface, go to **Setting->Call Features->Auto Refuse Timeout(30-240)**.
2. Configure and save the following setting:

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

SIP IP Call by Proxy

If the account of far site is an URI address (8000@XX.com), near site can use SIP IP address or SIP account to call the far site.

Procedure

1. On your web user interface, go to **Setting->Call Features->SIP IP Call by Proxy**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
SIP IP Call by Proxy	<p>Configures the SIP IP call by proxy.</p> <ul style="list-style-type: none"> • Off—when dialing the URI of the far site, the system uses SIP IP address to establish a connection. • On—when dialing the URI of the far site, the system uses SIP account to establish a connection. <p>Default: Off</p>	Web User Interface

Configuring Conference Room

You can configure conference room type, password and video layout.

Note:

If You log into the Yealink VC Cloud Management Service, the conference may be managed via the Yealink VC Cloud Management Service only, you cannot configure it on your system.

Conference Type

Yealink video conferencing system can act as a virtual meeting room, so that other devices can dial the system to join a meeting.

The video conferencing system supports the following two conference types:

Conference Types	Supported Model	Difference	Multipoint Allocation
Regular Mode	VC880/VC800/VC500/VC200	Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.	Up to 1 video call and 5 voice calls.
VMR Mode	VC880/VC800 video conferencing system with a multipoint license	<p>Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.</p> <p>Virtual meeting room 2: when participants call the virtual meeting room 2, only participants join the meeting, the moderator does not join the meeting.</p>	<p>The total MCU ways of two virtual meeting rooms is depended on the multipoint license you imported.</p> <p>You can allocate the MCU ways between two virtual meeting rooms respectively.</p>

Related Topic:[Viewing Device Type](#)

Regular Mode Conference

Regular mode conference provides virtual meeting room 1.

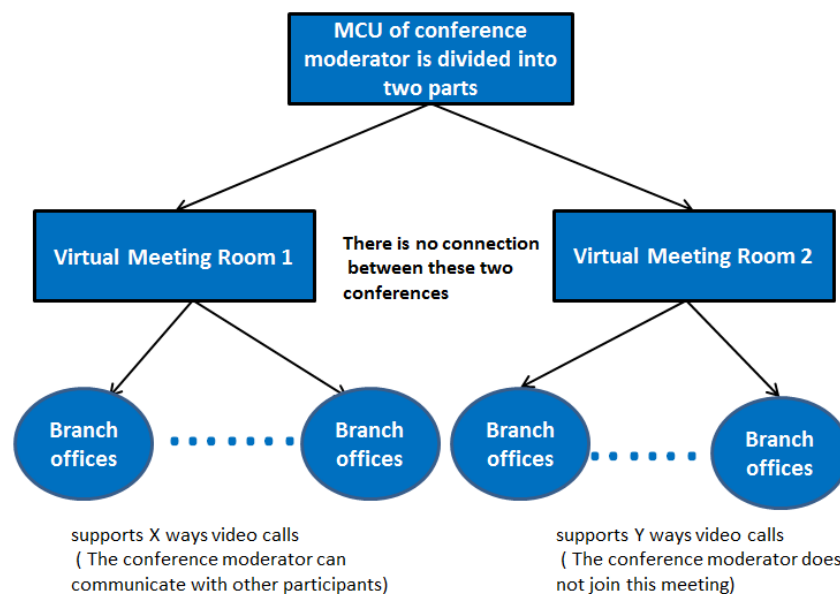
Selecting Regular Mode Conference

Procedure

1. On your web user interface, go to **Setting->Conference Setting**.
2. Select **Regular Mode** from the pull-down list of **Conference Type**.

VMR Mode Conference

In VMR mode conference, the MCU of moderator is used to host two independent conferences (corresponding to virtual meeting room 1 and virtual meeting room 2).



- If you import an 8 ways multipoint license to the VC880/VC800 system, $X+Y \leq 8$. Two virtual meeting rooms supports up to 8 ways video calls.
- If you import a 16 ways multipoint license to the VC880/VC800 system, $X+Y \leq 16$. Two virtual meeting rooms supports up to 16 ways video calls.
- If you import a 24 ways multipoint license to the VC880/VC800 system, $X+Y \leq 24$. Two virtual meeting rooms supports up to 24 ways video calls.

Note

When you import an 8 or 16 ways multipoint license to the VC880/VC800 system, the virtual meeting room 1 provides additional 5 voice calls.

Selecting VMR Mode Conference

VMR mode conference provides virtual meeting room 1 and 2. You can allocate the MCU ways between two virtual meeting rooms respectively.

Procedure

1. On your web user interface, go to **Setting->Conference Setting**.
2. Select **VMR Mode** from the pull-down list of **Conference Type**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Multipoint Allocation ->Virtual Meeting Room 1	Allocates the maximum ways of video calls for virtual meeting room 1.	Web User Interface
Multipoint Allocation ->Virtual Meeting Room 2	Allocates the maximum ways of video calls for virtual meeting room 2.	Web User Interface

Meeting Password

Depending on how a conference call is set up, you might be required to enter a meeting password to join a conference. You can also require far site to enter a meeting password to prevent unauthorized participants from joining conference calls hosted by your system.

If you host a regular mode conference, you need to configure a password for virtual meeting room 1. If you host a VMR mode conference, you need to configure passwords for virtual meeting room 1 and virtual meeting room 2 respectively.

Configuring Meeting Password

Procedure

1. On your web user interface, go to **Setting->Conference Setting**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Virtual Meeting Room 1->Meeting Password	Enables or disables the system to configure a password for virtual meeting room1. <ul style="list-style-type: none"> • On • Off Default: Off	Web User Interface
Virtual Meeting Room 1->Meeting Room	Configures the password for virtual meeting room 1.	Web User Interface

Parameter	Description	Configuration Method
1Password		
Virtual Meeting Room 2->Meeting Password	<p>Enables or disables the system to configure a password for virtual meeting room 2.</p> <ul style="list-style-type: none"> On Off <p>Default: Off</p>	Web User Interface
Virtual Meeting Room 2->Password	Configures the password for virtual meeting room 2.	Web User Interface

Related Topic:

[Conference Type](#)

Joining the Meeting

If the virtual meeting room requires no password, dial IP address or account to enter the virtual meeting room.

If the virtual meeting room requires a password, dial **IP##meeting password** or **meeting password@IP** to enter the virtual meeting room.

For example:

- The IP address of moderator is 10.3.6.201.
- 123 is meeting password for virtual meeting room 1.
- 456 is meeting password for virtual meeting room 2.

Participants can dial **10.3.6.201##123** or **123@10.3.6.201** to enter the virtual meeting room 1.

Participants can dial **10.3.6.201##456** or **456@10.3.6.201** to enter the virtual meeting room 2.

Without a meeting password or with a wrong meeting password, the call will fail.

Related Topic:

[Placing a Call by Entering a Number](#)

Configuring Voice Activation

Voice activation displays the active speaker in largest pane. Other participants are displayed in a strip beside the active speaker. To minimize the changes in the layout, when a new speaker is identified, the image of the previous speaker is replaced by the new speaker.

Note

Voice activation is only applicable to VC880/VC800 system with a multipoint license. It is not applicable to

VC500/VC200 endpoint.

Voice activation works only when the conference call has more than two participants.

Procedure

1. On your web user interface, go to **Setting->Conference Setting**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Voice Activation	Enables or disables voice activation. Default: Enabled	Web User Interface
Voice Hold Active Duration	Configures the voice activation interval. If voice duration of the new speaker is greater than this interval, the image of the previous speaker is replaced by the new speaker. Default: 1s.	Web User Interface

Configuring View Switching

View switching allows the video images on the monitor change automatically. It is initiated when the number of participants exceeds the number of windows in the selected video layout.

There are two modes for view switching:

- **Average Mode:** Up to 9 video images can be displayed in **Equal N×N** layout. When the number of participants exceeds 9, all participants' video images will be switched automatically. Video image of the active speaker is indicated by an orange border. If you share content, the PC content is fixed at the top-left corner and will not be switched automatically.
- **1+N Mode:** Up to 8 video images can be displayed in **Speaker View** layout and **OnePlusN** layout. When the number of participants exceeds 8, all participants' video images (except the active speaker) will be switched automatically. If you share content, the PC content is given prominence in the largest pane. The active speaker is fixed at the bottom-left corner, and other video images will be switched automatically.

Note

View switching is only applicable to VC880/VC800 system with a multipoint license. It is not applicable to VC500/VC200 endpoint.

Configuring Average Mode

In **Equal N×N** layout, when the number of participants exceeds 9, all participants' video images will be switched automatically. You can configure the switching mode.

Procedure

1. On your web user interface, go to **Setting->Conference Setting->Average Mode**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. Default: 30s. The video images will be switched automatically every 30 seconds.	Web User Interface
Single View Round	Switches one video image at a time.	Web User Interface
Full Screen Round	Switches all video images at a time.	Web User Interface

Configuring 1+N Mode

In **Speaker View** layout and **OnePlusN** layout, when the number of participants exceeds 8, all participants' video images (except the active speaker) will be switched automatically.

