Yealink

Full HD Video Conference System Administrator Guide

VC880

VC500/PVT950

VC200

PVT980

Version 40.10 | Apr.2019

Contents

About This Guide

Yealink administrator guide provides general guidance on configuring, customizing, managing, and troubleshooting video conferencing systems. This guide is not intended for an administrator who is experienced in system administration.

This guide is applicable to the following Yealink device:

- VC880 video conferencing system
- VC800 video conferencing system
- VC500 Pro video conferencing system
- VC500 video conferencing system
- VC200 video conferencing system
- PVT980 video conferencing system
- PVT950 video conferencing system

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	×	√

Note:

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

- *Related Documentations*

Related Documentations

The following related documents are available:

- Video conferencing System Quick Start Guide, which describes how to assemble the system and configure the conference room and the 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 the network for your systems.
- Yealink VCR11 Remote Control Quick Reference Guide, which describes how to use the VCR11 Remote Control.
- Yealink CPW90-BT Bluetooth Wireless Microphones Quick Start Guide, which describes how to connect CPW90-BT Bluetooth wireless microphones to the 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 the VCS codec to the wireless network and provide wireless AP via WF50.
- Yealink WPP20 Wireless Presentation Pod Quick Start Guide, which describes how to connect WPP20 wireless presentation pod to the VCS codec.

- 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 CTP20 Quick Start Guide, which describes how to connect CTP20 to the VCS codec.
- Yealink VCM34 Quick Start Guide, which describes how to connect VCM34 to the VCS codec.

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/?language=zh_cn.

Getting Started

This chapter introduces the basic operation of VCS.

- *Hardware Overview*
- *LED Instructions*
- *Powering On and Off*

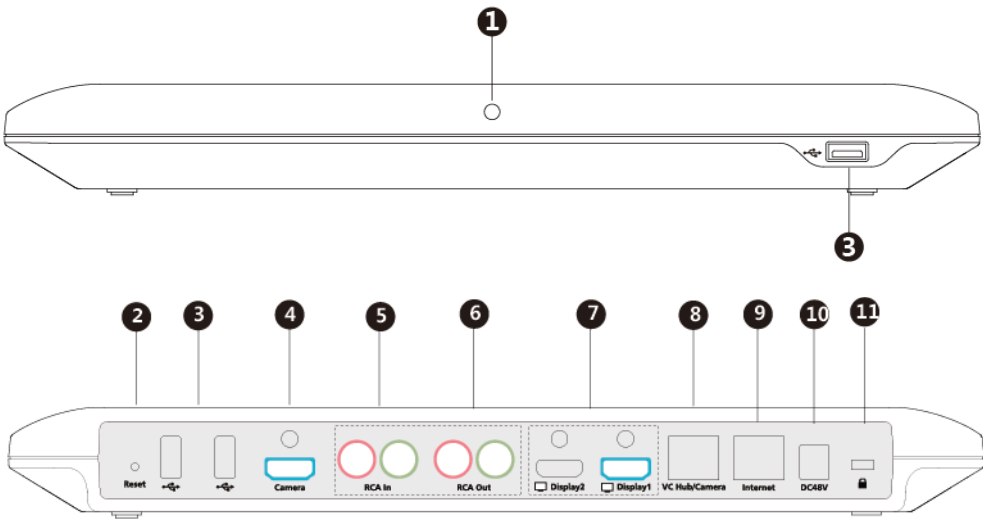
Hardware Overview

- *Hardware of VC880 Codec*
- *Hardware of PVT980 Codec*
- *Hardware of VC800 Codec*
- *Hardware of VC500/PVT950 Codec*
- *Hardware of VC200 Codec*
- *Hardware of VCC22 Video Conferencing Camera*
- *Hardware of VCH50 Video Conferencing Hub*
- *Hardware of CP960 Conference Phone*
- *Introduction of CTP20 Touch Panel*
- *Hardware of WPP20 Wireless Presentation Pod*
- *Hardware of CPE90 Wired Expansion Microphones*
- *Hardware of CPW90-BT Bluetooth Wireless Microphone*
- *Hardware of VCR11 Remote Control*

Hardware of VC880 Codec

With 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 spilt-type structure can meet the deployment requirement of the control room which separates from a large conference room.

The following introduces the corresponding ports on VC880.



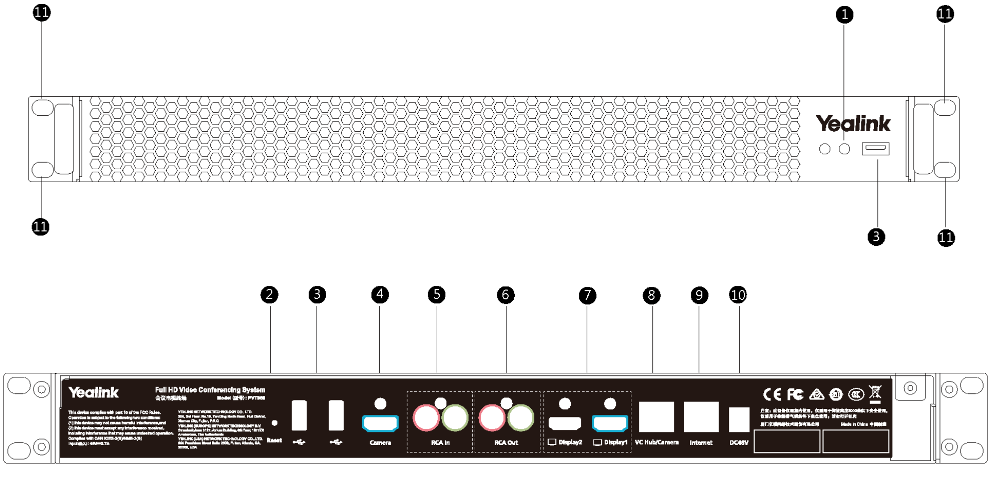
	Port Name	Description
①	LED Indicator	Indicate different status of the system.
②	Reset Key	Reset the system to factory defaults.
③	USB	• Connect to a USB flash drive. Insert a USB flash drive for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. • Insert a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
④	Camera Port	Connect to a third-party camera via an HDMI cable.
⑤	RCA In	Connect to an audio input device via a RCA cable.
⑥	RCA Out	Connect to an audio output device via a RCA cable.
⑦	Display	Connect to a monitor.

	Port Name	Description
⑧	VC Hub/Camera	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub. • Connect this port to the Camera port on theVCC22 video conferencing camera. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • It is used to connect to VCM34.
⑨	Internet	Connect to the network device.
⑩	DC48V	Connect to the power source via a power adapter.
⑪	Security Slot	Allow you to connect a universal security cable to the codec, so you can lock the codec down. The system cannot be removed when locked.

Hardware of PVT980 Codec

PVT980, targeted at large meeting room, is applicable to the meeting room with cabinet or the lecture hall. Owning rich physical interfaces for audio and video connection, PVT980 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.

The following introduces the corresponding ports on PVT980.



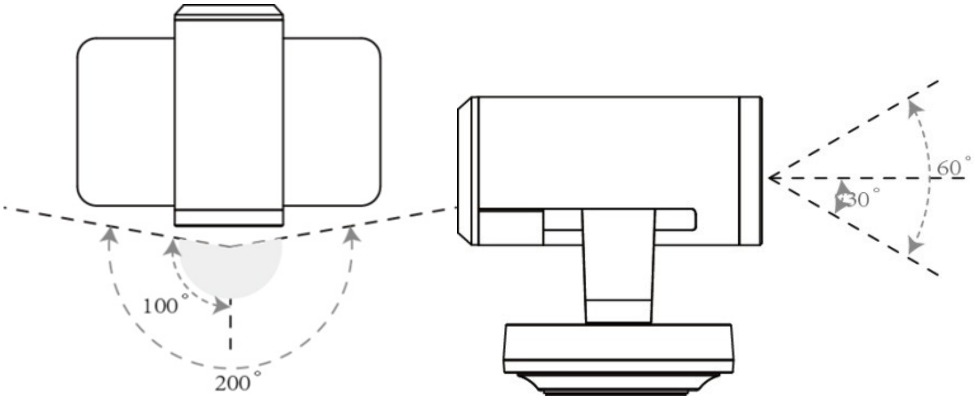
	Port Name	Description
①	LED Indicator	Indicate different status of the system.
②	Reset Key	Reset the system to factory defaults.

	Port Name	Description
③	USB	- Connect to a USB flash drive Insert a USB flash drive for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. - Insert a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. - Insert a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. - Insert a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
④	Camera Port	Connect to a third-party camera.
⑤	RCA In	Connect to an audio input device via a RCA cable.
⑥	RCA Out	Connect to an audio output device via a RCA cable.
⑦	Display	Connect to a monitor for displaying video images.
⑧	VC Hub/Camera	- If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub. - Connect this port to the Camera port on theVCC22 video conferencing camera. - If you need an audio device, connect this port to the Internet port on the CP960 Conference phone.
⑨	Internet	Connect to the network device.
⑩	DC48V	Connect to the power source via a power adapter.
⑪	Slot hole	Use the screws to lock the PVT980 system to the rack.

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*

- *Rear Panel of VC800 Codec*

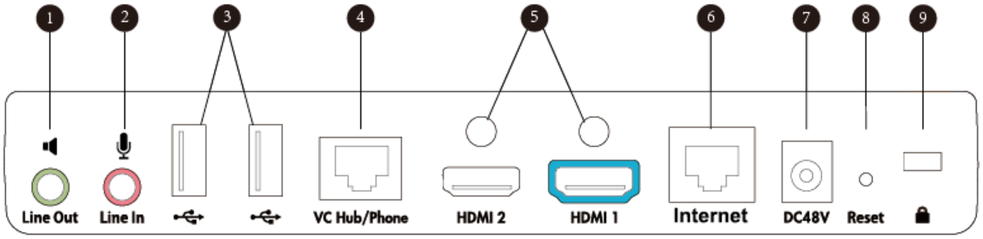
Front Panel of VC800 Codec

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

Related information

LED Instructions of VC880/VC800/VC500/VC200/PVT980/PVT950

Rear Panel of VC800 Codec



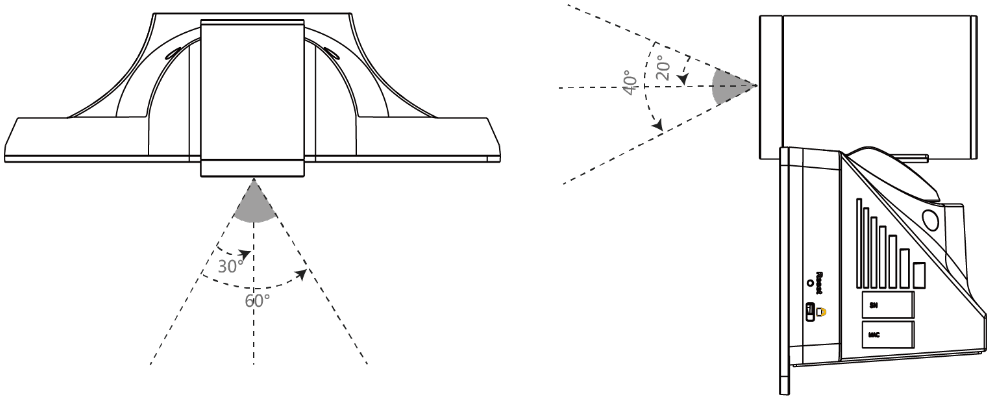
	Port Name	Description
①	Line Out	Connect to an audio output device via an audio cable (3.5mm).
②	Line In	Connect to an audio input device via an audio cable (3.5mm).
③	USB	• Connect to a USB flash drive. Insert a USB flash drive for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. • Insert a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
④	VC Hub/Phone	• If you want to use wired sharing to present, 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. • It is used to connect to VCM34.
⑤	HDMI	Connect to a monitor.
⑥	Internet	Connect to the network device.

	Port Name	Description
⑦	DC48V	Connect to the power source via a power adapter.
⑧	Reset Key	Reset the system to factory defaults.
⑨	Security Slot	Allow you to connect a universal security cable to the codec, so you can lock the codec down. The system cannot be removed when locked.

Hardware of VC500/PVT950 Codec

VC500/PVT950 codec compresses outgoing video and audio data, transmits this information to the far site, and decompresses incoming data.

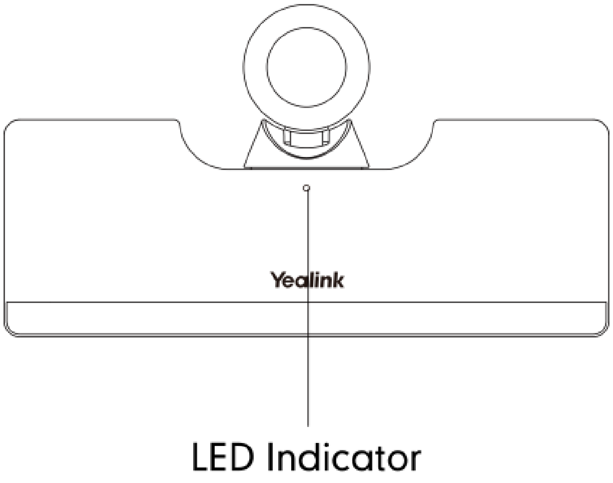
VC500/PVT950 codec, compatible with different audio devices, supports 16:9 and 4:3 aspect ratios and can adapt to the monitors automatically. The VC500/PVT950 camera can be panned (± 30 degrees range), tilted (± 20 degrees range) and support 5 x optical zoom, white balance and automatic gain.



- *Front Panel of VC500/PVT950 Codec*
- *Rear Panel of VC500/PVT950 Codec*

Front Panel of VC500/PVT950 Codec

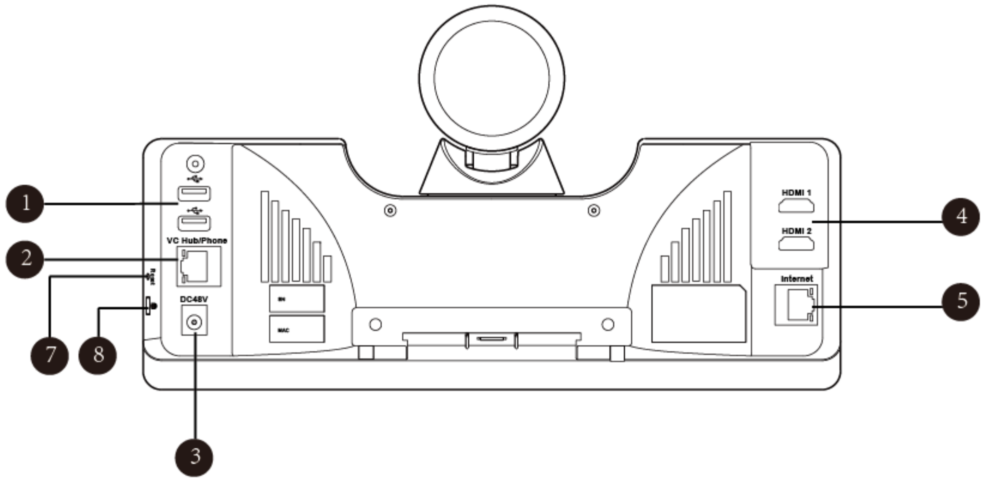
The LED indicator in front of the camera indicates different status of the endpoint.



Related information

LED Instructions of VC880/VC800/VC500/VC200/PVT980/PVT950

Rear Panel of VC500/PVT950 Codec



	Port Name	Description
①	USB	• Connect to a USB flash drive Insert a USB flash drive for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. • Connect to an audio input device via an USB to line input adapter. • Connect to an audio output device via an USB to line input adapter. • Insert a WF50 Wi-Fi USB Dongle for connecting Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
②	VC Hub/Phone	• If you want to use wired sharing to present, 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. • It is used to connect to VCM34. (It is not available to PVT950)
③	DC48V	Connect to the power source via a power adapter.
④	HDMI 1	Connect to a monitor for displaying video images.