Procedure

1. On your web user interface, go to **Setting->Conference Setting->1+N Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. Default: 30s. The video images will be switched automatically every 30 seconds.	Web User Interface
View Round	Configure how many video images to be switched at a time. Valid values: 1 to 7 Default: 1	Web User Interface
Full Screen Round	Switches all video images at a time.	Web User Interface

Securing the System

Topics:

[User and Administrator](#)

[Configuring Auto Logout Time](#)

[Transport Layer Security \(TLS\)](#)

[Secure Real-Time Transport Protocol \(SRTP\)](#)

[H.235 Defending against Attacks](#)

For detailed information about configuring security settings, see the following topics.

User and Administrator

There are two roles for accessing video conferencing system: user and administrator.

On web user interface, administrator has full permission to access every menu, and some menus are hidden for user.

On monitor, administrator has full permission to access every menu, while user needs to enter user password to access some menus.

Configuring an Administrator Password

The default administrator name is "admin" and the administrator password is "0000". For security reasons, you should change them as soon as possible.

Procedure

- Do one of the following:
 - On your web user interface, go to **Security->Security**.
 - On your remote control, go to **More->Setting->Advanced->Password Reset**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
User Type	Select Administrator.	Web User Interface
Old Password/ Current Password	Enters the old administrator password. Note: The default administrator password is "0000".	Web User Interface Remote Control
New Password	Configures a new administrator password. Note: You can leave the password blank.	Web User Interface Remote Control

Parameter	Description	Configuration Method
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".	Web User Interface Remote Control

Enabling the User Role

You can assign a user role.

Procedure

1. On your web user interface, go to **Security->Security**.
2. Select **Enabled** from the pull-down list of **User Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
User Type	Select User.	Web User Interface
User Mode	Enables the user role.	Web User Interface
User Password	Configures a user password. Note: It is configurable only when the user mode is enabled.	Web User Interface

Configuring Auto Logout Time

The system will log out of the web user interface automatically after being inactive for a period of time. You need to re-enter the login credentials to login.

Procedure

1. On your web user interface, go to **Setting->General->General Information->ReLogOffTime(1-1000min)**.
2. Configure and save the following setting:

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

Transport Layer Security (TLS)

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.

Supported Cipher Suites

The system supports TLS version 1.0, 1.1 and 1.2. 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
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- 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-RC2-CBC-MD5
- EXP-RC4-MD5

TLS Transport Protocol

You can provide secure communication for SIP signaling using TLS transport protocol.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->Zoom/Pexip/BlueJeans/Custom.**
 - On your web user interface, go to **Account->SIP Account->Transport.**
 - On your remote control, go to **More->Settings->Advanced->SIP Account->Transport.**
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Transport	<p>Configures the transport protocol for SIP signaling.</p> <ul style="list-style-type: none"> • UDP—provides best-effort transport via UDP for the SIP signaling. • TCP—provides reliable transport via TCP for SIP signaling. • TLS—provides secure communication for SIP signaling. • DNS-NAPTR—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. <p>Default:</p> <p>For Zoom/Pexip/BlueJeans/Custom platform, the default value is TCP.</p> <p>For SIP account, the default value is UDP.</p>	<p>Web User Interface</p> <p>Remote Control</p>

Managing the Trusted Certificates List

When the system serves as a TLS client and requests a TLS connection with a server, the system should verify the server certificate sent by the server to decide whether it is trusted based on the trusted certificates list.

The trusted certificates list contains the default and custom certificates.

- **Default Certificates:** The system has 36 built-in trusted certificates. For more information refer to

[Default Certificates List](#) on page 156.

- **Custom Certificates:** You can upload up to 10 trusted certificates to the system. The format of the certificates must be *.pem, *.cer, *.crt and *.der.

Procedure

1. On your web user interface, go to **Security->Trusted Certs.**
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Only Accept Trusted Certificates	<p>Enables or disables the system to only trust the server certificates in the trusted certificates list.</p> <p>Default: Enabled</p> <p>Note: If it is enabled, the system will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the system trust the server.</p> <p>If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
Common Name Validation	<p>Enables or disables the system to mandatorily validate the CommonName or SubjectAltName of the server certificate sent by the server. This security verification rules are compliant with RFC 2818.</p> <p>Default: Disabled</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
CA Certificates	<p>Configures the type of certificates in the Trusted Certificates list for the system to authenticate for the TLS connection.</p> <ul style="list-style-type: none"> • Default Certificates • Custom Certificates • All Certificates <p>Default: Default Certificates</p> <p>Note: If you change this parameter, the system will reboot to make the change take effect.</p>	Web User Interface
Upload Trusted Certificate File	<p>Configures the access URL of the custom trusted certificate used to authenticate the connecting server.</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

Default Certificates List

Yealink video conferencing system trusts the following CAs by default:

- VeriSign Class 3 Public Primary Certification Authority - G5
- GeoTrust Universal CA
- Equifax Secure eBusiness CA-1
- Thawte Server CA
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 4 Public Primary Certification Authority - G3
- Thawte Premium Server CA
- thawte Primary Root CA - G2
- thawte Primary Root CA - G3
- GeoTrust Global CA 2
- GeoTrust Universal CA 2
- GeoTrust Primary Certification Authority
- GeoTrust Global CA
- Class 3 Public Primary Certification Authority
- -Thawte Personal Freemail CA
- thawte Primary Root CA
- -VeriSign Universal Root Certification Authority
- Equifax Secure Certificate Authority
- DigiCert High Assurance EV Root CA
- Equifax Secure Global eBusiness CA-1
- Yealink Equipment Issuing CA
- GeoTrust Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- Deutsche Telekom Root CA 2
- Class 1 Public Primary Certification Authority
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 Secure Server CA - G
- quickconnect.starleaf.com
- yealinkvc.com
- StarLeaf CA
- Class 1 Public Primary Certification Authority - G2
- Class 2 Public Primary Certification Authority - G2
- Class 3 Public Primary Certification Authority - G2

- Class 4 Public Primary Certification Authority - G2

Note

Yealink endeavors 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 \(TLS\)](#) on page 153.

Managing the Server Certificates

The system can serve as a TLS server. When clients request a TLS connection with the system, the system sends the server certificate (device certificate) to the clients for authentication.

The server certificate contains the default and custom certificates.

- **Default Certificates:** a unique server certificate and a generic server certificate.
 - a) **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).
 - b) **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.
- **Custom Certificates:** 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.

Procedure

1. On your web user interface, go to **Security->Server Certs**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Device Certificates	Configures the type of the server certificates for the system to send for TLS authentication. <ul style="list-style-type: none"> • Default Certificates • Custom Certificates Default: Default Certificates Note: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Upload Server Certificate File	Configures the access URL of the server certificate the system sends for authentication. Note: Only one server certificate can be uploaded to the system. The server certificate you want to upload must be in *.pem or *.cer format.	Web User Interface

Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the RTP during SIP calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP feature simultaneously. When this feature is enabled on both sites, the encryption type used in the session is negotiated between the systems. This negotiation process is compliant with [RFC 4568](#).

Rules of SRTP for media encryption in SIP calls:

Far \ Near	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

When you place a call that enables SRTP, the system sends an INVITE message with the RTP encryption algorithm to the destination system. As described in [RFC 3711](#), RTP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

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:NzFINTUwZDk2OGVIOTc3YzNkYTkWZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

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

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNIOTNkOWRiYzRiMjM0Yzcz
a=sendrecv
```

```
a=ptime:20
a=fmtp:101 0-15
```

Note

If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information, refer to [TLS Transport Protocol](#) on page 154.

Related Topic:

[Transport Layer Security \(TLS\)](#)

SRTP Configuration

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->Zoom/Pexip/BlueJeans/Custom**.
 - On your web user interface, go to **Account->SIP Account->SRTP**.
 - On your web user interface, go to **Account->SIP IP Call->SRTP**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
SRTP	Specifies the SRTP type. <ul style="list-style-type: none"> Disabled—encrypted calls are not supported. Optional—both encrypted and unencrypted calls are supported. Secure calls are supported only if the far end supports encryption. Compulsory—unencrypted calls are not supported. Default: Disabled	Web User Interface

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

H.235

H.235 encrypts the RTP during H.323 calls to avoid interception and eavesdropping. The parties participating in the call must enable H.235 feature simultaneously. When this feature is enabled on both sites, the encryption type used in the session is negotiated between the systems.

Rules of H.235 security in H.323 calls:

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

H.235 Configuration

Procedure

- Do one of the following:
 - On your web user interface, go to **Account->VC Platform->Video Conference Platform->Platform Type->StarLeaf**.
 - On your web user interface, go to **Account->H.323**.
- Configure and save the following setting:

Parameter	Description	Configuration Method
H.235	Specifies the H.235 type. <ul style="list-style-type: none"> Disabled—encrypted calls are not supported. Optional—both encrypted and unencrypted calls are supported. Secure calls are supported only if the far end supports encryption. Compulsory—unencrypted calls are not supported. Default: Disabled	Web User Interface

When H.235 is enabled on both sites, RTP streams will be encrypted, and a lock icon appears on the monitor of each system after successful negotiation.

Defending against Attacks

VCS sometimes receives calls from unknown caller, and the calls may be unable to answer. To ensure the communications security of the VCS, you can configure abnormal call answering feature to handle abnormal SIP incoming call or configure safe mode call feature to verify H.323 incoming call.

Abnormal Call Answering

When destination address of the incoming SIP call does not match local address, the call is considered to be an abnormal call. You can reject the abnormal SIP incoming call, or answer it using IP address or SIP account randomly.

Procedure

1. On your web user interface, go to **Setting->Call Features->Abnormal Call Answering**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Abnormal Call Answering	<p>Specifies the account type for answering abnormal SIP incoming calls.</p> <ul style="list-style-type: none"> • Disabled—reject the abnormal SIP incoming calls. • Account Answer—use the SIP account to answer the abnormal SIP incoming calls. • IP Call Answer—use IP address to answer the abnormal SIP incoming calls. <p>Default: IP Call Answer</p>	Web User Interface

Configuring Safe Mode Call

Safe mode call feature is used to verify whether the incoming H.323 call is coming from a H.323 endpoint.

Procedure

1. On your web user interface, go to **Setting->Call Features->Safe Mode Call**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Safe Mode Call	<p>Enables or disables the safe mode call feature</p> <ul style="list-style-type: none"> • Disabled—Answer incoming H.323 calls directly without validation. • Enabled—Verify whether the incoming H.323 call is coming from a H.323 endpoint. If it is, the system will answer it. If not, the incoming call will be rejected. <p>Default: Disabled</p>	Web User Interface

Managing the Directory

Topics:

[Local Directory](#)

[Cloud Directory](#)

[Enterprise Directory](#)

[Lightweight Directory Access Protocol \(LDAP\)](#)

[Searching for Contacts](#)

[Placing Calls to Contacts](#)

[Meeting Whitelist](#)

[Meeting Blacklist](#)

This chapter describes how to manage and configure directory settings. Your system provides local directory, Yealink cloud directory, Yealink enterprise directory and LDAP directory.

Local Directory

You can add, edit, delete, search or simply dial a contact from the local directory.

Adding Local Contacts and Conference Contacts

A conference contact consists of one or more local contacts. You can establish a conference call quickly by calling the conference contact.

Adding a Local Contact

You can add 500 local contacts to your system at most.

Procedure

- Do one of the following:
 - For VC880/VC800/VC500, on your web user interface, go to **Directory->Local Directory->New Contact->Local**.
 - For VC200, on your web user interface, go to **Directory->Local Directory->New Contact**.
 - On your remote control, go to **Dial->Directory->New Contact**.
- Configure and save the following settings:

Parameter	Description	Configuration Method
Name	Configures the contact name.	Web User Interface

Parameter	Description	Configuration Method
		Remote Control
Number	Configures the contact number.	Web User Interface Remote Control
Add New Number	Add up to 3 numbers to the contact.	Web User Interface Remote Control
Bandwidth	<p>Configures the bandwidth used in a call with this contact.</p> <p>Default: Auto. It means the system will select the appropriate bandwidth automatically.</p> <p>Note: When you call a local contact, the call rate that applies (video call rate or bandwidth) is the rate with the lower value. For more information, refer to Video Call Rate on page 138.</p>	Web User Interface Remote Control

Adding a Conference Contact

You can add 100 conference contacts at most.

Note

Conference contact is only applicable to VC880/VC800 system with a multipoint license. It is not applicable to VC500/VC200 endpoint.

Procedure

- Do one of the following:
 - On your web user interface, go to **Directory->Local Directory**.
Check the checkboxes of desired local contacts.
go to **New Contact->Conf**.
 - On your remote control, go to **Dial->Directory**.
Select **Conference Contacts** from the pull-down list of **All Contacts**.
Select **New Conference**.
Add the desired local contacts to the members List.
Enter the conference name.
- Save the change.

Note

The number of local contacts that you can add to a conference contact depends on the imported multipoint license.

For example, if you import a 24 ways license to your VC880/VC800 system, up to 24 local contacts can be

added to a conference contact.

Related Topics

[Viewing Multipoint License Status](#)

Importing a Local Contact List

You can upload a local contact list to your system to add multiple contacts at a time. The system supports the XML and CSV format contact lists.

Procedure

1. On your web user interface, go to **Directory->Local Directory->Import/Export->Import**.
2. Click **Browse** to locate a local contact list from your local system.
3. If you import a CSV format contact list, Configure and save the following settings:

Parameter	Description	Configuration Method
The first line as the title	It will prevent importing the title of the local contact information which is located in the first line of the CSV file. <ul style="list-style-type: none"> • Check—do not import the first line of the CSV file. • Uncheck—import the first line of the CSV file. 	Web User Interface
Delete Old Contacts	It will delete all existing local contacts while importing the contact list.	Web User Interface
Ignore	This column will not be imported to the system.	Web User Interface
Display Name	This column will be imported to the system as the local contact's name. Note: This column must be imported to the system, or you cannot import the local contact list.	Web User Interface
group	This column will be imported to the system as the group.	Web User Interface
number	This column will be imported to the system as the local contact's number.	Web User Interface
Bandwidth	This column will be imported to the system as the local contact's bandwidth.	Web User Interface

Exporting Local Contacts List

You can export a local contact list in XML format from your system. So that you can share with other systems.



Procedure

1. On your web user interface, go to **Directory->Local Directory->Import/Export->Export XML**.

Editing Local Contacts

You can change or add more information to your local contacts at any time.

Procedure



1. Do one of the following:
 - On your web user interface, go to **Directory->Local Directory**.
Hover your cursor over the local contact you want to edit.
Click  in the pop-up detail box.
 - On your remote control, go to **Dial->Directory**.
Select the desired contact and then press the right navigation key to select **Edit**.
 - On your CP960 conference phone, tap **Directory**.
Tap  after the desired contact.
Edit the contact information.
2. Save the change.

Deleting Local Contacts

You can delete a contact, multiple contacts or all contacts in your local directory.

Deleting a Local Contact

Procedure

1. Do one of the following:
 - On your web user interface, go to **Directory->Local Directory**.
Hover your cursor over the local contact you want to delete.
Click  in the pop-up detail box.
 - On your remote control, go to **Dial->Directory**.
Select the desired contact and then press the right navigation key to select **Delete**.
 - On your CP960 conference phone, tap **Directory**.
Tap  after the desired contact, and then tap **Delete**.

Deleting Multiple Local Contacts

Procedure

1. On your web user interface, go to **Directory**->**Local Directory**.
2. Check the checkboxes of desired local contacts.
3. Go to **Delete Contacts**->**Selected**.

Deleting All Local Contacts

Procedure

1. On your web user interface, go to **Directory**->**Local Directory**.
2. go to **Delete Contacts**->**Delete All**.

Cloud Directory

Cloud directory appears only when you log into the Yealink VC Cloud Management Service. Contact your system administrator for more information.

Cloud directory includes all Yealink cloud contacts which are created by your cloud enterprise administrator. Note that only the cloud enterprise administrator can add, edit and delete Yealink cloud contacts on the Yealink VC Cloud Management Service.

On your system, you can only search for and place calls to the Yealink cloud contacts.

There are three types of YMS contact:

- **Contacts:** The users with Yealink Cloud accounts. The Yealink Cloud enterprise administrator can create departments for users.
- **Room system:** The devices with Yealink Cloud accounts in the video meeting room.
- **Virtual Meeting Room:** It is also called the permanent VMR. The Yealink Cloud enterprise administrator can determine whether to synchronize the permanent VMR to the video conferencing system.

Related Topic:

[Registering a Yealink Cloud Account](#)

Enterprise Directory

Enterprise directory appears only when you log into the Yealink Meeting Server. Contact your system administrator for more information.

Enterprise directory includes all YMS contacts which are created by your enterprise administrator. Note that only the enterprise administrator can add, edit and delete YMS contacts on the Yealink Meeting Server.

On your system, you can only search for and place calls to the YMS contacts.

There are four types of YMS contact:

- **User:** The users have YMS accounts. The enterprise administrator can create departments for users.
- **Room system:** The devices registered YMS accounts in the video meeting room.
- **Third party device:** The devices without YMS accounts.
- **VMR:** It is also called the Permanent VMR. The enterprise administrator can determine whether to synchronize the permanent VMR to your system.

Related Topic:

[Registering a YMS Account](#)

Lightweight Directory Access Protocol (LDAP)

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. You can configure the systems 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)

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

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on systems.

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

Configuring LDAP

Procedure

1. On your web user interface, go to **Directory->LDAP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