	Port Name	Description
⑤	Internet	Connect to the network device.
⑥	Reset Key	Reset the system to factory defaults.
⑦	Security Slot	Allow you to connect a universal security cable to the codec, so you can lock the codec down. The system cannot be removed when locked.

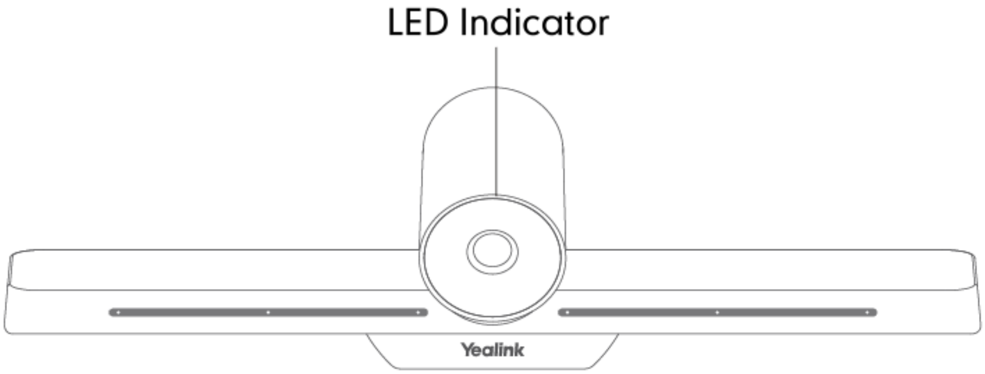
Hardware of VC200 Codec

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*
- *Rear Panel of VC200 Codec*
- *Bottom of VC200 Codec*

Front Panel of VC200 Codec

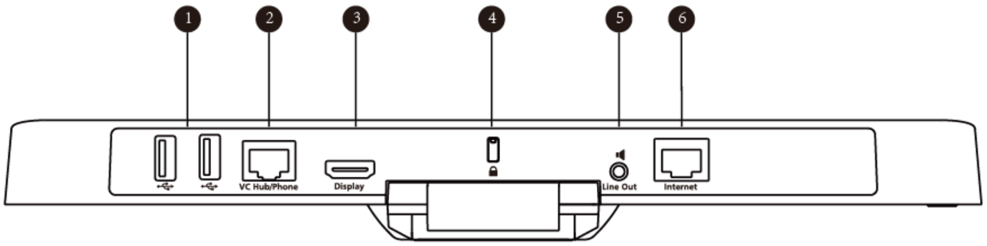
The LED indicator in front of the camera indicates different statuses of the endpoint.



Related information

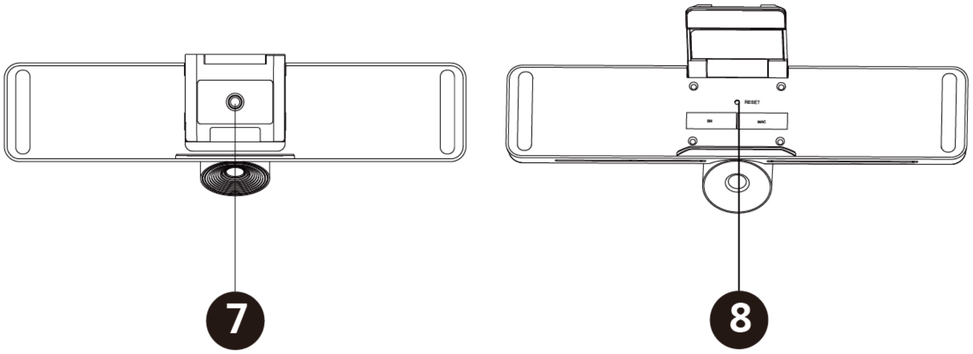
LED Instructions of VC880/VC800/VC500/VC200/PVT980/PVT950

Rear Panel of VC200 Codec



	Port Name	Description
①	USB	• Connect to a USB flash drive for storing screenshots, recording videos or capturing packets. If multiple USB flash drives are connected, only the latter one can be identified. • Insert a PSTN box CPN10 to connect to the PSTN (Public Switched Telephone Network).
②	VC Hub/Phone	• If you want to use wired sharing to present, 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. • It is used to connect to VCM34.
③	Display	Connect to a monitor.
④	Security Slot	Allow you to connect a universal security cable to the codec, so you can lock the codec down. The system cannot be removed when locked.
⑤	Line Out	Connect to an audio output device via an audio cable (3.5mm).
⑥	Internet	Connect to the PoE via the network cable.

Bottom of VC200 Codec

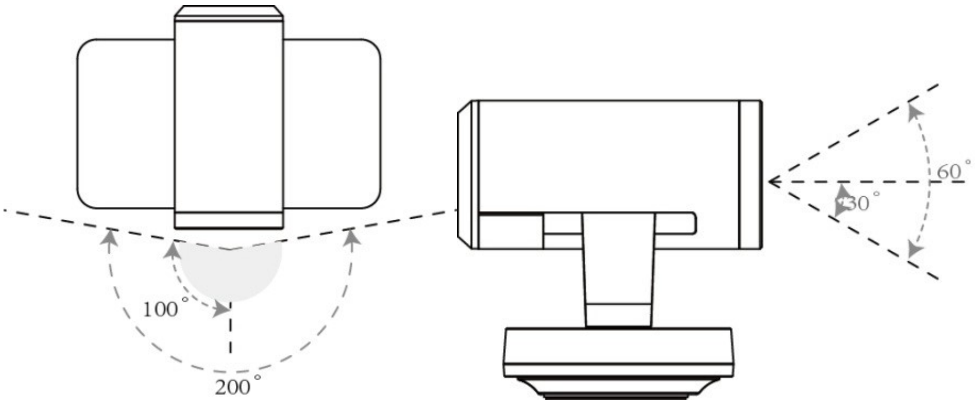


	Port Name	Description
⑦	VESA	Fix the endpoint to the TV stand or a tripod using a 1/4”-20 UNC screw.
⑧	Reset Key	Reset the system to factory defaults.

Hardware of VCC22 Video Conferencing Camera

VCC22 is a video conferencing camera for VC880/VC800/PVT980. It adopts 12x optical zoom lens, supports 1080P/60 frame full HD video, has OSMO and PTZ function, and processes professional video quality and environmental adaptability. You can connect up to 9 VCC22 video conferencing cameras to the VC880/PVT980 video conferencing system, and 8 to VC800 video conferencing system.

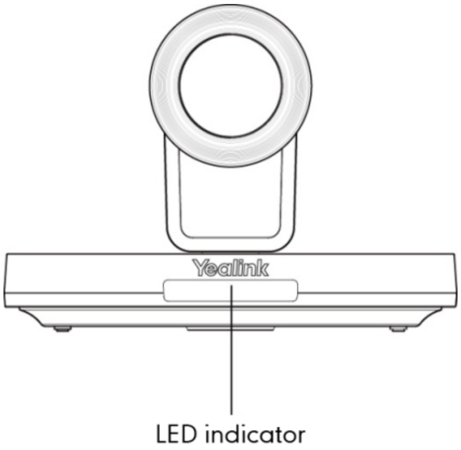
The VC800 camera can be panned (± 100 degrees range), tilted (± 30 degrees range) and supports 12 x optical zoom, white balance and automatic gain.



- *Front Panel of VCC22 Video Conferencing Camera*
- *Rear Panel of VCC22 Video Conferencing Camera*

Front Panel of VCC22 Video Conferencing Camera

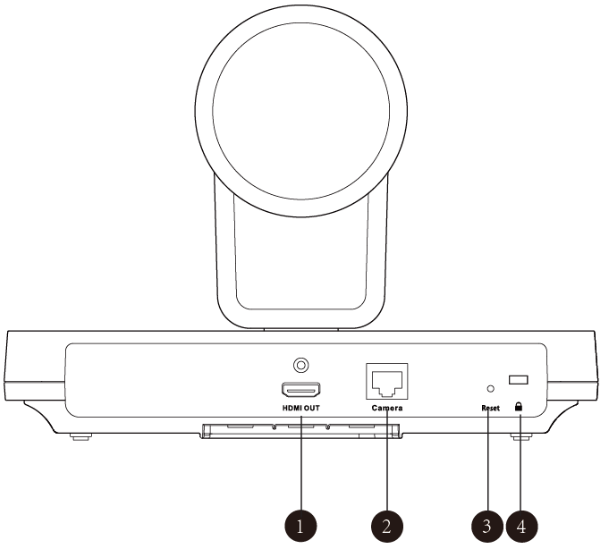
The LED indicator in front of the camera indicates different status of the endpoint.



Related information

LED Instructions of VCC22 Video Conferencing Camera

Rear Panel of VCC22 Video Conferencing Camera



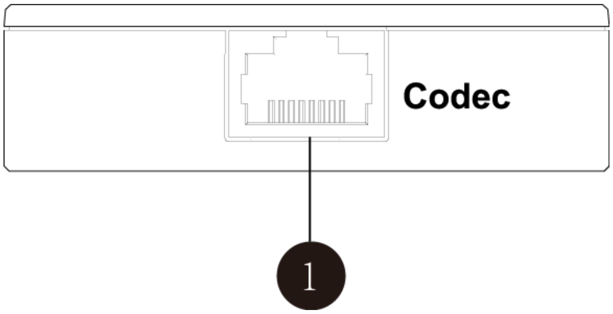
	Port Name	Description
①	HDMI Out	Connect to a monitor for displaying shared content.
②	Camera Port	Connect to a PoE switch.
③	Reset Key	Reset the camera to factory defaults.
④	Security Slot	Allow you to connect a universal security cable to VCC22, so you can lock it down. The camera cannot be removed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

Hardware of VCH50 Video Conferencing Hub

You can connect VCH50 to the computer for presenting. 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.

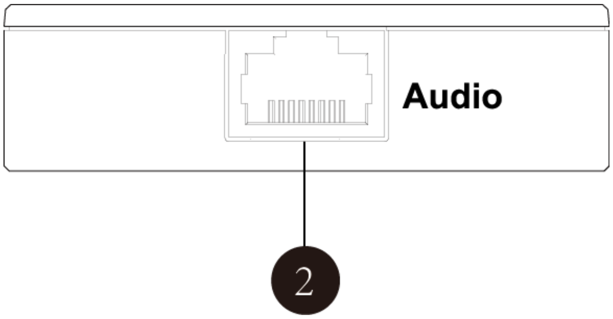
- *Left Side of VCH50 Cable Hub*
- *Right Side of VCH50 Cable Hub*
- *Rear Panel of VCH50 Cable Hub*

Left Side of VCH50 Cable Hub



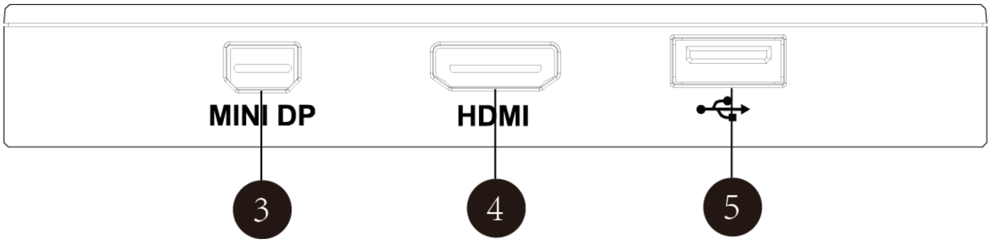
	Port Name	Description
①	Codec	Connect to the video conferencing system via the provided 7.5m network cable.

Right Side of VCH50 Cable Hub



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

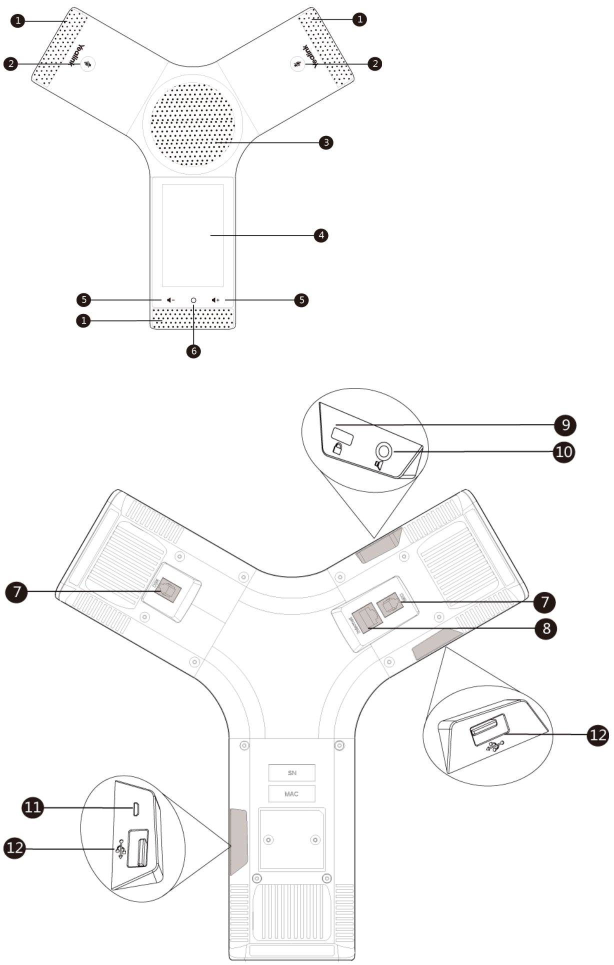
Rear Panel of VCH50 Cable Hub



	Port Name	Description
③	MINI DP	Connect to PC via Mini-DP cable for sharing contents.
④	HDMI	Connect to PC via HDMI cable for sharing contents.
⑤	USB	Connect to a USB flash drive Insert a USB flash drive for storing screenshots, recording videos or capturing packets.

Hardware of CP960 Conference Phone

You can use CP960 conference phone as a microphone and a speaker when you are using VC200/VC500/VC800/VC880/PVT980/PVT950 to place calls. You can also place calls, answer calls or view directory and history on the CP960 conference phone.

CP960 Conference Phone	NO.	Item	Description
 1 2 3 4 5 6 7 8 9 10 11 12 SN MAC	①	Three Internal Microphones	Support 360-degree audio pickup at a radius of up to 6 meters.
	②	Mute Button	• Indicate the status of the device and the call. • Toggle mute feature.
	③	Speaker	Provide audio output.
	④	Touch Screen	5 inch (720 x 1280) capacitive (5-point) touch screen.
	⑤	Volume Touch Keys	Adjust the volume of the speaker, ringer or media.
	⑥	HOME Touch Key	Return to the idle screen.
	⑦	Wired Mic Ports	Allow you to connect CPE90 to your phone (optional).
	⑧	Internet Port	• 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	Allow 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.

CP960 Conference Phone	NO.	Item	Description
	⑪	Micro USB Port	This port is unavailable when CP960 conference phone works with the video conferencing system.
	⑫	USB Port	• Connect a USB flash drive to store screenshots, recording videos or captured packets. • Connect to the mini USB port on the charge cradle to charge the CPW90 wireless expansion microphones. If multiple USB flash drives are connected, only the latter one can be identified.