LDAP Enable	Enables or disables the LDAP feature on the system. Default: Disabled	Web User Interface
LDAP Name Filter	Configures the name attribute for LDAP searching. Example: ((cn=*)(sn=*))	Web User Interface
LDAP Number Filter	Configures the number attribute for LDAP searching. Example: ((telephoneNumber=*)(mobile=*))	Web User Interface
LDAP TLS Mode	Configures the connection mode between the LDAP server and video conferencing system. <ul style="list-style-type: none"> • LDAP—Unencrypted connection between LDAP server and the system (port 389 is used by default). • LDAP TLS Start—TLS/SSL connection between LDAP server and the system (port 389 is used by default). • LDAPS—TLS/SSL connection between LDAP server and the system (port 636 is used by default). Default: LDAP	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 log into 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


Parameter	Description	Configuration Method
LDAP Password	Configures the password to log into the LDAP server. Note: The password is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user password to access the LDAP server.	Web User Interface
LDAP Base	Configures the root path of the LDAP search base. Example: cn=manager,dc=yealink,dc=cn	Web User Interface
Max Hit(1~32000)	Configures the maximum number of search results to be returned by the LDAP server.	Web User Interface
LDAP Name Attributes	Configures the name attributes of each record to be returned by the LDAP server. Note: multiple name attributes should be separated by spaces. Example: cn sn	Web User Interface
LDAP Number Attributes	Configures the number attributes of each record to be returned by the LDAP server. Note: multiple numbers attributes should be separated by spaces. Example: telephoneNumber mobile	Web User Interface
LDAP Display Name	Configures the display name of the contact record displayed on the LCD screen. Note: multiple numbers attributes should be separated by spaces. Example: %cn	Web User Interface
Protocol	Configures the protocol for the LDAP server. Note: Make sure the protocol value corresponds with the version assigned on the LDAP server.	Web User Interface
Match Incoming Call	Enables or disables the system to match caller numbers with LDAP contacts. Default: Disabled Note: If the match is successful, the system will display the caller name when receives an incoming call.	Web User Interface

Parameter	Description	Configuration Method
Match Outgoing Call	<p>Enables or disables the system to match outgoing call numbers with LDAP contacts.</p> <p>Default: Enabled</p> <p>Note: If the match is successful, the system will display the contact name when places a call.</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

Searching for Contacts




You can enter search criteria to find desired contact quickly.

Procedure

- Do one of the following:
 - On your web user interface, go to **Directory->Local Directory**.
 - On your remote control, go to **Dial->Directory**.
 - On your CP960 conference phone, tap **Directory**, and then tap .
- Enter a few or all characters of the contact name or numbers in the **Search** field.

Placing Calls to Contacts

Procedure

- Do one of the following:
 - On your web user interface, go to **Directory->Local Directory**.
Hover your cursor over the local contact you want to call.
Click  or  in the pop-up detail box to place a video or voice call.
 - On your remote control, go to **Dial->Directory**.
Select the desired contact and then press the right navigation key to select **Video Call** or **Voice Call**.
 - On your CP960 conference phone, tap **Directory**.
Tap  after the desired contact and then tap **Video Call** or **Voice Call**.

Meeting Whitelist

You can add meeting whitelist. Users in the whitelist can join your conference call directly without

meeting password even if you have enabled the meeting password feature. Your system supports up to 100 whitelist records.

Note

Users in the whitelist can join virtual meeting room 1 of conference moderator without a password. If conference moderator hosts a VMR mode conference, users in the whitelist still need password to join virtual meeting room 2.

Configuring Meeting Whitelist

Procedure

1. On your web user interface, go to **Directory->Meeting Whitelist->Meeting Whitelist Number**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Meeting White list Number	Add the IP address, account or domain name of the far site to the meeting whitelist. Default: blank	Web User Interface

3. Click **Add** to add the meeting whitelist.

Deleting Meeting Whitelist

Procedure

1. On your web user interface, go to **Directory->Meeting Whitelist**.
2. Click **Delete** to delete the meeting whitelist.

Meeting Blacklist

You can add meeting blacklist. Your system will refuse incoming calls from the blacklist automatically. Your system will not remind incoming calls or save call history from blacklist. Your system supports up to 100 blacklist records.

Adding Meeting Blacklist

Procedure

1. On your web user interface, go to **Directory->Meeting Blacklist->Meeting Blacklist Number**.

2. Configure and save the following setting:

Parameter	Description	Configuration Method
Meeting Blacklist Number	Add the IP address, account or domain name of the far site to the meeting blacklist. Default: blank	Web User Interface

3. Click **Add** to add the meeting blacklist.

Deleting Meeting Blacklist

Procedure

1. On your web user interface, go to **Directory->Meeting Blacklist**.
2. Click **Delete** to delete the meeting blacklist.

Managing the Call Log

Topics:

[Saving History Record](#)

[Adding a History Record to Local Directory](#)

[Deleting History Records](#)

[Placing Calls to History Records](#)

Call log consists of four lists: Missed Calls, Placed Calls, Received Calls, and Forwarded Calls. The system supports up to 100 entries. The call log contains call information such as remote party identification and time and date of the call.

Saving History Record

You can configure the system to save the history records or not.

Procedure

- Do one of the following:
 - On your web user interface, go to **Setting->Call Features->History Record**.
 - On your remote control, go to **More->Setting->Call Features->History Record**.
- Configure and save the following setting:


Parameter	Description	Configuration Method
History Record	Enables or disables the system to log the call history (missed calls, placed calls, and received calls) in the call lists. Default: Enabled	Web User Interface Remote Control

Adding a History Record to Local Directory

You can add a history record to the local directory.

Procedure

- Do one of the following:
 - On your remote control, go to **Dial->History**.
Select the desired history record and then press the right navigation key to select **Add to Contact**.
 - On your CP960 conference phone, tap **History**.

Tap  after the history record and then tap **Add to Contact**.


2. Configure the settings.

Deleting History Records

You can delete a history record, multiple history records or all history records.

Deleting a History Record

Procedure

1. Do one of the following:
 - On your remote control, go to **Dial->History**.
Select the desired history record and then press the right navigation key to select **Delete**.
 - On your CP960 conference phone, tap **History**.
Tap  after the desired history record, and then tap **Delete**.

Deleting Multiple History Records

Procedure

1. On your web user interface, go to **Directory->History**.
2. Check the checkboxes of desired history records.
3. Go to Delete **Calllogs->Selected**.




Deleting All History Records

Procedure

1. Do one of the following:
 - On your web user interface, go to **Directory->History**.
Go to **Delete Calllogs->Delete All**.
 - On your remote control, go to **Dial->History**.
Select the desired history record from the pull-down list of **All Calls**.
Select **Delete**.

Placing Calls to History Records

Procedure

1. Do one of the following:
 - On your web user interface, go to **Directory->History**.
Hover your cursor over the history record you want to call.
Click  or  in the pop-up detail box to place a video or voice call.
 - On your remote control, go to **Dial->History**.
Select the desired history record and then press the right navigation key to select **Video Call** or **Voice Call**.
 - On your CP960 conference phone, tap **History**.
Tap  after the desired history record and then tap **Video Call** or **Voice Call**.

Placing a Call

Topics:

[Placing a Call by Entering a Number](#)

[Placing a Call from the Search Result](#)

[Editing Numbers before Calling](#)



You can use your system just like a regular phone to place calls in numerous ways easily.

Placing a Call by Entering a Number

You can place a call to following account types:

- IP address (for example: 192.168.1.15)
- H. 323 account
- SIP account
- Cloud account
- PSTN account
- SIP URI (for example: 2210@sip.com)

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500, on your web user interface, go to **Home**. For VC200, on your web user interface, go to **VC200**.
Enter the number, and select the desired call type and video call rate.
Click **Video Call** or **Voice Call** to place a video or voice call.
 - On your remote control, go to **Dial**.
Enter the number, and select the desired call type from the pull-down list of **Call Type**.
Press the right navigation key to select  (video call) or  (voice call).
 - On your CP960 conference phone, tap **Dial**.
Enter the number, and select the desired call type from the pull-down list of **All**.
Tap **Send** to place a video call.

Related Topic:

[Video Call Rate](#)

[Account Polling](#)

Placing a Call from the Search Result

You can enter search criteria on the dialing screen to find your desired contact or number, and then place a call.

Make sure search source list is configured and the call match feature is enabled.

Procedure

1. Do one of the following:
 - On your remote control, go to **Dial**.
 - On your CP960 conference phone, tap **Dial**.
2. Select the desired call type.
3. Enter a few or all characters of the contact name or numbers in the **Search** field.
4. Dial the search result.

Related Topic:

[Search Source List in Dialing](#)


[Call Match](#)

[Placing a Call by Entering a Number](#)

Editing Numbers before Calling

In the dialing screen or history screen, you can edit the contact numbers or history records and then dial out.

Procedure

1. Do one of the following:
 - On your remote control, go to **Dial** or go to **Dial->History**.
Select the desired history record and then press the right navigation key to select **Edit before calling**.
 - On your CP960 conference phone, tap **Dial** or tap **History**.
Tap  after the desired history record and then tap **Edit before calling**.
2. Edit the number and dial out.

Accessories with Your System

Topics:

[Using the VCC22 Video Conferencing Cameras](#)

[Using the CPW90 Wireless Microphones with VCS](#)

[Using the CPW90 Wireless Microphones with CP960](#)

[Using the CPW90-BT Bluetooth Wireless Microphones with VCS](#)

This section describes the how to use VCC22 video conferencing cameras, CPW90 wireless microphones and CPW90-BT Bluetooth wireless microphones. For more information on other accessories, refer to related guide.

Using the VCC22 Video Conferencing Cameras

You can connect up to 9 VCC22 video conferencing cameras to the VC880 video conferencing system. You can connect up to 8 VCC22 video conferencing cameras to the VC800 video conferencing system. For more information, refer to [Yealink VCC22 Camera Quick Start Guide](#).

VCC22 video conferencing cameras are not applicable to VC500/VC200 video conferencing endpoint.

Controlling VCC22 Camera

When the system is idle, you can choose the desired camera to capture video images.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Home->Camera Layout**.
 - On your remote control, press the right navigation key twice to enter the cameras list.
 - On your CP960 conference phone, tap **Camera->The current control camera**.
2. Select the desired camera and then adjust the angle and focus.


Adjusting Camera Layout

During a call, all video streams captured from the connected near-site cameras are synthesized to one video stream, and then sent to the far site. You can change the camera layout during a call.