Related information

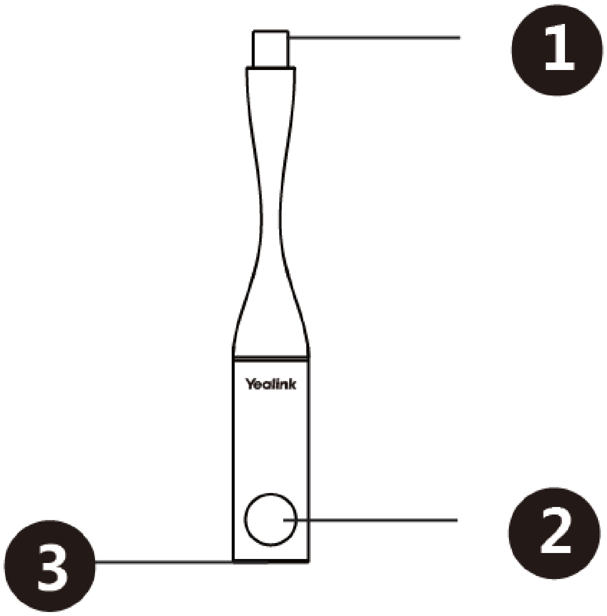
LED Instructions of CP960 Conference Phone

Introduction of CTP20 Touch Panel

As the controller of VCS devices, CTP20 touch panel can help you fully control VC200/VC500/VC800/VC880 system. You can use it to place calls, initiate conferences, adjust the volume, control the camera, record videos, and so on. What’s more, CTP20 supports collaborative editing and the note feature, that is to say, participants can add notes to the presentation or to the whiteboard, which can improve the communication efficiency of the traditional video conferencing presentation.

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.



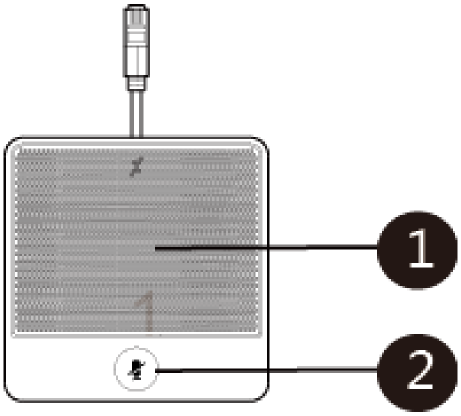
	Name	Description
①	USB	Connects to the video conferencing system to obtain Wi-Fi profile. Connects to the PC for sharing content.
②	Presentation button	Presses it to start or to stop sharing the full screen of the PC. Long presses it for 3 seconds and release it, and then choose the window you want to share.
③	LED Indicator	Indicates the status.

Related information

LED Instructions of WPP20 Wireless Presentation Pod

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.



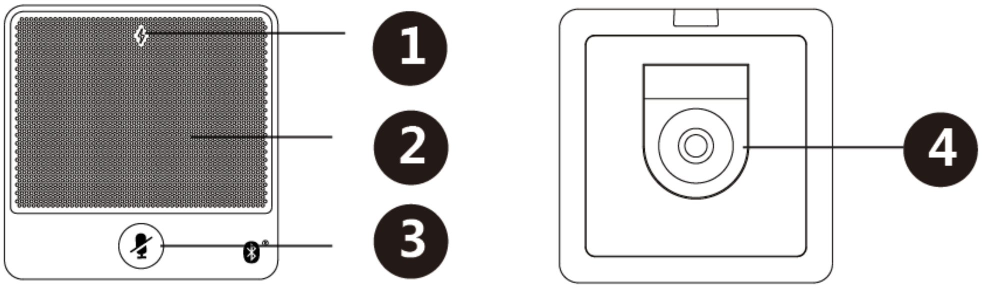
	Name	Description
①	Built-in Microphones	Supports 360-degree audio pickup at a radius of up to 3 meters.
②	Mute Button	• Indicates call status. • Toggles mute feature.

Related information

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.



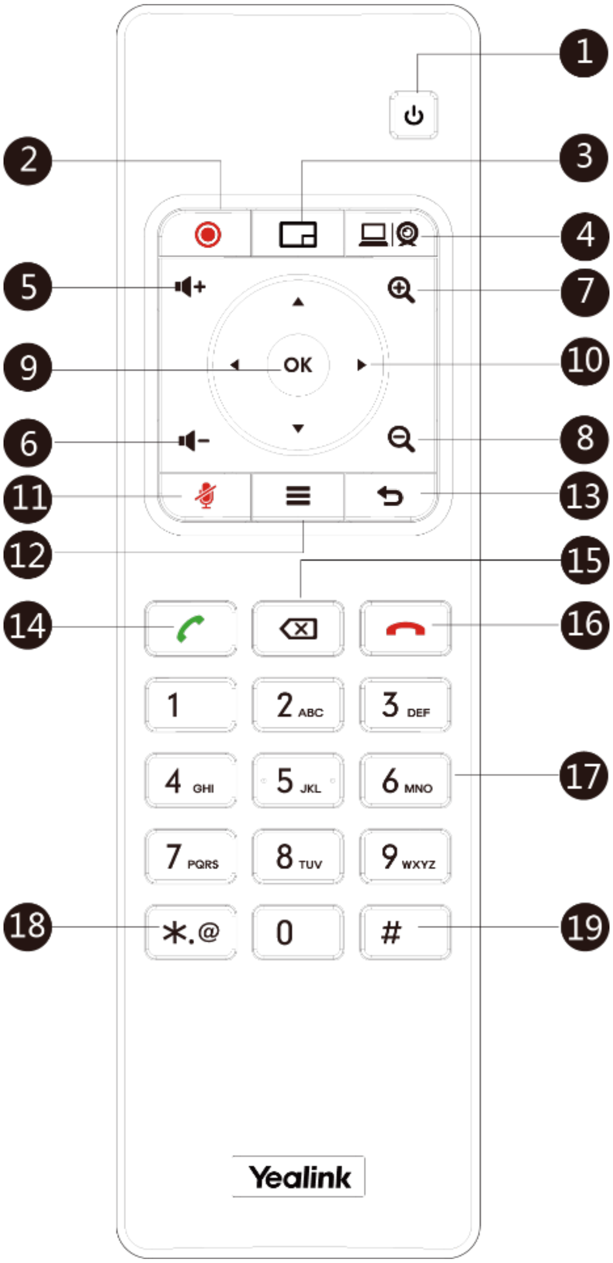
	Name	Description
①	Battery Indicator LED	Indicates the battery information.
②	Built-in Microphones	Supports 360-degree audio pickup at a radius of up to 3 meters.
③	Mute Button	• Indicates call status. • Toggles mute feature.
④	Charging Slot	Put the CPW90-BT on the charging cradle to charge.

Related information

LED Instructions of CPW90-BT Bluetooth Wireless Microphones Battery Indicator LED

Hardware of VCR11 Remote Control

The VCR11 remote control enables you to operate a video conferencing system. This includes placing the ongoing calls, adjusting specify the volume, controlling the camera, navigating screens, and more. The following table introduces the keys on the remote control.



NO.	Item	Description
1	Switch	• Power the system on and off. • Put the system to sleep or wakes the system.
2	Video recording key	Start or stop recording the video and audio.
3	Layout key	Adjust the layout during a video call.
4	Customization key	Customize the key function. This key can be configured as the Presentation key (default), the Input key, the ScreenShot key or Mute Speaker key.
5	Volume up key	Increase the speaker volume.

NO.	Item	Description
6	Volume down key	Decrease the speaker volume.
7	Zoom in key	• Increase the focal length of the camera. • Zoom in the screenshot. • Turn the page up.
8	Zoom out key	• Decrease the focal length of the camera. • Zoom out the screenshot. • Turn the page down.
9	OK key	Go the sub-menu, confirm actions or answer incoming calls.
10	Arrow key	• Navigate through menu items. • Pan and tilt the camera to adjust the viewing angle.
11	Mute key	Toggle the mute feature.
12	Home key	• Return to the idle screen when the device is not in a call. • Open the Talk Menu during a call.
13	Return key	Return to the previous menu.
14	Dial key	Enter the pre-dialing screen, the dialing screen or the answering screen.
15	Delete key	• Delete the text. Delete one character at a time. Long press to delete all characters in the input field. • One touch to capture packets. When the device is connected to the USB flash drive, long press it for 2 seconds to start capturing packets and long press it for 2 seconds again to stop capturing packets.
16	Hang up key	• End a call or exits a conference call. • Return to the idle screen.
17	Numeric keypad	• Enter digits. • Go to the pre-dialing screen.
18	Asterisk key	Enter the special characters: .@*.
19	Pound key	Enter the pound key (#).

Related information

Using VCR11 Remote Control

LED Instructions

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

- *LED Instructions of VC880/VC800/VC500/VC200/PVT980/PVT950*
- *LED Instructions of VCC22 Video Conferencing Camera*
- *LED Indicator of CTP20*
- *LED Instructions of CP960 Conference Phone*
- *LED Instructions of CPE90 Wired Expansion Microphones*
- *LED Indicators of CPW90-BT Bluetooth Wireless Microphones*
- *LED Instructions of WPP20 Wireless Presentation Pod*

LED Instructions of VC880/VC800/VC500/VC200/PVT980/PVT950

LED Status	Description
Solid green	The system is powered on.
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/PVT980 system is powered on.
	The VC880/VC800/PVT980 is upgrading firmware.
	The VCC22 video conferencing camera is working.
Solid red	The VC880/VC800/PVT980 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 Indicator of CTP20

LED Status	Description
Solid green	VCS codec is powered on.
Solid red	CTP20 is in sleep mode.
Solid orange	CTP20 is not connected to VCS codec.

LED Instructions of CP960 Conference Phone

LED Status	Description
Solid red	The CP960 conference phone is initializing.

LED Status	Description
	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 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 CP960 conference phone is idle.
	The CPE90 is disconnected to CP960 Conference Phone.

LED Indicators of CPW90-BT Bluetooth Wireless Microphones

- *LED Instructions of CPW90-BT Bluetooth Wireless Microphones Battery Indicator LED*
- *LED Instructions of CPW90-BT Bluetooth Wireless Microphones Mute Indicator LED*

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 and the battery indicator LED on the CPW90-BT is still off, it means the CPW90-BT is turned off.

LED Instructions of CPW90-BT Bluetooth Wireless Microphones Mute Indicator LED

LED Status	Description
Slowly flashing yellow	The CPW90-BT is searching for signal.
Fast flashing yellow	The CPW90-BT is in the pairing mode.
Solid red	The system is muted.
Solid green	The system can pick voice.
Slowly flashing red	The system is receiving an incoming call.
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 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*
- *Powering Off the System*
- *Initialization Process Overview*

- *Configuration Methods*

Powering On the System

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

Procedure

On your remote control, press ⏻.
Your system is powered on successfully, and the LED indicator illuminates solid green.

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 goes out.

Initialization Process Overview

The initialization process of the system is responsible for network connectivity and the 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*
- *Configuring the VLAN*
- *Querying the DHCP (Dynamic Host Configuration Protocol) Server*
- *Running the Setup Wizard*

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 rest, navigate the screens and perform the required steps to configure the system.

Tip:

You can run the setup via your remote control or CTP20.

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

You can configure following features according to the setup wizard.

Menu	Description
Language	Set the language displayed on the CP960 conference phone/CTP20/the monitor. The default language is Simplified Chinese.
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	The default administrator password is “0000”. For security reasons, you should change it as soon as possible. The new password must be at least six characters, preferably mixing with digits and letters.
Firewall Port Mapping	Displays the firewall port mapping 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/Yealink Meeting Server/StarLeaf/Zoom/Pexip/BlueJeans/EasyMeet/Custom platform.

Configuration Methods

You can configure your system via web user interface, VCR11 remote control, CTP20 or CP960 conference phone.

- *Using Web User Interface*
- *Using VCR11 Remote Control*
- *Using CTP20 Touch Panel*
- *Using 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 into the Web User Interface*
- *Configuring the Web Server Type*

Logging into the Web User Interface

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

Note: We recommend that you use the Chrome or Internet Explorer 11 to access the web user interface. Some features may not work properly if you are using other or older browser.

1. Open a web browser and enter the device IP address in the address bar.
2. Enter the administrator username and the password.
3. Click **Login**.

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

Related tasks

Configuring the Web Server Type

Related information

User and Administrator

Configuring the Web Server Type

The 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/PVT980/PVT950: 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **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 by using the HTTP protocol. **Default**: On.	Web user interface Remote control CTP20
HTTP Port	Specifies the HTTP port for the user to access the system’s the web user interface. **Valid value**: Any integer from 1 to 65535. Ensure that the configured port is not occupied. **Default**: 80	Web user interface
HTTPS	Enables or disables the user to access the system web user interface by using the HTTPS protocol. **Default**: On.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
HTTPS port	Specifies the HTTPs port for the user to access the system's the web user interface. **Valid value**: Any integer from 1 to 65535. Ensure that the configured port is not occupied. **Default**: 443	Web user interface
HTTP & HTTPS	Enables or disables the user to access the web user interface via the HTTP and HTTPS protocol. **Default**: On.	CTP20
Off	Disables the user to access the web user interface via the HTTP and HTTPS protocol. **Default**: Off.	CTP20

Using VCR11 Remote Control

You can use the real remote control or virtual remote control to configure and use the system. You can disable the remote control if it is not needed or not available.

- *Using the Virtual Remote Control*
- *Customizing the Key Type*
- *Disabling Remote Control Keys*
- *Disabling the Remote Control*

Using the Virtual Remote Control

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

Procedure

1. On your web user interface, go to **Home** > **Remote Control**.
   The virtual remote control appears.
2. Click the corresponding keys on the remote control to control the system.
3. Click **Remote Control** to close the virtual remote control.

Customizing the 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** > **Remote Control** > **Custom Key Type**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Custom Key Type	Specifies a feature for the custom key on the remote control. • **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. **Default**: Presentation.	Web user interface

Disabling Remote Control Keys

All keys on the remote control are enabled by default. If you do not want to use some keys on the remote control, you can disable them.

Procedure

1. On your web user interface, go to **Setting** > **Remote Control**.
2. In the **Enable Remote Control Key** field, turn off the corresponding key.
3. Click **Confirm**.

Disabling the Remote Control

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

Procedure

1. On your web user interface, go to **Setting** > **General** > **General Information** > **Remote Control Enabled**.
2. Configure and save the following setting:

Parameter	Description	Configuration Method
Remote Control Enabled	Select Off to disable the remote control. **Note**: the default value is **On**. If you select Off, you cannot use the remote control or the virtual remote control to control the system.	Web user interface

Using CTP20 Touch Panel

You can use CTP20 Touch Panel to configure and control VCS. For more information about CTP20 Touch Panel, refer to *Yealink CTP20 Quick Start Guide*.

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

This chapter introduces how to deploy VCS.

- *Traditional Deployment Methods*
- *Cloud Deployment Method*

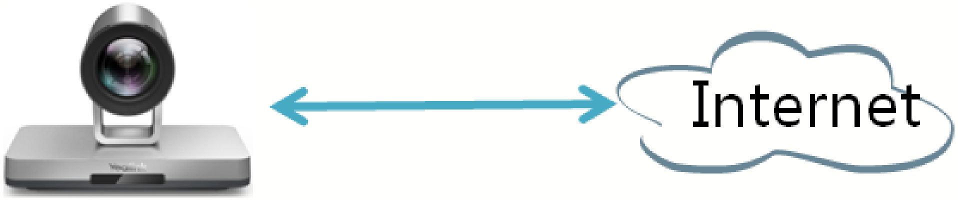
Traditional Deployment Methods

If you do not use cloud-based service, you can choose the traditional deployment method to deploy your VCS.

- *Public IP Configuration*
- *Port Forwarding*
- *NAT*
- *STUN*
- *H.460*
- *Intelligent Traversal*
- *VPN*

Public IP Configuration

For a higher demand of the audio and video, you can connect your video conferencing system 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 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
H.323	1719-1720	UDP/TCP

Description	Port Range	Port Type
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 information

NAT

NAT

Many application-layer protocols, for example multimedia protocols (H.323/SIP), have the address or the 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 the address and the port of application-layer protocols, which guarantees the accuracy of the communication in the application layer.

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 the address and the 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* .

- *Configuring NAT*
- *Enabling Static NAT for SIP Calls*
- *Route Traversal*

Configuring NAT

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **NAT/Firewall** > **NAT Configuration**.
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **NAT/Firewall** > **NAT**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static NAT/Type	Specifies the static NAT type. • **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. **Default**: Off.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
NAT Public IP Address/Public IP Address	• 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.	Web user interface Remote control CTP20

Related tasks

Enabling Static NAT for SIP Calls

Related information

Port Forwarding

Enabling Static NAT for SIP Calls

You can use H.323 protocol to make private-to-public calls after you configure the port forwarding and enable the static NAT feature. If you want to use SIP protocol to make private-to-public calls, you also need to enable the static NAT settings for the SIP protocol.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **NAT Traversal**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **SIP IP Call** > **NAT Traversal**.
   - On your CTP20, tap **Setting** > **Advanced** > **SIP IP Call** > **NAT Traversal**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select the static NAT.	Web user interface Remote control CTP20

Related tasks

Configuring NAT

Related information

Port Forwarding

Route Traversal

In the intranet, if there is 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 the 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.

Attention:

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

- *Route Traversal*

Route Traversal

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **NAT/Firewall** > **NAT Configuration**.
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **NAT/Firewall** > **NAT**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static NAT/Type	Select Manual/Manual Settings, and then configure the NAT address manually.	Web user interface Remote control CTP20
NAT Public IP Address/Public IP Address	Configures the NAT address for the system manually.	Web user interface Remote control CTP20
Route Traversal	Configures the route traversal type. • **Auto**—NAT works only when making a call to a public address. NAT does not work when making a call to a private address. • **Compulsion**—NAT works whatever 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 *Enabling Static NAT for SIP Calls* .

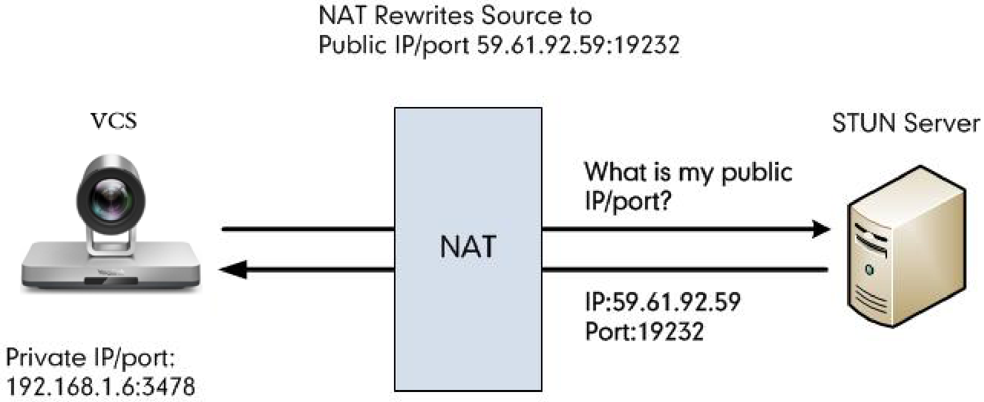
STUN

If you want to use the VCS system in the intranet to place calls to the VCS system in the extranet, you can use STUN server, as well as configure ALG on the router or enable static NAT on the system.

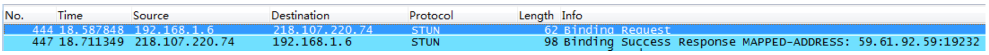
The STUN is a tool, which allows the system behind a NAT to first discover the presence of a NAT, and then the mapped public IP address, and the port number that the NAT has allocated for the UDP flows to remote parties. Those information is used to establish UDP communication between two system behind the NATs.

STUN is a client/server protocol. The system works as a STUN client, sending exploratory STUN messages to the STUN server, and then, the STUN server uses those messages to determine the public IP address and the port (which is used to connect the public network to the intranet), 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 the mapped IP address and the port are placed in the Binding Response: Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232.



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



```
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
```

Note:

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

- *Configuring STUN*
- *Selecting STUN for SIP Calls*

Configuring STUN

Procedure

1. Do one of the following:

- On your web user interface, go to **Network** > **NAT/Firewall** > **STUN Config**.
- 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**.
- On your CTP20, tap **Setting** > **Advanced** > **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**: Off.	Web user interface Remote control CTP20
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 CTP20

Parameter	Description	Configuration Method
STUN port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Default**: 3478.	Web user interface Remote control CTP20

Selecting STUN for SIP Calls

If you want to make private-to-public calls via SIP protocol, you can enable STUN feature for SIP protocol.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **NAT Traversal**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **SIP IP Call**.
   - On your CTP20, tap **Setting** > **Advanced** > **SIP IP Call** > **NAT Traversal**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select STUN.	Web user interface Remote control CTP20

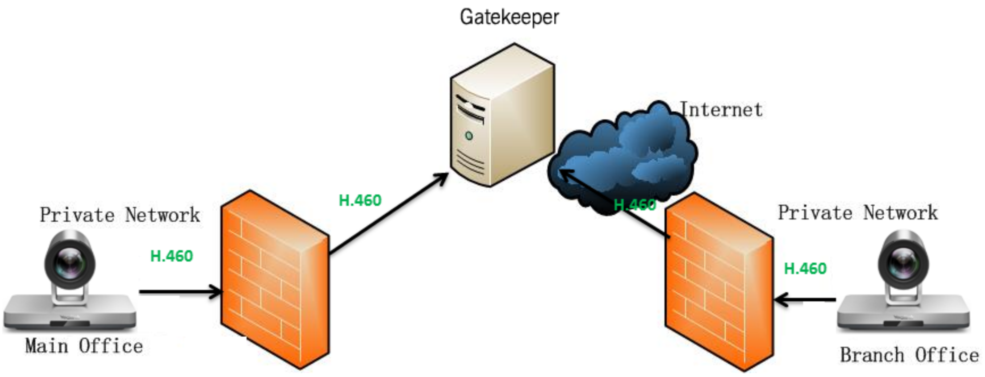
Related tasks

Configuring SIP Settings

Configuring NAT

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 the static NAT settings automatically.

- *Configuring H.460 for H.323 Calls*

Configuring H.460 for H.323 Calls

If you want to make private-to-public calls via H.323 protocol, you can enable H.460 feature for H.323 protocol.

Procedure

1. 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 Active**.
   - On your CTP20, tap **Setting** > **Advanced** > **H.323** > **H.460**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.460 Active	Enables or disables H.460 firewall traversal for H.323 calls. **Default**: Off.	Web user interface Remote control CTP20

Related tasks

Configuring H.323 Settings

Intelligent Traversal

Some branch offices lack IT professionals, which means that professional network configuration (for example: port forwarding) is impossible. To solve this issue, Intelligent Traversal allows you to simply deploy your VCS in the intranet, and assign an IP address to VCS, which can be used to access the public network. After that you can place calls to the VCS in the public network via your intranet VCS.

Although this method is not applicable to the incoming calls.

- *Audio & Video Intelligent Traversal*
- *Data Intelligent Traversal*

Audio & Video Intelligent Traversal

When a VCS in the intranet calls the VCS in the public network, the audio & video streams send by the VCS in the intranet may carry the intranet IP addresses, as a result, the VCS in the public network fails to send the audio& video streams to the VCS in the intranet. Besides, the problem of one-way audio or video and no image of the VCS in the public network may occurs to the VCS in the intranet. The above problems can be solved by the feature of audio & video intelligent traversal.

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

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

The VCS A locates in the intranet with the feature of audio & video intelligent traversal enabled, 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 will send RTP data to the negotiated IP address of A (private IP address provided in the Session Description Protocol), as a result, A may see 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*

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 settings:

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 with 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. Therefore, the VCS B can share content normally.

- *Configuring Data Intelligent Traversal*

Configuring Data Intelligent Traversal

Procedure

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

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

The VPN (Virtual Private Network) technology establishes a private tunnel on the public network through key exchange, encapsulation, authentication and encryption, to ensure the integrity, privacy, and validity of the transmitted data. Yealink video conferencing system uses OpenVPN to achieve VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before the 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 with the VPN server.

For more information, refer to *OpenVPN Feature on Yealink IP Phones*.

- *Related VPN Files*
- *Configuring VPN*

Related VPN 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 directories of the OpenVPN certificates, the key and the configuration file:

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

Configuring VPN

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **VPN**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Advanced Network** > **VPN**.

     For VC200: on your remote control, go to **More** > **Network** > **Wired Network** > **NAT/Firewall** > **VPN**.
   - On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **VPN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active **VPN**	Enables or disables VPN feature on the system. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Upload VPN Config	Uploads the compressed package of VPN-related files (*.tar) to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Cloud Deployment Method

When holding a video conference, customers may 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 changes in the way of organizational communication. With video conference platform, organizations can communicate easily because the public IP address and the complex network settings are unnecessary. Challenges such as infrastructure costs and interoperability are also eliminated. Both the head office and the branch offices can use the cloud deployment method. Besides, both the inbound and the outbound calls are available.

Configuring System Settings

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

- *Configuring Network Settings*
- *Configuring Account Settings*
- *Configuring the Video Conference Platform*
- *Configuring General Settings*
- *Configuring the Audio Settings*
- *Configuring Video Settings*
- *Configuring Content Sharing*
- *Configuring Camera Settings*
- *Call Settings*
- *Configuring the Conference Room*
- *Configuring the Security Features*
- *Managing the Directory*
- *Managing the Call Log*
- *Placing a Call*

Configuring Network Settings

The following introduces how to configure network settings.

- *IPv4 and IPv6 Network Settings*
- *DHCP Options*
- *VLAN*
- *Wi-Fi*
- *Wireless Access Point*
- *802.1x Authentication*
- *Network Speed and Duplex Mode*
- *Restricting Reserved Ports*
- *Quality of Service (QoS)*
- *Adjusting MTU of Data Packets*

IPv4 and IPv6 Network Settings

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

Note:

Yealink video conferencing systems comply with the DHCPv4 specifications documented in *RFC 2131*, and the DHCPv6 specifications documented in *RFC 3315*.

- *IP Addressing Mode Configuration*
- *Configuring IPv4*
- *Configuring IPv6*

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**.
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wired Network** > **IP Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
IPv4/IPv6/IP Mode	Configures the IP address mode. **Note**: the default mode is IPv4. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Configuring IPv4

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

Ensure that your network 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 VC200: on your remote control, go to **More** > **Network** > **Wired Network** > **IPv4**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired 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. **Note**: the default value is **On**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Static IP	Enables or disables the system to use manually configured network settings. **Note**: the default value is **Off**. 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. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Subnet Mask	Configures the subnet mask assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Gateway	Configures the gateway assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Static DNS	Enables or disables DNS feature. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Primary DNS/DNS primary Server	Configures the primary DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Secondary DNS/DNS Secondary Server	Configures the secondary DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Configuring IPv6

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.

Before you begin

Ensure that your network mode is set to IPv6 or IPv4&IPv6.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **LAN Configuration** > **IPv6 Config**.
   - 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wired Network** > **IPv6**.
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 **Note**: the default value is **On**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Static IP	Enables or disables the system to manually configured IPv6 network settings. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
IP address	Configures the IPv6 address assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
IPv6 prefix((0~128)/ **IP prefix**	Configures the IPv6 prefix. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Gateway	Configures the IPv6 default gateway. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Static IPv6 DNS/ **Static DNS**	Enables or disables the static IPv6 DNS feature. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Primary DNS/DNS primary Server	Configures the primary IPv6 DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Secondary DNS/DNS Secondary Server	Configures the secondary IPv6 DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

DHCP Options

The DHCP information with labels carries with the corresponding network and other control information. The information is called option. After connected to the network, the device will broadcast the DISCOVER request which carries the DHCP options of the network information. The DHCP server will replay the corresponding option after receiving the request.

Note:

For more information on DHCP options, refer to *RFC 2131* or *RFC 2132*.

- *Supported DHCP Option for IPv4*
- *DHCP Option 42, Option 2*
- *DHCP Option 12*

Supported DHCP Option for IPv4

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

Parameter	DHCP Options	Description
Subnet Mask	1	Specify the client’s subnet mask.
Time Offset	2	Specify the offset of the client's subnet in seconds from the 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.

Parameter	DHCP Options	Description
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.
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 tasks

NTP Settings

DHCP Option 12

You can specify a hostname for the system when using DHCP. When the system sends the request of DHCP DISCOVER, it will report the configured host name to the DHCP server via DHCP option 12. For more information, refer to *RFC 1035*.

- *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 settings:

Parameter	Description	Configuration Method
Host Name	Configures the host name of the system. **Note**: When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12. For more information, contact the network administrator. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

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*
- *Configuring VLAN Manually*
- *Configuring DHCP VLAN*

Configuring LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the systems to receive (transmit) the device-related information from (to) the directly connected devices that also uses the protocol on the network, and to store the information about other devices.

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

- *Configuring LLDP*

Configuring LLDP

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **Advanced** > **LLDP**.
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **LLDP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active	Enables or disables the LLDP feature on the system. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Packet Interval(1-3600s)	Configures the interval (in seconds) for the system to send LLDP requests. **Default**: 60 seconds. The value can be any integer from 1 to 3600. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

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

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **VLAN** > **Internet Port**.
   - 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **VLAN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active	Enables or disables VLAN for the Internet port. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
VID(1-4094)	Specifies the identification of the Virtual LAN. **Note**: the default value is 1. The value can be any integer from 1 to 4094. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Priority	Configures the VLAN priority. **Note**: the default value is 0. The value can be any integer from 0 to 7. The smaller the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

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 (it should be predefined on the DHCP server first) by default. The administrator 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	Enables or disables the DHCP VLAN discovery feature on the system. **Note**: the default value is **On**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
Option	Configures the DHCP option from which the system obtains the VLAN settings. You can configure at most 5 DHCP options and separate them by commas. **Note**: the value can be any integer from 128 to 254. **Default**: 132. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Wi-Fi

For VC880/VC800/VC500/PVT980/PVT950: 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*
- *Viewing the Wireless Network Status*
- *Forgetting a Wi-Fi Connection Profile*
- *Disabling the Wi-Fi Feature*

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.

Note: If you connect the codec to the wireless network via CTP20, make sure that CTP20 is wired to the codec.

- *Connecting to the Wireless Network*
- *Connecting to a Hidden Wireless Network*

Connecting to the Wireless Network

You can manually connect your phone to a wireless network.

Procedure

1. Do one of the following:
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wi-Fi**.

     For VC200: on your remote control, go to **More** > **Network** > **Wi-Fi**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless Network**.
2. Enable **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. Do one of the following:

- If you use the remote control, select the corresponding Wi-Fi (SSID), and press OK.

  If the network is secure, enter its password in the **Password** field, and select **Join to Network**.
- If you use CTP20, select the corresponding Wi-Fi (SSID).

  If the network is secure, enter its password in the **Password** field, and tap **Join to Network**.

Connecting to a Hidden Wireless Network

Some wireless networks do not broadcast their SSIDs, which makes them unavailable to find. In order to connect to one of those networks, you need to connect to one of them manually.

Procedure

1. Do one of the following:
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wi-Fi**.

     For VC200: on your remote control, go to **More** > **Network** > **Wi-Fi**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless Network**.
2. Enable **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. Enter the name of the wireless network.
6. Select the desired value from the drop-down menu of **Security Mode**.
7. Configure the corresponding parameters.
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**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wi-Fi** > **Wi-Fi Status**.

     For VC200: on your remote control, go to **More** > **Network** > **Wi-Fi** > **Wireless Status**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless Network** > **Wireless Status**.
2. View the detailed wireless network information (for example, SSID or the signal strength).

Forgetting a Wi-Fi Connection Profile

The system will automatically save the Wi-Fi that has been connected ever. If you are connected to a wireless network and would no longer like to connect to it automatically, you can choose to forget it. Next time you need enter the Wi-Fi password to connect the Wi-Fi.