Procedure

1. Do one of the following:
 - When the system is idle, on your web user interface, go to

Setting->Camera->Camera->Multi-camera Default Layout.

- When the system is during a call, on your web user interface, go to **Home->Camera Layout**.
- On your remote control, press  or OK key to open **Talk Menu**, and select **Camera Layout**.
- On your CP960 conference phone, tap **Camera Layout**.

2. Configure and save the following setting:

Parameter	Description	Configuration Method
Multi-camera Default Layout/Camera Layout	<p>Configures the camera layout during a video call.</p> <ul style="list-style-type: none"> • 1+N: the selected camera is given prominence in the largest pane. Other cameras are displayed in small panes. • Selected Speaker: the selected camera is seen in a large pane. • Equal N×N: every camera is given equal prominence in equal-sized panes. <p>Default: 1+N</p>	<p>Web User Interface</p> <p>Remote Control</p> <p>CP960 Conference Phone</p>

3. If you select **1+N** or **Selected Speaker** as the camera layout, you should choose a camera you want to focus on.

Using the CPW90 Wireless Microphones with VCS

CPW90 wireless microphones can work as the audio input devices of your video conferencing system. You can connect up to 2 CPW90 wireless microphones to the video conferencing system.

Registering CPW90 with VCS



If you purchase video conferencing system and wireless microphones together, they are already paired. Just turn the wireless microphones on to use them. Make sure a DD10 USB dongle is connected before you use the wireless microphones.

If you purchase wireless microphones separately, you need to pair them with video conferencing system manually.

Procedure

1. Connect the DD10 USB dongle to one of the USB ports on the video conferencing system.
2. Do one of the following:
 - On your web user interface, go to **Settings->Wireless Microphone->Search Mic**.

- On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone->Add Wireless Micphone.**
3. Place the wireless microphones on the charger and long press the mute button for 5 seconds until the mute LED indicator fast flashes yellow.

The wireless microphones are paired with the video conferencing system. And the  (unregistered) icon on the status bar will change to  (registered).

Deregistering CPW90 from VCS

Procedure

1. Do one of the following:
 - Remove the DD10 USB dongle.
 - On your web user interface, go to **Setting->Wireless Micphone->Deregistration.**
 - On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone.** Select a wireless microphone and then select **Unbind.**

Viewing CPW90 Information

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Wireless Micphone.**
 - On your remote control, go to **More->Status->Wireless Micphone.**
2. You can view the following information:
 - Register Status
 - MIC Model
 - MICROPHONE IPEI
 - Battery Status
 - Idle Time (estimated standby time)
 - Work Time (estimated working time)

Finding the Registered CPW90

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Wireless Micphone->Find.**
 - On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone.**

Select a wireless microphone and then select **Find**.

The mute indicator LED on the CPW90 flashes red and green alternately.

2. Stop finding.

Using the CPW90 Wireless Microphones with CP960

CPW90 wireless microphones can work as the audio input devices of your CP960 video conference phone. You can connect up to 2 CPW90 wireless microphones to the CP960 video conference phone.

Registering CPW90 with the CP960

If you purchase CP960 conference phone and wireless microphones together, they are already paired. Just turn the wireless microphones on to use them.

If you purchase wireless microphones separately, you need to pair them with CP960 conference phone manually.

Procedure

1. On your CP960 conference phone, go to **Settings->Wireless Microphone**.
2. Tap **Searching new MIC** to search for a CPW90.
3. Turn on the CPW90.
The CPW90 enters the registration mode automatically. And the mute indicator LED on the CPW90 fast flashes yellow.
4. The CPW90 registers with the CP960 conference phone automatically.
If the registration is successful, the mute indicator LED on the CPW90 goes out and the touch screen of CP960 conference phone prompts the CPW90 information: battery, work time and standby time.

Note

You can register up to two wireless expansion microphones to a CP960 conference phone.

Deregistering CPW90 from the CP960 Conference Phone

Procedure

1. On your CP960 conference phone, go to **Settings->Wireless Microphone**.
2. Select the desired microphone, and then tap **Detail**.
3. Tap **Unbind** to deregister the CPW90.

Viewing CPW90 Information

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Wireless Micphone**.
 - On your remote control, go to **More->Status->Wireless Micphone**.
 - On your CP960 conference phone, go to **Settings->Wireless Microphone->Detail**.
2. You can view the following information:
 - Register Status
 - MIC Model
 - MICROPHONE IPEI
 - Battery Status
 - Work Time (estimated working time)
 - Standby Time (estimated standby time)

Finding the Registered CPW90

Procedure

1. On your CP960 conference phone, tap **Settings->Wireless Microphone**.
2. Select the desired microphone, and then tap **Find**.

The mute indicator LED on the CPW90 flashes red and green alternately.
3. Tap **Exit**.

Using the CPW90-BT Bluetooth Wireless Microphones with VCS

CPW90-BT Bluetooth wireless microphones can work as the audio input devices of your video conferencing system. You can connect up to 2 CPW90-BT Bluetooth wireless microphones to the video conferencing system.

Registering CPW90-BT with VCS


If you purchase video conferencing system and Bluetooth wireless microphones together, they are already paired. Just turn the Bluetooth wireless microphones on to use them. If the model of your videoconferencing system is VC500/VC800/VC880, make sure a BT42 Bluetooth USB Dongle is connected before you use the Bluetooth wireless microphones.

If you purchase Bluetooth wireless microphones separately, you need to pair them with video

conferencing system manually.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Settings->Wireless Micphone->Search Mic**.
 - On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone->Add Wireless Micphone**.
2. Place the Bluetooth wireless microphones on the charger and long press the mute button for 5 seconds until the mute LED indicator fast flashes yellow.

The Bluetooth wireless microphones are paired with the video conferencing system. And the (unregistered) icon on the status bar will change to  (registered).



Deregistering CPW90-BT from VCS

Procedure

1. Do one of the following:
 - For VC500/VC800/VC880, remove the BT42 Bluetooth USB Dongle.
 - On your web user interface, go to **Setting->Wireless Micphone->Deregistration**.
 - On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone**.
Select a wireless microphone and then select **Unbind**.

Viewing CPW90-BT Information

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Wireless Micphone**.
 - On your remote control, go to **More->Status->Wireless Micphone**.
2. You can view the following information:
 - Register Status
 - MIC Model
 - MICROPHONE IPEI
 - Battery Status
 - Idle Time (estimated standby time)
 - Work Time (estimated working time)

Finding the Registered CPW90-BT

Procedure

1. Do one of the following:

- On your web user interface, go to **Setting->Wireless Micphone->Find**.
- On your remote control, go to **More->Setting->Video & Audio->Wireless Micphone**.
Select a wireless microphone and then select **Find**.

The mute indicator LED on the CPW90-BT flashes red and green alternately.

2. Stop finding.

System Maintenance

Topics:

[Exporting or Importing Configuration Files](#)

[Rebooting the System](#)

[Resetting the SD Card](#)

[Resetting the System](#)

[System Log Files](#)

[Packets Capture](#)

[System Firmware](#)

[License](#)

The following topics describe system maintenance, such as how to set up a system profile, perform a factory restore, and upgrade the system firmware.

Exporting or Importing Configuration Files

You can export configuration file(s) to check the current configuration of the system and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration.

Exporting BIN Files from the System

Procedure

1. On your web user interface, go to **Settings->Configuration->Export Configuration**.
2. Click **Export** to open the file download window, and then save the file to your computer.

Importing BIN Files to the System

Procedure

1. On your web user interface, go to **Settings->Configuration->Export Configuration**.
2. Click **Browse** to locate a BIN configuration file from your computer.
3. Click **Import** to import the configuration file.

Rebooting the System

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Upgrade->Reboot**.
 - On your remote control, go to **More->Setting->Advanced->Reboot & Reset->Reboot**.

Resetting the SD Card

You can reset SD card (local storage) of VC200 video conferencing endpoint to clear all captured screenshots and recorded videos.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Setting->Upgrade->Reset Built-in SD Card**.
 - On your remote control, go to **More->Setting->Advanced->Reboot & Reset->Reset Built-in SD Card**.

Resetting the System

Generally, some common issues may occur while using the system. You can reset your system and camera to factory configurations after you have tried all troubleshooting suggestions, but do not solve the problem.

Resetting the System using Configuration Methods

If you use configuration methods to reset your system, the system, the CP960 conference phone (if connected) and VCC22 video conferencing camera (if connected) are reset synchronously.

Procedure

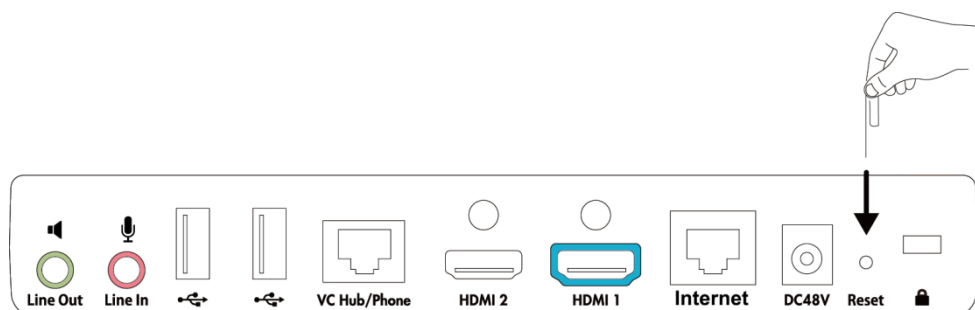
1. Do one of the following:
 - On your web user interface, go to **Setting->Upgrade->Reset to Factory Setting**.
 - On your remote control, go to **More->Setting->Advanced->Reboot & Reset->Reset**.

Resetting the System using Reset Button

If you use the reset button to reset your system, the system, the CP960 conference phone (if connected) and VCC22 video conferencing camera (if connected) are reset synchronously.

Procedure

1. On your video conferencing system or the VCC22 video conferencing camera, using tiny object (for example, the paper clip) to press and hold the reset button for 15 seconds until the monitor turns black.



Take VC800 as an example

Note

Do not power off the system when resetting the factory settings.

System Log Files

System log files are essential when troubleshooting the system issues. System log files contain information about system activities and the system configuration profile.

You can choose to generate the log files on your system (local logging) or sent local files to the syslog server in real time (syslog logging).

Configure System Log Level

You can determine the log level before exporting it.

Procedure

1. On your web user interface, go to **Setting->Configuration->System Log Level**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
System Log Level	Specify the system log level. 0 -system is unusable 1 -action must be taken immediately 2 -critical condition 3 -error conditions 4 -warning conditions 5 -normal but significant condition	Web User Interface

Parameter	Description	Configuration Method
	<p>6-informational</p> <p>Default: 6</p> <p>Note: Higher value indicates more detailed content.</p>	

Local Logging

You can choose to generate the log file on your system, and export it to your computer if necessary.

Exporting the Log Files to a Local Computer

Procedure

1. On your web user interface, go to **Setting->Configuration->Export System Log**.
2. Mark the **Local** radio box in the **Export System Log** field.
3. Click **Export** to open the file download window, and then save the file to your local system.

Viewing the Log Files

You can verify whether you got the correct log through the following key fields:

- <0+emerg>
- <1+alert>
- <2+crit>
- <3+error>
- <4+warning>
- <5+notice>
- <6+info>

The default local log level is 6.

The following figure shows a portion of a h323ptrace0.log file:

```
02/01 00:00:03.917 tlibthrd.cxx(519) PTLib Started thread 0x1dd84480 (2477) H323 Cleaner:0xb69e4460
02/01 00:00:11.410 h323pluginmgr.cxx(749) PLUGIN Unable to read default options
02/01 00:00:11.411 h323pluginmgr.cxx(749) PLUGIN Unable to read default options
02/01 00:00:11.443 h323pluginmgr.cxx(2951) H323PLUGIN Media format G.728 already exists
02/01 00:00:11.443 h323pluginmgr.cxx(2951) H323PLUGIN Media format G.729 already exists
02/01 00:00:11.492 sockets.cxx(131) Socket SetDefaultIpAddressFamilyV4
02/01 00:00:11.493 tlibthrd.cxx(429) ---thread create pipe 14 , 15
02/01 00:00:11.493 osutil.cxx(204) PwLib File handle high water mark set: 15 Thread unblock pipe
02/01 00:00:11.493 tlibthrd.cxx(439) PTLib Created thread 0x1dd4268 H323 Listener:%0x
02/01 00:00:11.495 sockets.cxx(2424) PIPSocket SetExtNetWork addr: 0.0.0.0
02/01 00:00:11.495 sockets.cxx(1694) Socket Listen for addr: 0.0.0.0
02/01 00:00:11.496 osutil.cxx(204) PwLib File handle high water mark set: 16 PTCPSocket
02/01 00:00:11.497 h323ep.cxx(1392) H323 Started listener Listener[ip$*:1720]
02/01 00:00:11.498 tlibthrd.cxx(608) PTLib Thread high water mark set: 3
02/01 00:00:11.498 h4601.cxx(1781) H460 Endpoint Attached
02/01 00:00:11.501 tlibthrd.cxx(519) PTLib Started thread 0x1dd4268 (8961) H323 Listener:b699b460
02/01 00:00:11.501 transports.cxx(1233) H323 Awaiting TCP connections on port 1720
02/01 00:00:11.502 transports.cxx(1182) TCP Waiting on socket accept on ip$*:1720
02/01 02:37:24.533 h323ep.cxx(2665) H323 Cleaning up connections
02/01 02:37:24.533 h323ep.cxx(1403) H323 Removing listener
02/01 02:37:24.544 tlibthrd.cxx(429) ---thread create pipe 16 , 19
```


Syslog Logging

You can also configure the system to send syslog messages to a syslog server in real time.

You should specify the IP address or host name of the syslog server.

Exporting the Log Files to a Syslog Server

Procedure

1. On your web user interface, go to **Setting->Configuration->Export System Log**.
2. Mark the **Server** radio box in the **Export System Log** field.
3. Enter the IP address or domain name of the syslog server in the **Server Name** field.
4. Click **Export**.

Viewing the Syslog Messages on Your Syslog Server

You can view the syslog file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the syslog:

```
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > PhoneStatusBar( 837): updateNotificationShade
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > CommonWork( 837): onNoticeCountChange 3
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > KeyguardUpdateMonitor( 837): received broadcast android.intent.action.PHONE_STATE
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > VolumePanel.15b7c48d( 837): onVolumeChanged(streamType: STREAM_VOICE_CALL, flags: 4096=FLAG_HIDE_UI)
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > VolumePanel.15b7c48d( 837): resetTimeout at 1517563864586 delay=3000 touchExploration=false
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > KeyguardUpdateMonitor( 837): received broadcast android.intent.action.PHONE_STATE
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > KeyGuardDelegate( 837): mIsInIdle true
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > CommonWork( 837): enableAccountLabel true
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > StatusBar( 837): hello world
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > PhoneStatusBar( 837): updateNotificationShade
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > CommonWork( 837): onNoticeCountChange 2
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > KeyGuardDelegate( 1022): mIsInIdle true
Feb 2 17:31:04 CP960 ap1c[609]: ANDR<6+info > WarningView( 1022): com.android.yealink.ShowTitleShowTitle falseSetTitleString null
```

Packets Capture

You can capture packets in three ways: capturing the packets via web user interface, remote control or using the Ethernet software. Engineers can analyze the packet captured for troubleshooting purpose.

Capturing the Packets via Web User Interface

You can capture packets via web user interface and then export it to the computer.

Procedure

1. On your web user interface, go to **Setting->Configuration**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Packet Capture Count	Configures the count of the number of packets to capture. Default: 5	Web User Interface
Packet Capture Device	Configures the port where you want to capture packets: <ul style="list-style-type: none"> • WAN—capture packets of the wired network. • ext0—capture packets of the CP960 conference phone. • wlan0—capture packets of the wireless network. Default: WAN.	Web User Interface
Packet Capture Clip Bytes	Configures the number of bytes (in kb) of the packet to capture. Default: 1024	Web User Interface
Pcap Filter Type	Configures the filter type of the packet to capture. Valid Values: <ul style="list-style-type: none"> • Custom—Customize the packet filter string. • SIP or H245 or H225—Capture SIP, H245 and H225 packets. • RTP—Capture RTP packets. Default: Custom	Web User Interface
Packet Filter String	Customizes the packet filter string. Syntax: Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression Protocol: Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used. Direction: Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2". Host(s):	Web User Interface

Parameter	Description	Configuration Method
	<p>Values: net, port, host, portrange.</p> <p>If no host(s) is specified, the "host" keyword is used.</p> <p>For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1".</p> <p>Logical Operations:</p> <p>Values: not, and, or.</p> <p>Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right.</p> <p>For example:</p> <p>"not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23".</p> <p>"not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)".</p> <p>Example: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8</p> <p>Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8.</p> <p>Default: Blank</p> <p>Note: It only works if the parameter "Pcap Filter Type" is set to Custom.</p>	

3. Click **Confirm**.
4. Click **Start** to start capturing signal traffic.
5. Reproduce the issue to get stack traces.
6. Click **Stop** to stop capturing.
7. Click **Export** to open the file download window, and then save the file to your computer.

Capturing the Packets via Web User Interface

You can customize the packet filter string to capture the desired packets.

Syntax:

Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression

The following table introduces the syntax.

Syntax	Description
Protocol	Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

Syntax	Description
	Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used.
Direction:	Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2".
Host(s):	Values: net, port, host, portrange. If no host(s) is specified, the "host" keyword is used. For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1".
Logical Operations:	Values: not, and, or. Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right. For example: "not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23". "not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)".

Example: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8

Packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8.



Capturing the Packets via Remote Control

You can capture the packets via remote control, and store the packets to the USB flash driver.

Before You Begin

If you want to save packets to the USB flash driver, make sure a USB flash drive is connected, and the USB feature is enabled.

Procedure

1. Long press  when the system is idle or during a call.
The monitor prompts "Onekey-capture has been turned on, press the Backspace key for 2s to turn off it".
2. Long press  for 2 seconds to stop capturing packets.
The packets are saved in the yealink.debug folder on your USB flash driver.

Related Topic:

Configuring USB Storage

Capturing the Packets via Ethernet Software

If your computer installs an Ethernet software (for example: Sniffer, Ethereal or Wireshark software), you can use it capture packets.

Procedure

1. Connect the Internet ports of your system and your computer to the same HUB, and then use Ethernet software to capture the signal traffic.

System Firmware

The newly released firmware version may add new features. Because of this, Yealink recommends you to update the latest firmware.

The following table lists the associated and latest firmware name for each system model (X is replaced by the actual firmware version).

Model	Firmware Name	Example
VC200 video conferencing endpoint	80.x.x.x.rom	80.32.0.3.rom
VC880 video conferencing system	63.x.x.x.rom	63.32.0.3.rom
VC800 video conferencing system		
VC500 video conferencing endpoint		
VCC22 video conferencing camera		
CP960 video conference phone	73.x.x.x.rom	73.80.0.65.rom
WPP20 Wireless Presentation Pod	81.x.x.x.rom	81.10.0.1.rom

You can download the latest firmware online:

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

Upgrading Firmware

You can upgrade firmware of the system and accessories.

Note

Do not close and refresh the browser when the system is upgrading firmware via web user interface.
Do not unplug the network cables and power cables when the system is upgrading firmware.

Procedure

1. On your web user interface, go to **Setting->Upgrade**.

2. In the corresponding field, click **Browse** to locate the firmware from your PC.
3. Click **Upgrade** to upgrade the firmware.

License

Importing Device Type License

If your system is a demo machine, namely it is used by agents to demonstrate system functions to the customers. The monitor will prompt "DEMO ONLY, NOT FOR RESELL".

A DEMO machine supports 24 ways multipoint calls (an original caller and 24 other sites). You can change the demo machine to be a normal machine by importing a device type license. After changing to a normal machine, the system supports one video call and five voice calls (an original caller and six other sites).

Procedure

1. On your web user interface, go to **Security->License**.
2. Click **Browse** to locate the device type license (the file format must be *.dat) from your local system.
3. Click **Upload** to import the device type license.

Viewing Device Type

Procedure

1. Do one of the following:
 - On your web user interface, go to **Security->License**.
 - On your remote control, go to **More->Status->License**.

- On your CP960 conference phone, go to **Settings->Status**.

Parameter	Description	Configuration Method
Device Type	Indicates your system is a demo machine or normal machine. <ul style="list-style-type: none"> • Demo machine • Normal Machine 	Web User Interface Remote Control CP960 Conference Phone

Multipoint License

You can use your VC880/VC800 system to participate in multipoint video conferences. Multipoint video conferences require a multipoint license. Multipoint license is not applicable to VC500/VC200 endpoint.

Maximum connections of the multipoint licenses are described as below:

Multipoint License Type	Maximum Connections	Description
VC200/VC500/VC880/VC800 without a multipoint license	One video call with a presentation and 5 voice calls (a conference moderator and 6 participants).	Multipoint video conferences are unsupported.
VC880/VC800 with a trial multipoint license	24 ways video call with a presentation (a conference moderator and 24 participants)	Period of validity: 15-day free trial VC880/VC800 models can use this trial multipoint license. You can download it from Yealink website.
VC880/VC800 with an 8 ways multipoint license	8 ways video call with a presentation and 5 voice calls (a conference moderator and 13 participants).	Period of validity: Eternal You need to contact Yealink resellers to purchase it, please provide the MAC address of your VC880/VC800 when purchasing.
VC880/VC800 with a 16 ways multipoint license	16 ways video call with a presentation and 5 voice calls (a conference moderator and 21 participants).	
VC880/VC800 with a 24 ways multipoint license	24 ways video call with a presentation (a conference moderator and 24 participants)	

Importing Multipoint License

Procedure

1. On your web user interface, go to **Security->License**.

2. Click **Browse** to locate the multipoint license (the file format must be *.dat) from your local system.
3. Click **Upload** to import the multipoint license.

Viewing Multipoint License Status

Procedure

1. Do one of the following:
 - On your web user interface, go to **Security->License**.
 - On your remote control, go to **More->Status->License**.
 - On your CP960 conference phone, go to **Settings->Status**.

Parameter	Description	Configuration Method
Multipoint Status	Indicates whether a multipoint license has been imported to the system or not. <ul style="list-style-type: none"> • Active • Inactive (without a multipoint license or the imported multipoint license has expired) 	Web User Interface Remote Control CP960 Conference Phone
Multipoint Ways	Indicates the multipoint license imported to the system. <ul style="list-style-type: none"> • Unsupported • 8 Ways • 16 Ways • 24 Ways 	Web User Interface Remote Control CP960 Conference Phone
Period of validity/ Period	Indicates the validity period of the imported multipoint license. <ul style="list-style-type: none"> • Unsupported • X~Y Available • Eternal 	Web User Interface Remote Control CP960 Conference Phone

Note

Upgrading the system or performing a factory reset will not affect the imported multipoint license.

If the system has been imported a trial multipoint license and the license has not expired, and you import a permanent multipoint license to the system, the permanent multipoint license will overwrite the trial multipoint license.

If the system has been imported a permanent multipoint license, and you import a trial multipoint license to the system, the permanent multipoint license will not be overwritten.

If you import a new permanent multipoint license to the system, the previous permanent multipoint license will be overwritten.

Trouble Shooting

Topics:

[General Issues](#)

[Call Issues](#)

[Audio Issues](#)

[Video Issues](#)

[Placing a Test Call](#)

[LED Instructions](#)

[System Diagnostics](#)

[System Status](#)

[Viewing Call Statistics](#)

When your system is unable to operate properly, you need to troubleshoot issues.

Make sure that the system is not physically damaged when experiencing a problem. Check whether the cables are loose and the connections are correct or not.

General Issues

Symptom	Reason	Solution
Your system does not respond to the remote control.	The remote control battery is dead.	Replace batteries.
	The remote control battery is installed incorrectly.	Installed batteries correctly.
	Aim the remote control at the wrong direction.	Aim the remote control at the sensor when you perform a task.
	You may control the far-site camera during a call.	Ensure that you are controlling the near-site camera.