Procedure

1. Do one of the following:
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wi-Fi**.

     For VC200: on your remote control, go to **More** > **Network** > **Wi-Fi**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless Network**.
2. If you use the remote control, select the desired Wi-Fi and press OK.

If you use the CTP20, Tap the desired network.

3. Select **Forget the Network**.

Disabling the 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**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wi-Fi**.

     For VC200: on your remote control, go to **More** > **Network** > **Wi-Fi**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless Network**.
2. Disable the Wi-Fi.

Wireless Access Point

For VC880/VC800/VC500/PVT980/PVT950: you need to connect a WF50 Wi-Fi USB Dongle to the system for providing the wireless AP. For VC200: you can provide wireless AP directly.

- *Enabling the Wireless Access Point*
- *Configuring Wireless Access Point*
- *Viewing the Connected Devices*
- *Adding Connected Devices to the Blacklist*
- *Removing Devices from the Blacklist*
- *Disabling the Wireless Access Point*

Enabling the Wireless Access Point

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wireless AP**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wireless AP**.

     For VC200: on your remote control, go to **More** > **Network** > **Wireless AP**.
   - If CTP20 is wired to the device, on your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP**.
2. Enable the Wireless AP.
3. If you already enabled Wi-Fi, select OK to turn it off.

Configuring Wireless Access Point

You can configure the wireless access point for the devices.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wireless AP**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Wireless AP** > **Configure AP**.

     For VC200: on your remote control, go to **More** > **Network** > **Wireless AP** > **Configure AP**.
   - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP** > **Configure AP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
AP name	Configures the name of wireless AP.	Web user interface Remote control CTP20
Security mode	Configures the security mode of the wireless AP. • None • WPA2-PSK **Default**: WPA2-PSK.	Web user interface Remote control CTP20
AP Password	Configures the password of the wireless AP. **Note**: only when the security mode is WPA2-PSK do you need to configure this parameter.	Web user interface Remote control CTP20
Network Sharing	Enables or disables the system to share its wired network to the connected devices. • **On**—The connected devices can use an Internet connection. • **Off**—The connected devices cannot use an Internet connection. **Default**: Off.	Web user interface
Frequency	Configures the frequency of the wireless AP. • 2.4G • 5G **Default**: 5G.	Web user interface Remote control CTP20
Channel	Configures the channel of the wireless AP. **Default**: Auto.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
AP IP Address	Configures the generation type of wireless AP address. • **Auto**—generates the wireless AP address automatically. The default network segment is 192.168.144.X. • **Manual**—If automatically generated network segment conflicts with the one you use, you can change the network segment manually. **Default**: Auto.	Web user interface
IP address	Configures the IP address of the wireless AP. Only when the AP IP Address is manual do you need to configure this parameter.	Web user interface

Viewing the Connected Devices

Procedure

1. Do one of the following:
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP** > **AP Device List**.
2. View the names and the MAC addresses of the connected devices.

Adding Connected Devices to the Blacklist

You can add connected devices to the blacklist, and the device is disconnected from the wireless AP.

Procedure

1. Do one of the following:
    - 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**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP** > **AP Device List**.
2. Do one of the following:
    - If you use the remote control, select the desired device and press OK.
    - If you use the CTP20, select the desired device.

    The monitor prompts “Move the device into blacklist?”.
3. Select **OK**.

    The device is disconnected from your system, and cannot be connected to the wireless AP provided by your system any more.

Removing Devices from the Blacklist

You can remove devices from the blacklist, so that the devices can connect to the wireless AP provided by your system.

Procedure

1. Do one of the following:
    - On your remote control, go to **More** > **Setting** > **Advanced** > **Wireless AP** > **Blacklist**.

      For VC200: on your remote control, go to **More** > **Network** > **Wireless AP** > **Blacklist**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP** > **Blacklist**.
2. Do one of the following:
    - If you use the remote control, select the desired device and press OK.
    - If you use the CTP20, select the desired device.

   The monitor prompts “Remove the device from blacklist?”.
3. Select **OK**.

   After removed from the blacklist, he device can search and connect to the wireless AP provided by your system.

Disabling the Wireless Access Point

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **Wireless AP**.
    - On your remote control, go to **More** > **Setting** > **Advanced** > **Wireless AP**.

      For VC200: on your remote control, go to **More** > **Network** > **Wireless AP**.
    - On your CTP20, tap **Setting** > **Advanced** > **Wired Network** > **Wireless AP**.
2. Disable the wireless AP.

802.1x Authentication

You can use 802.1x authentication to restrict the unauthorized devices to accessing the LAN. The 802.1x authentication can be used to authenticate the devices connected to the port before the system processes all the businesses.

The system supports the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (Device and CA certificates are required, password is not required)
- EAP-PEAP/MSCHAPv2 (CA certificates are required)
- EAP-TTLS/EAP-MSCHAPv2 (CA certificates are required)

For more information on 802.1X authentication, refer to *Yealink 802.1X Authentication*.

- *Configuring the 802.1x Authentication*

Configuring the 802.1x Authentication

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **Advanced** > **802.1x**.
    - 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**.

- On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **802.1 Mode**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
802.1x Mode	Specifies the 802.1x authentication mode. • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 **Note**: the default value is disabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Identity	Configures the user name for 802.1x authentication. **Note**: the default value is blank. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
MD5 Password	Configures the password for 802.1x authentication. **Note**: the default value is blank. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
CA Certificates	Upload the CA certificates. **Note**: upload the CA certificates when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPv2, or EAP-TTLS/EAP-MSCHAPv2. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
Device Certificates	Upload the device certificates. **Note**: Configures the access URL of the server certificate when the 802.1x authentication mode is configured as EAP-TLS. 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*
- *Configuring Transmission Methods*

Supported Transmission Methods

The supported transmission methods for VC880/VC800/VC500/PVT980/PVT950 system’s Internet port are listed below:

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

The supported transmission methods for VC200 endpoint’s Internet port are listed below:

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

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

Restricting Reserved Ports

By default, the system communicates through TCP and UDP ports from 50000 to 51000 for the video, the voice, the presentation, and the camera control. The system uses only a small number of these ports during a call. The specific number of the port 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**.
   - 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **NAT/Firewall** > **Reserved Port**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
UDP Port Scope/ **UDP Lowest Port—UDP Highest Port**	Configures the range of the UDP ports. **Note**: the default UDP port range is from 50000 to 51000. The valid value is from1024 to 65000. **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 CTP20
TCP Port Scope/ **TCP Lowest Port—TCP Highest Port**	Configures the range of the TCP ports. **Note**: the default TCP port range is from 50000 to 51000. The valid value is from1024 to 65000. **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 CTP20

Quality of Service (QoS)

Video conferencing system is subject to the bandwidth and the delay. Therefore, the QoS is very important for the network having limited bandwidth. 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

Some issues, such as the video packet loss and delay may cause the video images distorted and unclear. 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.

- *Configuring QoS*

Configuring QoS

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **QoS**.
   - 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **QoS**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
QoS	Enables or disables the QoS feature. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Audio Priority	Configures the DSCP (Differentiated Services Code Point) for audio packets. **Default**: 63. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20
Video Priority	Configures the DSCP (Differentiated Services Code Point) for video packets. **Note:** the default value is 34. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Data Priority	Configures the DSCP (Differentiated Services Code Point) for data packets. **Note**: the default value is 63. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

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, which may result in poor quality video at the receiving device. You can set the maximum MTU size of the data packets sent by the system.

About this task

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:
   - On your web user interface, go to **Network** > **Advanced** > **MTU**.
   - 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)**.
   - On your CTP20, tap **Setting** > **Advanced** > **Advanced Network** > **Network MTU (1000-1500)**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Network MTU (1000-1500)	Specifies the maximum MTU size (in bytes) of data packets sent by the system. **Note**: the value can be any integer from 1000 to 1500. The default value is 1500. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Restricted Single Packet Mode	Enables or disables the restricted single packet mode. • **Off**—sends data packets by using multiple packets mode. • **On**—sends data packets by using single packet mode. **Note**: the default value is **Off**. Some third-party devices only accept the data packets sent by single packet mode. If local system sends data packets by using multiple packets mode, the video call may appear the mosaic phenomenon. To avoid this situation, enable this configuration. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring Account Settings

This chapter provides information on how to configure account settings.

- *Configuring SIP Settings*
- *Configuring H.323 Settings*
- *Configuring PSTN*

Configuring SIP Settings

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

- *Configuring SIP Accounts*
- *Configuring SIP IP Call*

Configuring SIP Accounts

Yealink video conferencing system supports Session Initiation Protocol (SIP). If your server supports SIP, you can configure a SIP account for your device, and other users can call you by dialing your SIP account.

Procedure

1. 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **SIP Account**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Account Active/SIP Account	Enable or disable SIP Accounts. **Note**: the default value is **On**. If it is set to **disabled**, the devices cannot place or receive calls via the SIP protocol.	Web user interface Remote control CTP20
Username	The username of this SIP account. **Default**: blank.	Web user interface Remote control CTP20
Register Name	The registration name of this SIP account. **Default**: blank.	Web user interface Remote control CTP20
Password	The registration password of this SIP account. **Default**: blank.	Web user interface Remote control CTP20
Server Host/Server	The IP address or domain name of the SIP server. **Default**: blank.	Web user interface Remote control CTP20
Port	Configures the port of the SIP server. **Note**: the default port number is 5060. The value can be any integer from 0 to 65535.	Web user interface Remote control CTP20
Enable Outbound Proxy Server/Outbound	Enables or disables the device to send requests of the SIP account to the outbound proxy server. **Default**: Off.	Web user interface Remote control CTP20
Outbound Proxy Server/ Outbound Server	Configure the IP address or the domain name of the outbound proxy server for this SIP account. **Note**: only the outbound proxy server is enabled do you need to configure this parameter.	Web user interface Remote control CTP20
Port	Configure the port of the outbound proxy server. **Note:** the default port number is 5060. The value can be any integer from 0 to 65535.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • DNS-NAPTR—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: UDP.	Web user interface Remote control CTP20
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the SIP server again. **Default**: 3600 seconds.	Web user interface Remote control CTP20
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30.	Web user interface

Parameter	Description	Configuration Method
Rport	Enables or disables the RPORT feature on the device. When the VCS is behind a NAT device, you can enable this feature for the port traversal with the SIP sever. **Default**: Off. The Rport feature need the support of the SIP server. For more information, refer to *RFC 3581*.	Web user interface

Configuring SIP IP Call

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

Procedure

1. 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
SIP IP Call	Enables or disables the SIP IP Call. **Default**: On. **Note**: When it is set to On on both sites, the system can call the far site by dialing an IP address directly.	Web user interface Remote control CTP20
Transport	Configures the type of transport protocol for the SIP IP call. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. **Default**: TCP.	Web user interface Remote control CTP20

Configuring H.323 Settings

You can place IP calls via the H.323 protocol. If your network uses a gatekeeper, you can register an H.323 account for the system, and specify its H.323 name and extension. This allows others to call you via your H.323 name or the extension instead of the IP address.

- *Configuring H.323 Accounts*
- *H.323 Tunneling*

Configuring H.323 Accounts

Procedure

1. 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.323 Protocol	Enables or disables the H.323 protocol. **Note**: the default value is **On**. Only when it is set to On can the H.323 account be registered. When it is set to On on both sites, the devices can call each other by dialing an IP address directly.	Web user interface Remote control CTP20
H.323 Account	Enables or disables the H.323 account. **Note**: the default value is **On**. If it is set to **Off**, the devices cannot place or receive calls via the H.323 protocol.	Web user interface Remote control CTP20
H.323 Name	Specifies the device name that can be identified by the gatekeepers and gateways. **Default**: blank. If two devices are registered to the same gatekeeper, they can make point-to-point calls by dialing their H.323 names.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
H.323 Extension	Specifies the device extension that can be identified by the gatekeepers and gateways. **Note**: the default value is blank. If two devices are registered to the same gatekeeper, they can make point-to-point calls by dialing their extensions.	Web user interface Remote control CTP20
Gatekeeper Mode/Gatekeeper Type	Configures the gatekeeper mode. • **Off**—the system does not use a gatekeeper. • **Auto**—the system automatically discovers a gatekeeper. • **Manual**—specify the IP address and the port for the gatekeeper manually. You need manually configure the IP address and the port for the gatekeeper. **Default**: Off.	Web user interface Remote control CTP20
Gatekeeper IP Address 1/ Gatekeeper Server 1	Configures the IP address or the domain name for the primary gatekeeper. **Note**: the default value is blank. Only when the configuration type is manual do you need to configure this parameter.	Web user interface Remote control CTP20
Port/Gatekeeper Port 1	Configures the port for the primary gatekeeper. **Note**: the default port number is 1719. The value can be any integer from 0 to 65535.	Web user interface Remote control CTP20
Gatekeeper IP Address 2/ Gatekeeper Server2	Configures the IP address or the domain name for the secondary gatekeeper. **Note**: the default value is blank. Only when the configuration type is manual do you need to configure this parameter. If the device cannot access the primary gatekeeper, the device will send the registration request to Gatekeeper Server2.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Port/Gatekeeper Port 2	Configures the port for the secondary gatekeeper. **Note**: the default port number is 1719. The value can be any integer from 0 to 65535.	Web user interface Remote control CTP20
Gatekeeper Authentication/ Gatekeeper Verify	Enables or disables support for the gatekeeper authentication. **Note**: the default value is **Off**. When Gatekeeper Authentication is enabled, the gatekeeper can ensure that only the trusted H.323 systems are allowed to access the gatekeeper.	Web user interface Remote control CTP20
Gatekeeper Username	Specifies the username used for the gatekeeper authentication. **Note**: the default value is blank.	Web user interface Remote control CTP20
Gatekeeper Password	Specifies the password for the gatekeeper authentication. **Note**: the default value is blank.	Web user interface Remote control CTP20
Protocol Monitor Port	Specifies the port of the H.323 call signaling. If you fail to place an IP call to other party via H.323 protocol, it may be caused by the ISP limiting the 1720 port, so you need modify the protocol monitor port, and call the far site by dialing h323:ip:port. **Note**: the default value is 1720. The modification on this port is only applicable for the H.323 IP call.	Web user interface

Parameter	Description	Configuration Method
Local Early Media	Enables or disables the local early media feature on the device. • **Off**—the local system sends an Open Logical Channel (OLC) message and receives the acknowledgement message of OLC from the far site. After receiving the acknowledgement message, the system may transmit RTP streams to the far site. • **On**—the system sends an 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**: Off.	Web user interface

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. H.323 tunneling is supported by the video conferencing system. 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**.
   - On your CTP20, tap **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**: Off.	Web User Interface Remote control CTP20

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*. After PSTN is connected, you can take the PSTN as one audio and use the PSTN to join the conference mixing with the audio and video.

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**.
   - On your CTP20, go to **Setting** > **Advanced** > **PSTN Account**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Account Active/PSTN Account	Enables or disables the PSTN account. **Default**: On.	Web user interface Remote control CTP20
Label/PSTN Account Label	Configures the PSTN account label.	Web user interface Remote control CTP20

Configuring the Video Conference Platform

You can log into the following video conference platform:

- Yealink VC Cloud
- Yealink Meeting Server
- StarLeaf
- Zoom
- Pexip
- BlueJeans
- EasyMeet
- Videxio
- Custom

Note:

If you purchase the VC200 Custom Edition for Yealink Cloud, your endpoint can register a Yealink Cloud account only. Other Cloud platforms are unavailable on your endpoint. What’s more, you cannot register a SIP account or H.323 account, and cannot dial an IP address.

- *Yealink VC Cloud Management Service*
- *Yealink Meeting Server*
- *StarLeaf Cloud Platform*
- *Zoom Cloud Platform*
- *Pexip Cloud Platform*
- *Logging into the BlueJeans Cloud Platform*
- *Registering an EasyMeet Account*
- *Videxio Platform*
- *Registering a Custom Account*
- *Logging out of the Video Conference Platform*

- *Configuring the Third-party Virtual Meeting Room*

Yealink VC Cloud Management Service

The Yealink VC Cloud Management Service is a value-added and 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 VC Cloud Management Service, 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*

Registering a Yealink Cloud Account

You can use Yealink Cloud accounts to log into Yealink VC Cloud Management Service .

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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot register a Yealink Cloud account.	Web user interface Remote control CTP20
Platform Type	Select Yealink VC Cloud Management Service.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Login Type	Specifies the method for logging into the Yealink VC Cloud Management Service platform. • **PIN Code Login**: This method uses the user's PIN code to log into the Yealink VC Cloud Management Service platform. The 9-digit PIN code is disposable and expires if it is unused for 7 days. Contact your Cloud administrator when it expires. • **Username/password**: This method uses Yealink Cloud account to log into the Yealink VC Cloud Management Service platform. **Default**: PIN code.	Web user interface Remote control CTP20
PIN Code	Specifies the PIN code for logging into the Yealink VC Cloud Management Service platform. **Note**: the default value is blank. Only when you select to log into Yealink VC Cloud Management Service via PIN code can this feature be configured.	Web user interface Remote control CTP20
Username	Specifies the username for logging into the Yealink VC Cloud Management Service platform. **Note**: the default value is blank. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Password	Specifies the Password for logging into the Yealink VC Cloud Management Service platform. **Note**: the default value is blank. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Web user interface Remote control CTP20
Server Host/Server	The IP address or the domain name of Yealink VC Cloud Management Service platform. **Default**: yealinkvc.com.	Web user interface Remote control CTP20
Remember password	Enables or disables the device to remember the password. **Note**: the default value is **On**. If it is set to **On**, the password will be filled in automatically when you log in next time. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Remote control CTP20

Note:

A Yealink Cloud account can be logged into 5 devices 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*

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**.
- On your CTP20, go to **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 set to **Off**, your device cannot log into YMS.	Web user interface Remote control CTP20
Platform Type	Select YMS.	Web user interface Remote control CTP20
ID	Specifies the ID when registering this YMS account. **Default**: blank.	Web user interface Remote control CTP20
Password	Specifies the password when registering this YMS account. **Default**: blank.	Web user interface Remote control CTP20
Server Host/Server	The IP address or the domain name of Yealink meeting server. **Default**: blank.	Web user interface Remote control CTP20
Port	Select a port of Yealink meeting server. **Default port number**: 0	Web user interface
Outbound Proxy Server/ Outbound Server	The IP address or domain name of the outbound proxy server. **Default**: blank.	Web user interface Remote control CTP20
Remember password	Enables or disables the device to remember the password. **Note**: the default value is **Off**. If it is set to **On**, the password will be filled in automatically when you log in next time.	Remote control CTP20

Note:

A YMS account can be logged into 5 devices at most simultaneously.

If the enterprise administrator enables the **Device upgrade** feature on Yealink meeting server, video conferencing systems with YMS accounts logged into will upgrade the firmware automatically once they receive the new firmware from 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.
- Dial the Meeting ID to join the Virtual Meeting Rooms.
- Call between StarLeaf Cloud account and Microsoft Skype for Business/Lync account.

- *Registering a StarLeaf Account*

Registering a StarLeaf 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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot log into the StarLeaf Cloud platform.	Web user interface Remote control CTP20
Platform Type	Select StarLeaf.	Web user interface Remote control CTP20
QCP Code	Specifies the quick access code to log into the StarLeaf Cloud platform. **Default**: blank.	Web user interface Remote control CTP20

Note:

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

Zoom Cloud Platform

You can log into Zoom cloud platform and call into the permanent VMRs to join in the video conferences with other participants.

- *Logging into Zoom Cloud Platform*

Logging into Zoom 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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot log into the Zoom Cloud Platform.	Web user interface Remote control CTP20
Platform Type	Select Zoom.	Web user interface Remote control CTP20
Server/ **Server Host**	The IP address or the domain name of the Zoom server. **Default:** zoomcrc.com	Web user interface Remote control CTP20
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface

Parameter	Description	Configuration Method
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600.	Web user interface
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30.	Web user interface

Pexip Cloud Platform

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.
- Dial Microsoft Skype for Business/Lync account.

- *Registering a Pexip Account*

Registering a Pexip 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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot register a Pexip account.	Web user interface Remote control CTP20
Platform Type	Select Pexip.	Web user interface Remote control CTP20
Alias	Specifies the alias when registering a Pexip account. **Default**: blank.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Username	Specifies the username for this Pexip account. **Default**: blank.	Web user interface Remote control CTP20
Password	Specifies the password for this Pexip account. **Default**: blank.	Web user interface Remote control CTP20
Server Host/Server	The IP address or domain name of the Pexip server. **Default**: blank.	Web user interface Remote control CTP20
Port	The port of the Pexip server. **Default**: 0.	Web user interface Remote control CTP20
Remember password	Enables or disables the device to remember the password. **Note**: the default value is **Off**. If it is set to **On**, the password will be filled in automatically when you enter the username next time.	Remote control CTP20

Parameter	Description	Configuration Method
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600.	Web user interface
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30.	Web user interface

Note:

Yealink VCS also supports register a Pexip account via the standard H.323 or SIP 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 do the followings:

You can do the following things after logging into the BlueJeans Cloud Platform:

- Dial the Meeting ID to join the Virtual Meeting Rooms.
- Receive meeting schedule from the BlueJeans Cloud platform.

- *Logging into the BlueJeans Cloud Platform*

Logging into the BlueJeans 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**.
    - On your CTP20, go to **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 set to **Off**, your device cannot log into the BlueJeans Cloud Platform.	Web user interface Remote control CTP20
Platform Type	Select the BlueJeans Cloud Platform.	Web user interface Remote control CTP20
Server Host/Server	The IP address or the domain name of the BlueJeans server. **Default**: bjn.vc.	Web user interface Remote control CTP20
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface

Parameter	Description	Configuration Method
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600.	Web user interface
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30.	Web user interface

Registering an EasyMeet Account

You can register the EasyMeet account and do the following:

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

- Dial the EasyMeet account to establish a point to point call.
- Dial the Meeting ID to join the Virtual Meeting Rooms
- Receive meeting schedule from the EasyMeet Cloud platform.

- *Registering an EasyMeet Account*

Registering an EasyMeet 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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot register an EasyMeet account.	Web user interface Remote control CTP20
Platform Type	Select EasyMeet.	Web user interface Remote control CTP20
Username	Specifies the username for this EasyMeet account. **Default**: blank.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Password	Specifies the password for this EasyMeet account. **Default**: blank.	Web user interface Remote control CTP20
Server Host/Server	The IP address or the domain name of the EasyMeet server. **Default**: blank.	Web user interface Remote control CTP20
Outbound Proxy Server/ Outbound Server	The IP address or the domain name of the outbound proxy server. **Default**: blank.	Web user interface Remote control CTP20
Remember password	Enables or disables the device to remember the password. **Note**: the default value is **On**. If it is set to **On**, the password will be filled in automatically when you enter the username next time.	Remote control CTP20
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TLS.	Web user interface

Parameter	Description	Configuration Method
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Videxio Platform

You can log into Videxio platform and Videxio accounts will be automatically logged into the devices. Videxio platform is only available to VC200/VC500/VC800/VC880.

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

- Dial Videxio accounts to establish a point-to-point call.
- Dial third-party accounts registered in the Videxio platform to establish a conversation.
- Call into the Virtual Meeting Room to join the video conference with other devices.

- *Logging into Videxio Platform*

Related tasks

Configuring the Third-party Virtual Meeting Room

Logging into Videxio Platform

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Video Conference Platform**.
   - On your CTP20, go to **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 set to **Off**, your device cannot log into the Videxio platform.	Web user interface Remote control CTP20
Platform Type	Select Videxio.	Web user interface Remote control CTP20

Registering a Custom Account

You can register a custom account for communication.

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**.
   - On your CTP20, go to **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 set to **Off**, your device cannot register a custom account.	Web user interface Remote control CTP20
Platform Type	Select Custom.	Web user interface Remote control CTP20
Label	Configures the label for this custom account. **Default**: blank.	Web user interface Remote control CTP20
Username	Specifies the username for this custom account. **Default**: blank.	Web user interface Remote control CTP20
Register Name	Configures the register name for this custom account. **Default**: blank.	Web user interface Remote control CTP20
Password	Specifies the password for this custom account. **Default**: blank.	Web user interface Remote control CTP20
Server Host/Server	The IP address or the domain name of the server. **Default**: blank.	Remote control Web user interface CTP20
Port	Configures the port of the custom server. **Note**: the default port number is 0. The value can be any integer from 0 to 65535.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Remember password	Enables or disables the device to remember the password. **Note**: the default value is **Off**. If it is set to **On**, the password will be filled automatically when you enter the username next time.	Remote control
Transport	Configures the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configures the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Logging out of the Video Conference Platform

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform** > **Log Out**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **Video Conference Platform** > **Log Out**.
   - On your CTP20, go to **Setting** > **Advanced** > **Video Conference Platform** > **Log Out**.

   It prompts whether to log out the current account.
2. Click **OK**.

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.

About this task

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/EasyMeet/Videxio Platform) 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.

Note: Third-party virtual meeting room is not available on VC200 Custom Edition for Yealink Cloud.

Procedure

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

Parameter	Description	Configuration Method
VMR Name 1 to 5	Configures the virtual meeting room name. **Note**: • The VMR name 1 is Zoom by default. • The VMR name 1 is BlueJeans by default. • The VMR name 3 to 5 is empty by default. 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 Server 1 to 5	The IP address or the domain name of the VMR server. **Note**: • The VMR server 1 is zoomcrc.com by default. • The VMR server 2 is bjn.vc by default. • The VMR server 3 to 5 is empty by default. 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

The dialing screen of your web user interface and the monitor will appear the configured VMR. You can select the desired VMR from the pull-down menu, and then enter the conference ID to call the corresponding VMR.

Configuring General Settings

- *Setting the Site Name*
- *Setting the Language*
- *Setting Time and Date*
- *Allowing Website Snapshot*
- *Adjusting Backlight of the CP960 Conference Phone*
- *Customizing the Local Interface*
- *Configuring the Keyboard Input Method*
- *Configuring USB Storage*
- *Configuring Local Storage*
- *Capturing Screenshots by Using Remote Control*
- *Configuring Video Recording*

Setting the Site Name

You can customize the site name.

Procedure

1. 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**.
    - On your CTP20, tap **Setting** > **Basic** > **Site Name**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Site Name	Configures the site name of the system. **Note**: you can enter 64 characters at most.	Web user interface Remote control CTP20

Setting the Language

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

Procedure

1. 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**.
    - On your CTP20, tap **Setting** > **Basic** > **Language**.
2. Select the desired language.
3. Save the change.

Setting Time and Date

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

- *Expand-Time zone*
- *NTP Settings*
- *Configuring the DST*
- *Configuring Time and Date Manually*
- *Customizing the Time and Date Format*
- *Setting the Reminder*

Expand-Time zone

You can set the time difference between GMT (Greenwich Mean Time) and your location. Therefore, different areas can keep the time consistency for the commence and communication. The following table lists the available time zone on video conferencing system.

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

Time zone	Time zone	Time zone	Time zone
-08:00	Mexico (Tijuana, Mexicali)	+02:00	Jordan (Amman)
-08:00	United States-Pacifi 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)
-03:30	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 zone	Time zone	Time zone	Time zone
-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)

Time zone	Time zone	Time zone	Time zone
+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

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**.
    - On your CTP20, tap **Setting** > **Basic** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Manual Time/Time Type	Select **Off/SNTP Setting** to obtain the time and date from the NTP server automatically.	Web user interface Remote control CTP20
DHCP Time	Enables or disables the system to update time with the offset time offered by the DHCP server. **Note**: the default value is **Off**. It is only available to GMT 0.	Web user interface
Time Zone	Configures the time zone. For more information on available time zone, refer to *Expand-Time zone* . **Default**: +8China (Beijing).	Web user interface Remote control CTP20
NTP Primary Server/Primary Server	Configures the NTP primary server. **Default:** cn.pool.ntp.org.	Web user interface Remote control CTP20
NTP Secondary Server/ Secondary Server	Configures the NTP secondary server. **Default:** cn.pool.ntp.org.	Web user interface Remote control CTP20
Synchronism (15~86400s)	Configures the interval (in seconds) to update time and date from the NTP server. **Default**: 1000.	Web user interface

Configuring the DST

You can set Daylight Saving Time (DST) for the system according to the location. 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**.
   - On your CTP20, tap **Setting** > **Basic** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Daylight Saving Time	Configure the type of DST. The available types for the system are as below: • **Disabled**: do not use DST. • **Enabled**-use DST. You can manually configure the start time, the end time and the offset according to your needs. • **Automatic**-use DST. DST will be configured automatically. You do not need to manually configure the start time, the end time and the offset according to your needs. **Default**: Auto.	Web user interface Remote control CTP20
Fixed Type	Configures the DST calculation methods. The available types for the system are as below: • **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 when you enable Daylight Saving Time.	Web user interface
Start Date	When you select By Date as the fixed type, configure the start time of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface

Parameter	Description	Configuration Method
End Date	When you select By Date as the fixed type, configure the end time of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface
DST Start Month	When you select By Week as the fixed type, configures the start time of DST. **Note**: It only works when you enable Daylight Saving Time.	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 month, configures the end month of DST. **Note**: It only works when you enable Daylight Saving Time.	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 value: from -300 to +300. **Note**: It only works when you enable Daylight Saving Time.	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

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**.
   - On your CTP20, tap **Setting** > **Basic** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Manual Time/Time Type	Select **On/Manual Setting** to obtain the time and date from the NTP server automatically.	Web user interface Remote control CTP20

3. Configure the time and date.
4. Save the change.

Customizing the Time and Date Format

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

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**.
   - On your CTP20, tap **Setting** > **Basic** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Time Format	Configures the time format. • Hour12 • Hour24 **Default**: Hour24.	Web user interface Remote control CTP20
Date Format/Date	Configures the date format. The supported formats are as below: • 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 CTP20

Setting the Reminder

The system displays a clock on the hour during a call. You can disable it if you do not want to pay attention to time.

Procedure

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

Parameter	Description	Configuration Method
Time Reminder	Enables or disables the system to display a clock on the hour during a call. **Default**: On.	Web user interface

3. Configure the time and date.

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. Do one of the following:
   - On your remote control, go to **More** > **Setting** > **Basic**.
   - On your CTP20, tap **Setting** > **Basic**.
2. Enable **Website Snapshot**.

Adjusting Backlight of the CP960 Conference Phone

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

About this task

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

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

Procedure

Do one of the following:

- On your web user interface, go to **Setting** > **General** > **General Information** > **Backlight Time**.
- On your CP960 conference phone, tap **Setting** > **Display** > **Backlight**.
- On your CP960 conference phone, swipe down from the top of the screen to enter the control center.

  Drag the backlight slider.

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*
- *Hiding IP Address*
- *Hiding Heading Time*
- *Hiding the User Interface in Idle Screen*
- *Showing or Hiding Icons in a Call*

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.