	There are some objects are obstructing the sensor on the front of the camera.	Ensure that no objects are obstructing the sensor on the front of the camera.
	The remote control is broken.	Replace remote control.
You forget the administrator password for the system	You cannot access the advanced settings.	Reset your system.
Time and date is	The system fails to obtain the time and date	Contact your network

Symptom	Reason	Solution
wrong	from the SNTP server automatically.	administrator. Configure the time and date manually.
You cannot adjust the camera angle and focus	The local image is not selected.	Select local image using your remote control before adjusting camera.
	The system is in the operation menu.	Adjust the camera when the system is idle or during a call.
	The remote control is not working.	Check the remote control.
How to prevent monitor burn-in?	Ensure that static images are not displayed for long periods. Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.	Configure the automatic sleep time or screen saver.
	Unsuitable monitor parameters.	Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

Call Issues

Symptom	Reason	Solution
You cannot receive calls.	The network is unavailable.	Contact network administrator.
	Your system cannot receive calls when the far site dials your account, check whether your account is registered.	Register an account.
	DND (Do Not Disturb) mode is enabled.	Disable DND.
You fail to call far site.	Far site enables DND (Do Not Disturb) mode.	Contact the far site to disable DND.
	Account is not registered	Both sites register an account.
	Fail to dial the IP address of the far site.	At least one call protocol(SIP/H.323) is enabled.
		Ping the IP address of the far site. If it fails, contact the network administrator.
	The far site is powered off.	Contact the far site to power on the system.
	The call protocol(SIP/H.323) that far site uses is	Both sites use the same call protocol

Symptom	Reason	Solution
	different from yours.	(SIP/H.323).
	Encryption negotiation (SRTP/H.235) fails.	If one site is forced to use encryption, ensure that the other site enables encryption too.
	The firewall blocks the traffics.	Open necessary ports on the firewall.
	Your monitor prompts: Call Fail Busy Here. <ul style="list-style-type: none"> Far site rejects your SIP call. Far site does not answer your SIP call. Far site has reached maximum sessions when you place a SIP call. 	Contact the far site.
	Your monitor prompts: Call Fail Remote endpoint refused call. <ul style="list-style-type: none"> Far site rejects your H.323 call Far site does not answer your H.323 call. Far site has reached maximum sessions when you place an H.323 call. 	Contact the far site.
	Your monitor prompts: Network disconnected	Check the network connection.
	Your monitor prompts: Maximum number of sessions reached.	Maximum sessions is depend on the multipoint license imported to the system.

Audio Issues

Symptom	Reason	Solution
You cannot hear audio during a call.	Volume is set to 0.	Adjust volume.
	Far site mutes the microphone.	Contact the far site to check whether the microphone is unmuted.
You cannot hear clear audio during a call.	Volume is too low.	Adjust volume.
	Muffled audio reception from the far site may be caused by highly reverberant rooms.	Contact the far site to speak in close proximity to the phone.
	You choose a low-bandwidth audio codec.	Adjust the priority order of your audio codec.
	Noise devices, such as computers or fans.	Enable noise suppression.

Symptom	Reason	Solution
	Dust and debris may cause audio quality.	Do not use any kind of liquid or aerosol cleaner on the phone. A soft, slightly damp cloth should be sufficient to clean the top surface of the phone if necessary.
Far site cannot hear your audio during a call.	No audio input device.	Audio input device is connected correctly.
	Speaker of far site is obscured or damaged.	Ensure that speakers are not obscured or damaged. Do not stack items on top of the CP960 conference phone.
	Your microphone is muted.	Unmute the microphone..
	Volume of far site is set to 0.	Contact the far site to adjust volume.
You may experience poor voice quality during a call, such as intermittent voice, echo or other noise.	Users sit too far from or near to the microphone.	Adjust distance.
	The audio pickup device is moved frequently.	Put the audio pickup device in the fixed location.
	Network congestion.	Connect the network administrator.
	Cable gets old.	Replace the old cables with the new cables, and then check whether the new cables provide better connectivity.
You cannot hear ring tone when receive a call.	Volume is set to 0.	Adjust volume.

Video Issues

Symptom	Reason	Solution
Picture is blank on the monitor.	The system is sleeping.	Press any key on the remote control to wake the system.
	The system is powered off.	Power on the system.
	The HDMI cable is not connected to the system.	Verify that the monitor is connected correctly according to the Quick Start Guide.
Video quality is poor	Unsuitable monitor resolution.	Adjust the monitor resolution.

Symptom	Reason	Solution
	Packet is lost.	View the call statistics to check whether the packet is lost and contact network administrator.
	Unsuitable camera parameters.	Adjust the camera parameters, such as brightness and white balance.
	High-intensity indoor light or direct sunlight on the camera	Avoid this.
You cannot share content.	PC is not connected.	Connect a PC to your system.
	The PC is turned off.	Turn on the PC.
	The VCH50 video conferencing hub or WPP20 wireless presentation pod is broken.	Replace it.
	The WPP20 wireless presentation pod cannot connect to the video conferencing system.	<ul style="list-style-type: none"> • Connect the WPP20 to the video conferencing system to obtain Wi-Fi profile. • Make sure the wireless AP feature of video conferencing system is enabled.
Far site displays black screen when you share content.	The reason may be that the remote device is placed in the private LAN and its negotiated media address in the signaling is different from its actual public IP address. If you share contents in this situation, the contents will be sent to the negotiated media address other than the actual public IP address. This may lead to failure.	<p>You can configure network address adapter to let the content send to the actual public IP address.</p> <p>Procedure:</p> <ol style="list-style-type: none"> 1. On your web user interface, go to Setting->Call Features->Network Address Adapter. 2. Select one the following settings: <ul style="list-style-type: none"> • Disabled- send contents to the negotiated media address. • IP Adapter-send contents to the actual public IP address. • Port Adapter- send contents to the actual public port. • IP & Port Adapter- send contents to the actual public IP address and port.

Placing a Test Call

When you finish installing and deploying the video conferencing system, you can call the Yealink Demo site (117.28.251.50 or 117.28.234.45) to test your setup.

System Diagnostics

You can diagnose the audio, camera and network.

Diagnosing the Audio

You can check whether the speaker connected to your system can pick up voice and play audio normally.


Procedure

1. On your remote control, go to **More->Setting->Diagnose->Audio Diagnose**.
2. Start the speaker test.
3. Adjust the volume of the speaker.
4. Select **Stop** to stop the speaker test.

Diagnosing the Camera

You can check whether the camera can pan and change focus normally.

Procedure

1. Do one of the following:
 - For VC880/VC800/VC500, on your remote control, go to **More->Setting->Diagnose->Camera Diagnose**.
 - For VC200, on your remote control, go to **More->Diagnose->Camera Diagnose**.
2. Press the navigation key to adjust the camera position.
3. Press the zoom out/in key to zoom out or zoom in.
If the camera can move and zoom normally, it means that the camera is working well.
4. Press  to stop camera diagnostics.

Diagnosing the Network

The wrong network settings may result in inaccessibility of your system and poor network performance. You can use the ping or trace route to troubleshoot network connectivity problems.

Checking the Network Using “Ping” Method

You can use Ping method to diagnose the network. It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Diagnose**.
Select **Ping** from the pull-down list of **Command**.
 - For VC880/VC800/VC500, on your remote control, go to **More->Setting->Diagnose->Ping**.
 - For VC200, on your remote control, go to **More->Diagnose->Ping**.
2. Select **Start**.
3. You can also ping other IP address.
4. Select **Stop**.

Checking the Network Using “Trace Route” Method

You can use trace route method to diagnose the network. If the test is successful, the system lists the hops between the system and the IP address you entered. You can check whether congestion happens by viewing the time cost between hops.

Procedure

1. Do one of the following:
 - On your web user interface, go to **Network->Diagnose**.
 - Select **Trace Route** from the pull-down list of **Command**.
 - For VC880/VC800/VC500, on your remote control, go to **More->Setting->Diagnose->Trace Route**.
 - For VC200, on your remote control, go to **More->Diagnose->Trace Route**.
2. Select **Start**.
3. You can also trace route of a desired IP address.
4. Select **Stop**.

System Status

You might need to provide system information, such as network settings and firmware for technical support.

System Status List

Parameter	Description	Method
System information	<ul style="list-style-type: none"> System model Firmware version Hardware version Product ID Version 	Web User Interface Remote Control CP960 Conference Phone
	<ul style="list-style-type: none"> Uptime 	Web User Interface
WPP20 Status (if WPP20 is connected)	<ul style="list-style-type: none"> Firmware Version 	Web User Interface
Network	<ul style="list-style-type: none"> Network Type Internet Port/IP Mode 	Web User Interface Remote Control
	<ul style="list-style-type: none"> Internet Port Type MAC address Internet Port Type/LAN type IP address Subnet mask Gateway DNS server Public IP address (if the static NAT is enabled) 	Web User Interface Remote Control CP960 Conference Phone
Network Common	<ul style="list-style-type: none"> Public IP Address MAC Address Wi-Fi MAC Address 	Web User Interface Remote Control
Wifi AP Status (if Wi-Fi AP is enabled)	<ul style="list-style-type: none"> AP Enable AP Name Security Mode Password Network Sharing Band Channel 	Web User Interface Remote Control
Account status	<ul style="list-style-type: none"> Register status of Cloud platform Register status of SIP account Register status of H.323 account Register status of PSTN account 	Web User Interface Remote Control CP960 Conference Phone

Parameter	Description	Method
Camera	<ul style="list-style-type: none"> Status Device model Specification Hardware version 	Web User Interface Remote Control CP960 Conference Phone
Audio	<ul style="list-style-type: none"> Active microphone Active speaker 	Web User Interface Remote Control CP960 Conference Phone
VCS Phone	<ul style="list-style-type: none"> Status 	Remote Control
	<ul style="list-style-type: none"> Device model Serial number, Firmware version Hardware version IP address MAC address 	Web User Interface Remote Control
Wireless Microphone	<ul style="list-style-type: none"> Register status Product model MICPOD IPEI Power percent Idle time work time 	Web User Interface Remote Control CP960 Conference Phone
License	<ul style="list-style-type: none"> Device Type Multipoint Status Multipoint Ways Period of validity 	Web User Interface Remote Control CP960 Conference Phone

Viewing System Status

Procedure

- Do one of the following:
 - On your web user interface, go to **Status**.
 - On your remote control, go to **More->Status**.
 - On your CP960 conference phone, go to **Settings**.
- Select the desired list to view the status.



Viewing Call Statistics

If voice quality is poor during a call, you can view call statistics to find out why.

Call statistics includes: codec, bandwidth, total packet lost and other parameters about presentation.

For example, when a delay occurs or the video has a 'mosaic' look, you can view the total packet loss to check whether the packet has been lost.

Procedure

1. Do one of the following during a call:
 - For VC880/VC800/VC500, on your web user interface, go to **Home**. For VC200, on your web user interface, go to **VC200**.
Hover your cursor over the desired far site, and click  .
 - On your remote control, press  or OK key to open **Talk Menu**, and select **Call Statistics**.
Press up or down key to view the call statistics of the desired far site.
 - On your CP960 conference phone, go to **More->Statistics**.
Tap the desired far site to view the call statistics.