- *Setting Screen Saver for Monitor*
- *Setting the Screen Saver for CP960 Conference Phone*

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**.
   - On your CTP20, tap **Setting** > **Basic** > **Screensaver**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Screen Saver Wait Time	Configures the inactive time (in minutes) before the system starts the screen saver. **Default**: 1 minutes.	Web user interface Remote control CTP20

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

Setting the 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. select the corresponding screen saver type.
3. Configure and save the following settings:

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

Hiding IP Address

You can choose to hide the 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 settings:

Parameter	Description	Configuration Method
Hide IP address	Enables or disables the IP address to be displayed on the status bar. • **On**—do not display the IP address. • **Off**—display the IP address. **Default**: Off.	Web user interface

Hiding Heading Time

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

Procedure

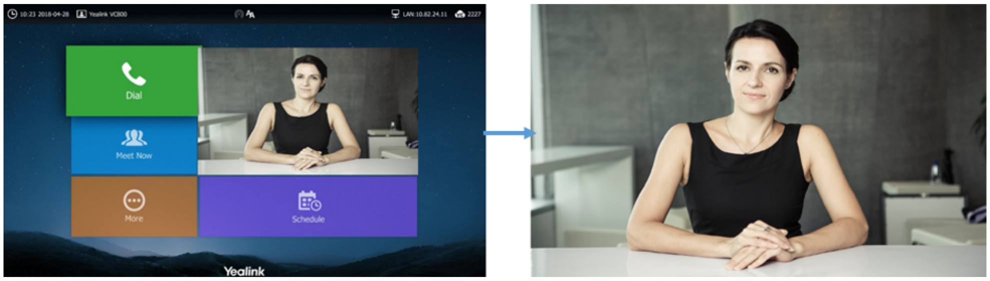
1. On your web user interface, go to **Setting** > **General** > **General Information** > **Hide Heading Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide Heading Time	Enables the monitor to hide the time and the date on the status bar. • **On**—do not display the heading time. • **Off**—display the heading time. **Default**: Off.	Web user interface

Hiding the User Interface in Idle Screen

You can choose to hide the user interface when the system is idle. The monitor only displays the local video or the PC content.

About this task



Procedure

1. On your web user interface, go to **Setting** > **General** > **General Information** > **Hide UI in Idle Screen**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide UI in Idle Screen	Enables the monitor to hides the user interface when the system is idle. • **On**—hide the user interface. • **Off**—display the user interface. **Default**: Off.	Web user interface

Showing or Hiding Icons in a Call

During a call, the system will show some information and icons (such as the call time, the mute icon and recording icon) by default, so that you can know the call status from these information and 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 setting:

Parameter	Description	Configuration Method
Title Bar	Enables or disables the system to hide the title bar during a call. • **Show**- the system displays the title bar. • **Hide with UI**- the system displays the title bar and then hide it after 5 seconds. • **Hide**- the system hides the title bar. **Default**: Hide with UI.	Web User Interface
Time Icon	Enables or disables the system to hide the call time during a call. • **Show**- the system displays the call time. • **Hide with UI**- the system displays the call time and then hide it after five seconds. • **Hide**- the system hides the title bar. **Default**: Hide with UI.	Web User Interface

Parameter	Description	Configuration Method
Mute Icon	Enables or disables the system to hide the mute icon (🔇) during a call. • **Show**- the system displays the mute icon. • **Hide with UI**- the system displays the mute icon and then hide it after five seconds. • **Hide**- the system hides the mute icon. **Default**: Hide with UI.	Web User Interface
Camera Icon	Enables or disables the system to hide the camera icon (📷) during a call. • **Show**- the system displays the camera icon. • **Hide with UI**- the system displays the camera icon and then hide it after five seconds. • **Hide**- the system hides the camera icon. **Default**: Hide with UI.	Web User Interface
Recording Icon	Enables or disables the system to hide the recording icon (●) during a call. • **Show**- the system displays the recording icon. • **Hide with UI**- the system displays the recording icon and then hide it after five seconds. • **Hide**- the system hides the recording icon. **Default**: Show.	Web User Interface

Parameter	Description	Configuration Method
Sitename Icon	Enables or disables the system to hide the site name during a call. • **Show**- the system displays the site name. • **Hide with UI**- the system displays the site name and then hide it after 5 seconds. • **Hide**- the system hides the site name. **Default**: Hide with UI.	Web User Interface
Hold Icon	Enables or disables the system to hide the hold icon (⏸) during a call. • **Show**- the system displays the hold icon. • **Hide with UI**- the system displays the hold icon and then hide it after five seconds. • **Hide**- the system hides the recording icon. **Default**: Hide with UI.	Web User Interface
Encryption Icon	Enables or disables the system to hide the encryption icon (🔓) during a call. • **Show**- the system displays the encryption icon. • **Hide with UI**- the system displays the encryption icon and then hide it after five seconds. • **Hide**- the system hides the encryption icon. **Default**: Hide with UI.	Web User Interface

Parameter	Description	Configuration Method
OutPut Mute Icon	Enables or disables the system to hide the output mute icon (🔇) during a call. • **Show**- the system displays the output mute icon. • **Hide with UI**- the system displays the output mute icon and then hide it after five seconds. • **Hide**- the system hides the output mute icon. **Default**: Hide with UI.	Web User Interface
SecondScreen Icon	Enables or disables the system to hide the secondscreen icon (👁) during a call. • **Show**- the system displays the secondscreen icon. • **Hide with UI**- the system displays the secondscreen icon and then hide it after five seconds. • **Hide**- the system hides the secondscreen icon. **Note**: the default value is **Hide with UI**. It is not applicable to VC200.	Web User Interface

Configuring the Keyboard Input Method

You can use the full keyboard on the screen to enter or to edit the data. 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. 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 ˅.

   The input method shown at the top has the highest priority.

Configuring USB Storage

If you have high requirement for data security, you can disable the USB storage. After disabling the feature, you cannot use the USB flash drive to store recorded videos, screenshots or captured packets.

Procedure

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

Parameter	Description	Configuration Method
USB Enable	Enables or disables the USB feature. **Note**: the default value is **On**. 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.

About this task

Note: The priority of local storage is lower than USB storage. When users disable 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** > **USB Config** > **Local Storage Enable**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Local Storage Enable	Enables or disables the local storage feature. **Note**: the default value is **On**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Capturing Screenshots by Using Remote Control

You can capture screenshot.

Before you begin

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

If you want to save the screenshot to local storage (only applicable to VC200), make sure the 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
Screenshot	Enables or disables to capture the screenshot by using the remote control. • **On**—you can take a screenshot by the remote control. • **Off**—you cannot take a screenshot by the remote control. **Default**: On.	Web user interface

- *Screenshot*

Related tasks

Configuring USB Storage

Configuring Local Storage

Screenshot

Procedure

Do one of the following:

- On your web user interface, go to **Home** > **Screenshot**.
- On your remote control, if 🖥 is set to the Screenshot key, press 🖥 to capture screenshot.
- On your CP960 conference phone, go to **More** > **Screenshot**.

Configuring Video Recording

You can record the video.

Before you begin

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

If you want to record the video to the 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	Enables or disables the video recording feature on the system. **Default**: On.	Web user interface

Parameter	Description	Configuration Method
Auto recording	Enables or disables the system to start recording automatically once a call is established. • **On**- the system starts recording automatically once a call is established. • **Off**- the system does not start recording automatically once a call is established. **Note**: the default value is **Off**. Only the Recording feature is enabled can this feature be available.	Web user interface
Auto Stop Recording	Enables or disables the system to stop recording automatically once a call is established. • **On**- the system stops recording automatically once a call is established. • **Off**- the system does not stop recording automatically once a call is established. **Default**: On.	Web user interface
Recording Notification	Enables or disables the system to show recording icon and recording prompt. • **On**- the recording icon and the duration are displayed on the system screen. • **Off**- the recording icon and the duration are not displayed on the system screen. **Default**: On.	Web user interface
WPP20 Recording Confirm (it is only available to VC200/VC500/ VC800/VC880)	Enables or disables the system to allow the action that you use WPP20 to record. **Default**: On.	Web user interface
Dual Screen Recording	Select the desired screen. You can record the video on the selected screen when you are using dual screen. • Screen 1+2: record video on dual screen • Screen 1 Only • Screen 2 Only **Default**: Screen 1+2. It is not applicable to VC200.	Web user interface

Related tasks

Configuring USB Storage

Configuring Local Storage

Configuring the Audio Settings

- *Configuring the Audio Output*
- *EQ Self-Adaption*
- *Audio Input*
- *Media Audio Input*
- *Key Tone*
- *Tones*
- *Codecs*
- *DTMF*
- *Muting the Microphone*
- *Muting Auto-Answered Calls*
- *Muting Auto-Dialed Calls*
- *Configuring the Noise Suppression*

Configuring the Audio Output

Model	Audio Output
VC880/VC800/VC200/PVT980	• **Auto**- selects the audio output with the highest priority. If the audio output with the highest priority is removed, the system will select the device with the second highest priority. The priority is VCS Phone>HDMI>Line Output. • **VCS Phone** • **HDMI** • **Line Output**
VC500/PVT950	• **Auto**- selects the audio output with the highest priority. The priority is VCS Phone>HDMI>USB Output. • **VCS Phone** • **HDMI** • **USB Output**

- *Specifying an Available Audio Output*

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 Settings** > **Audio Output**.
   - On your remote control, go to **More** > **Setting** > **Video & Audio** > **Audio Settings**.

     For VC200: on your remote control, go to **More** > **Setting** > **Audio Settings** > **Audio Output**.
   - On your CTP20, tap **Setting** > **Audio** > **Audio Output**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio Output	Specifies the audio output for the system. The supported types are as follows: • **Auto**- selects the audio output device with the highest priority. • **VCS Phone** - selects the CP960 conference phone. • **HDMI** - selects the built-in speakerphone of the monitor. If you connect two monitors to your system, only the HDMI 1 port is available for audio output. • **Line Output** –the speakerphone connected to VC880/VC800/VC200/PVT980 codec. • **USB Line out** - the audio output device connected to the USB port on the VC500/PVT950 codec by using a USB to Line-out adapter. **Note**: the default value is **Auto**. If VCS Phone is set as the audio output device manually or automatically, the audio input device must be VCS Phone.	Web user interface Remote control CTP20

Note:

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 information

EQ Self-Adaption

EQ Self-Adaption

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

For VC880/VC800/VC500/PVT980/PVT950: 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 to Line Output**.
- Every time you powered on the system, you find that **HDMI** or **Line Output**/**USB to Line Output** is the 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:

- The first time you connect a display device to VC200.
- Resetting to Factory

- Click **EQ Self Adaption**.
- *Configuring 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 settings:

Parameter	Description	Configuration Method
EQ Self-Adaption	Enables or disables the EQ self-adaption feature on the system. **Default**: On.	Web user interface
Start EQ Self Adaption	Starts the EQ self-adaption feature. **Note**: This configuration is only applicable to VC200 and appears only when the system satisfies the following conditions: • The VCS phone is not selected as the audio output device. • **EQ Self Adaption** is set to On.	Web user interface

Audio Input

- *Available Audio Input*
- *Specifying an Available Audio Input*

Available Audio Input

Model	Audio Output
VC880/VC800/PVT980	• **Auto**—the system automatically selects the audio input with the highest priority. The audio input priority is shown as below: • VCS Phone • Bluetooth Microphone • Line Input
VC200	• **Auto**—the system automatically selects the audio input with the highest priority. The audio input priority is shown as below: • VCS Phone • Built-in Microphone • Bluetooth Microphone • USB Line in

Model	Audio Output
VC500/PVT950	• Auto • VCS Phone • Bluetooth Microphone • USB Line in

Specifying an Available Audio Input

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**.
    - On your CTP20, tap **Setting** > **Audio** > **Audio Input**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio Input	Specifies the audio input for the system. The supported types are as follows: • **Auto** - selects the audio output with the highest priority. • **VCS Phone** - selects the CP960 conference phone. • **Built-in Microphone** - selects the VC200 built-in microphone. • **Bluetooth Microphone** - selects the CPW90-BT Bluetooth wireless microphones. • **Line Input**- the audio input device connected to the Line In port on the VC800 codec or to the RAC In port on the VC880/PVT980 codec. • **USB Line in** - the audio input device connected to the USB port on the VC200/ VC500/PVT950 codec by using a USB to Line-in adapter. **Default**: Auto.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Line AEC	Enables or disables echo cancellation for line input device. • **On**- eliminate the echo to the line input devices. If you select an acoustic device (for example: a microphone) to be the line input, you can enable this configuration. • **Off**- do not eliminate the echo to the line input devices. If you select a non-acoustic device (for example: a mobile phone) to be the line input, you can disable this configuration. **Note**: the default value is **Off**. This configuration is available only when 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.	Web user interface
Audio Line In	Configures the volume of line input device. **Note**: • **Valid value**: Integer from -50 to 50dB. • The default value 0 means to use the default sending volume. The value you set is based on the default value. • This configuration is available only when 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. • It is not applicable to VC200.	Web user interface

Note:

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

Media Audio Input

When the VCS device is connected to both a microphone and other media audio inputs (such as connected to a computer to play audio), you need to configure the type of media audio input, so that the mix input can be realized.

The sound from the media audio input device is mixed to the local output by default and can be mixed to the remote output.

Note: If the microphone is connected to the device via Line Input or USB to Line Input, you should not select the interface to which the microphone is connected when using the media audio input, otherwise there may be a strident sound.

- *Configuring Media Audio Input*

Configuring Media Audio Input

Procedure

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

     For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Media Audio Input**.
   - On your CTP20, tap **Setting** > **Audio** > **Media Audio Input**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Media Audio Input	Specify the media audio input connected to the device. The supported types are as follows: • **Off**- not use any media audio input. • **Line Input (No access)**- the media audio input device connected to RCA In port on VC880 or to the Line In port on VC800. • **USB to Line Input (No access)**- the media audio input device connected to the USB port on VC500/ VC200 via a USB to line input adapter. **Default**: Off.	Web user interface Remote control CTP20

Key Tone

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

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**.
   - On your CTP20, tap **Setting** > **Basic** > **Key Tone**.
2. Enable/disable **Key Tone**.

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*
- *Custom Tones Formats*
- *Customizing Tones*

Supported Tones

The system supports tones in the following countries. The tone set is a predefined by each country according to different device status. The tones of different countries varies.

Available tone sets for the system are described as below:

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 different tones for the system except for the default tone.

The custom tones formats are as below:

E1,E2,E3,E4,E5,E6,E7,E8 (you can configure up to 8 different tones which are separated by commas)

En=[!][F1][+F2][+F3][+F4] /Duration

Parameter explanation:

- 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.
- An exclamation mark “!” before tones : it means that the tone only rings once.

(for example, !250/200, 0/1000, 200+300/500, 500+1200/800, 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

Parameter	Description	Configuration Method
Ring Back	Customizes the ring-back tone for the system **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Busy	Customizes the busy tone for the system. **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Call Waiting	Customizes the call waiting tone for the system. **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Auto Answer	Customizes the auto answer tone for the system. **Note**: the default value is blank. When it is blank, the American tones are enabled.	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. The administrator can configure the codec and its priority for the devices.

- *Audio Codec*
- *Video Codecs*

Audio Codec

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*
- *Configuring Audio Codecs*

Supported Audio Codecs

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

Audio Codec	Algorithm	Bit Rate	Sample Rate	Reference
Opus	opus	8-12 Kbps 16-20 Kbps 28-40 Kbps 48-64 Kbps 64-128 Kbps	8 Ksps 12 Ksps 16 Ksps 24 Ksps 48 Ksps	RFC 6716
ARES	ARES	8-64kpbs	48 Ksps	No
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 the following audio bandwidths:

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	Specify the audio codecs to be used. **Note**: You can move the disabled codec to this field.	Web user interface
Disable Codecs	Specify the audio codecs that are not used. **Note**: You can move enabled codec to this field.	Web user interface

Parameter	Description	Configuration Method
Opus Sample Rate	Configure the sample rate of the opus audio codec. • 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	Enable or disable the special audio codec byte sequence. • **Off**—keep the current codec byte sequence. • **On**—different devices have different definition about audio codec byte sequence, which may lead to the audio incompatibility problems between Yealink and certain devices. You can enable this feature to solve these incompatibility problems. **Default**: Off.	Web user interface

Video Codecs

The video codecs 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*
- *Configuring Video Codecs*
- *Selecting an H.265 Mode*

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 HP	H264/90000	90—2048 kbps	5—30 fps	Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P
H.264	H264/90000			
H.263	H263/90000			Tx: CIF, 4CIF Rx: QCIF, CIF, 4CIF
H.263+	H263/90000			Tx: CIF Rx: CIF

Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.265	H265/90000			Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P

Note:

If you are using H.265 video codec during a one-way-video call, the system will negotiate with the other parties to use H264 High profile video codec automatically when more people join the 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 the disabled codec to this field.	Web user interface
Disable Codecs	Specifies the disabled video codecs. **Note**: you can move the enabled codec to this field.	Web user interface
SVT T (it is only available to VC200/VC500/VC800/VC880)	This feature is only available to H.264/H.264 video codecs. **Default**: Off.	Web user interface

Selecting an H.265 Mode

You can select VBR or CBR for the H.265 video codec according to your network bandwidth. It is only applicable to VC200 endpoint.

Procedure

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

Parameter	Description	Configuration Method
H.265 Mode	H.265 video codec. • **VBR**- the output data rate of the H.265 codec varies per time segment. You can save nearly half the bandwidth. • **CBR**- the output data rate of the H.265 codec is constant. If the latency issue appears in the call or video image is abnormal, it may result from packet loss, you can select this value to try to fix this issue. **Default**: VBR.	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*
- *Transmission Ways of DTMF Digits*
- *Configuring DTMF for SIP Protocol*
- *Configuring DTMF for H.323 Protocol*

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)). The switch can decode the frequency group and locate the corresponding key.

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Transmission Ways of DTMF Digits

Three ways to transmit DTMF digits during SIP calls is as below: RFC2833, INBAND, SIP INFO.

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/EasyMeet/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
   - On your remote control, go to **More** > **Setting** > **Advanced** > **SIP IP Call**.
   - On your CTP20, tap **Setting** > **Advanced** > **SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
DTMF Type	Configures the DTMF type. • **INBAND**—DTMF digits are transmitted in the voice band, together with the general RTP voice packet. • **RFC2833**—DTMF digits are transmitted by RTP packet which is compliant to RFC2833. • **SIP INFO**—DTMF digits are transmitted by SIP INFO. • **RFC2833+ SIP INFO**—DTMF digits are transmitted by RFC 2833 and the SIP INFO. **Default**: RFC2833.	Web user interface Remote control CTP20
DTMF Info Type	Configures the DTMF info type when DTMF type is set to SIP INFO or RFC2833+SIP INFO. • DTMF-Relay • DTMF • Telephone-Event **Default**: DTMF-Relay.	Web user interface Remote control CTP20
DTMF Payload Type (96~127)	Configures the value of DTMF payload. **Default**: 101.	Web user interface

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 settings:

Parameter	Description	Configuration Method
DTMF Type	Configures the DTMF type. • **INBAND**—DTMF digits are transmitted in the voice band, together with the general RTP voice packet. • **Auto**—the system automatically negotiates the way (INBAND, RFC2833 or SIP INFO) to transfer DTMF digits. **Default**: Auto.	Web user interface Remote control CTP20

Muting the 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:

- On your web user interface, go to **Home** > **Mute**.
- On your remote control, press 🔇.
- On your CP960 conference phone, tap the Mute key.
- On your CP960 conference phone’s touch screen, tap the Mute key.
- On your CPE90 wired expansion microphones, tap the Mute key.
- On your CPW90-BT Bluetooth wireless microphones, tap the Mute key.

If video conferencing system is muted, the icon 🔇 will appear on the local video.

- *Configuring Microphone Mute Mode*

Configuring Microphone Mute Mode

By default, if you enable the mute mode on a single microphone (CPE90/CPW90/CPW90-BT), other microphones will be muted 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 settings:

Parameter	Description	Configuration Method
Microphone Mute Mode	Configure the microphone mute mode. • **Synchronized**- if you mute/ unmute a microphone, other microphones will be muted/ unmuted simultaneously. • **Separated**- if you can only mute/unmute one microphones, others does not respond. **Default**: Synchronized.	Web user interface

Note:

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

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 the local conversation freely.

Procedure

1. 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**.
   - On your CTP20, tap **Setting** > **Basic** > **Auto Answer Mute**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Auto Answer Mute	Enables or disables the local microphone to be muted when an incoming call is answered automatically. **Note**: the default value is **On**. Only the Auto Answer Mute feature is enabled can this feature be available.	Web user interface Remote control CTP20

Related information

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.

About this task

Note: The system is still muted after you hang up.

Procedure

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

Parameter	Description	Configuration Method
Auto Dialout Mute	Enables or disables the system to turn off the microphone after the other party answers your call. **Default**: Off.	Web user interface

Configuring the 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
Temporal Noise Shaping(TNS)	Enables or disabled the Transient Noise Suppressor (TNS). • **On**—it can reduce the noise volume temporarily and block the noise in the voice. • **Off** **Default**: On.	Web user interface
Noise Barrier	Enables or disabled the noise barrier feature. • **On**—it can block the noise in the non-speech process. • **Off** **Default**: Off.	Web user interface

Configuring Video Settings

- *Changing the Video Input Source*
- *Selecting the Default Layout for a Single Screen*
- *Hiding Local Video Image in Equal Layout*
- *Configuring Change Layout by Content Sharing*
- *Specifying Content to the Secondary Screen*
- *Selecting Video Frame Rate and Resolution*
- *Maximizing Monitor Video Display*
- *Configuring the Monitor Resolution*

- *Configuring Automatic Sleep Time*
- *CEC Monitor Controls*
- *System Integrated with Control Systems*

Changing the Video Input Source

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

Procedure

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 the Default Layout for a 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** > **Layout** > **Default Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Default Layout of Single Screen	Configures the default layout of single screen when a call is established. • **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). **Default**: Picture-in-picture.	Web user interface

Hiding Local Video Image in Equal Layout

If you want to focus on the far sites or the PC content in a call (its video layout is equal layout), you can choose to hide the local video image.

Procedure

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

Parameter	Description	Configuration Method
Equal Display Local	Select **Off** to hide local video image when the video layout is equal. • **On**—the local video image is shown. • **Off**—the local video image is hidden. **Default**: On.	Web user interface

Configuring Change Layout by Content Sharing

The feature of **Change Layout by Content Sharing** is enabled by default. When you are presenting on the PC, the layout in the device is changed into 1+N or voice-activated mode automatically, and the content is enlarged and displayed in the screen. This feature is only available to VC200/VC500/VC800/VC880.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Layout**.
2. Enable or disable **Change Layout by Content Sharing**.

Related information

Configuring Content Sharing

Specifying Content to the Secondary Screen

When you connect dual display screen, you can specify the content to be displayed on the secondary monitor. It is not available on the VC200 video conferencing system.

Procedure

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

Parameter	Description	Configuration Method
Output For Display 2	Specify the content to be displayed on the secondary monitor. • **Auto**—The secondary monitor displays the content in this priority: PC>VC880/VC800/VC500/PVT980/PVT950 Camera>Camera N. • **PC**—The secondary monitor displays the PC content. • VC880/VC800/VC500/PVT980/PVT950 Camera—The secondary monitor displays the video images from the local camera. • **Camera N**—The secondary monitor displays the video images from the connected camera N. **Note**: the default value is **Auto**. After you specify “Output for Display 2”, you can still modify the content to be displayed on the secondary monitor temporarily during a call by using the “Focus” feature. But the next time you establish a call, the content to be displayed on the secondary monitor is controlled by the “Output For Display 2” .	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	Enables or disables 60fps for a video call. **Note**: the default value is **On**. It is not applicable to VC200.	Web user interface

Parameter	Description	Configuration Method
Frame	Specifies the maximum frame rate of the video. • 5fps • 15fps • 30fps • 60fps—this option appears only when you enable 60fps. **Default**: 30fps.	Web user interface
Main->Resolution	Specifies the maximum resolution of the video. • 1080P • 720P **Default**: 1080P.	Web user interface

Note:

If both parties do not use H.265 codec, and choose to use WDR exposure mode and 60fps, the call will switch to auto exposure mode automatically. For more information, refer to *Adjusting the White Balance* .

Maximizing Monitor Video Display

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

Procedure

1. Do one of the following:
    - On your remote control, go to **More** > **Setting** > **Basic** > **Display**.
    - On your CTP20, tap **Setting** > **Basic** > **Display**.
2. Use left or right navigation key to adjust the **Display(90%-100%)** slider.
3. Save the change.

Configuring the 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 **Setting** > **Display** > **Output Resolution**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Display1	Configures the output resolution of primary monitor. • **Auto**-select the highest output resolution automatically. • The available output resolutions (The available resolutions depend on the monitor you are using). **Default**: Auto.	Web user interface CP960 Conference Phone
Display 2	Configures the output resolution of secondary monitor. • **Auto**-select the highest output resolution automatically. • The available output resolutions (The available resolutions depend on the monitor you are using). **Default**: Auto.	Web user interface CP960 Conference Phone

Configuring Automatic Sleep Time

Static images displayed for long periods may lead to monitor burn-in, therefore, you can configure the automatic sleep time for the device. After the device goes to the sleep mode, “no signal” is displayed on the monitor.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Video & Audio** > **General Information** > **Automatic Sleep Time**.
   - On your remote control, go to **More** > **Setting** > **Basic** > **Automatic Sleep Time**.
   - On your CTP20, tap **Setting** > **Basic** > **Automatic Sleep Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Automatic Sleep Time	Configures the inactive time (in minutes) before the system enters sleep mode. **Note**: the default value is 10 minutes. When you power the system on and set the setup wizard, the automatic sleep time feature is disabled automatically. To protect the monitor, you should complete the setup wizard immediately.	Web user interface Remote control CTP20

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. The users can use a remote control to control all the devices connected by HDMI.

The CEC feature is enabled by default on VC880/VC800/VC500/PVT980/PVT950 video conferencing system. Ensure that all monitors connected to the system supports and enables the CEC feature. CEC feature is not applicable to VC200 video conferencing endpoint.

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*

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 settings:

Parameter	Description	Configuration Method
CEC Enable	Enables or disables the CEC feature. **Default**: On.	Web user interface

System Integrated with Control Systems

Yealink video conferencing system provides API for third-party control system to integrate with. Therefore, third-party control system can control Yealink video conferencing system via API.

- *Connection Settings for Control Systems*

- *Connection Methods of Control Systems*

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**: on. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Control Security Password	Enables or disables an authentication password when the control system tries to connect to the video conferencing system. **Default**: empty. **Note**: this parameter is only available for **Control Security Enabled**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Baud Rate	Configures the baud rate. • **2400** • **4800** • **9600** • **19200** • **38400** • **115200** **Default**: 115200 **Note**: It must be the same rate for the control system and Yealink video conferencing system.	Web user interface

Parameter	Description	Configuration Method
Data Bits	Configures the data bits. • **7** • **8** **Default**: 8 **Note**: It must be the same rate for the control system and Yealink video conferencing system.	Web user interface
Parity	Configures the parity. • **None** • **Odd** • **Even** • **Space** **Default**: Space **Note**: It must be the same rate for the control system and Yealink video conferencing system.	Web user interface
Stop Bits	Configures the stop bits. • **1** • **2** **Default**: 1 **Note**: It must be the same rate for the 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. Select one of the following:

- **LAN Connection**: Make sure the Yealink video conferencing system and the control system are in the same network segment. If you use this mode to control the system, TCP protocol is recommended. 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 the mode, the frame rate and the resolution for the shared content.

Note:

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

- *Configuring Dual-Stream Protocol*
- *Configuring Mix-Sending*
- *Configuring the Parameters of the Shared Content*

Configuring Dual-Stream Protocol

The dual-stream protocol allows the 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. Based on this protocol, the participants can share contents while having a video call.

The Yealink video conferencing system supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol).

- *Configuring the H.239 protocol*
- *Configuring BFCP (Binary Floor Control Protocol)*

Configuring the 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 settings:

Parameter	Description	Configuration Method
H.239	Enables or disables the H.239 protocol. **Default**: On.	Web user interface

Configuring BFCP (Binary Floor Control Protocol)

BFCP is used when sharing content with the remote in SIP calls.

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/EasyMeet / Videxio/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
BFCP	Enables or disables the BFCP. **Note:** For Zoom/Pexip/BlueJeans/EasyMeet/Videxio/Custom and SIP IP call, BFCP is enabled by default. For SIP account, BFCP is disabled by default. This feature is not available to Yealink StarLeaf Cloud platform.	Web user interface

Related tasks

Configuring Mix-Sending

Configuring Mix-Sending

During a call, the remote may not support dual-stream protocol. Therefore, you need enable this feature, so that multiple video streams (the local video + the local content) can be synthesized to one video stream and sent to the remote.

Procedure

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

Parameter	Description	Configuration Method
Mix	Enable or disable the mix-sending feature on the system. **Note**: the default value is **On**.	Web user interface

Note: If the call parties enable the dual-stream protocol, the dual-stream protocol will be used to sent multiple video streams.

Configuring the Parameters of the Shared Content

You can specify the mode, the maximum frame and the resolution for the shared content. Make sure that the definition of the presentation is good.

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	Configure the content sharing mode. • **Sharing Document**- select this mode to save bandwidth when you are sharing a document. • **Sharing Video**- select this mode to play video fluently when you are sharing a video. **Default**: Sharing Document.	Web user interface
Frame	Specify the maximum frame rate when the content is sharing. • 5fps • 15fps • 30fps **Default**: 15fps.	Web user interface
Resolution	Specify the maximum frame rate when the content is sharing. • 1080P • 720P **Default**: 1080P.	Web user interface
Automatic Content Sharing (it is only available to VC200/ VC500/VC800/VC880)	Configure whether to enable PC presentation on the system when the content is sharing. **Default**: On.	Web user interface

Configuring Camera Settings

- *Selecting a Camera*
- *Viewing Camera Status*
- *Adjusting Camera Angle and Focus*
- *Adjusting the White Balance*
- *Adjusting the White Balance*
- *Adjusting Graphics*
- *Configuring Other Settings of the Camera*
- *Allowing the Far-End System to Control Your Camera*
- *Setting the Camera Presets*
- *Configuring Continuous Auto Focus*

Selecting a Camera

You can configure camera parameters for a desired camera, customize its name and set the camera layout.

Procedure

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

Parameter	Description	Configuration Method
Camera	Configures the desired camera.	Web user interface
Status	Enables or disables the camera. **Note**: the default value id On. It is not applicable to VC200/ VC500/PVT950.	Web user interface
Multi-camera Default Layout	Configures the default camera layout when you use multiple cameras. The supported layouts are described as below: • 1+N • Selected speaker • Equal N×N **Note**: the default value is **1+N**. It is not applicable to VC200/ VC500/PVT950.	Web user interface
Select a camera	Select the camera you want to highlight. **Note**: The first connected camera. This configuration appears only if **Multi-camera Default Layout** is set to **1+N** or **Selected Speaker**. It is not applicable to VC200/ VC500/PVT950.	Web user interface

Viewing Camera Status

Procedure

1. Do one of the following:

   - On your web user interface, go to **Setting** > **Camera** > **Camera Info**.
   - On your remote control, go to **More** > **Status** > **Camera**.
   - On your CTP20, tap **Setting** > **Camera** > **Camera details**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Camera Name	Configures a name for the camera.	Web user interface
Model	The VCS codec model.	Remote control CTP20
IP address	The IP address of the selected camera.	Web user interface
Firmware version	The firmware version of the selected camera.	Web user interface
Hardware version	The hardware version of the selected camera.	Web user interface
SPEC	The specification of the selected camera.	Web user interface Remote control CTP20
MAC address	The MAC address of the selected camera.	Web user interface
Hardware version	The hardware version of the camera lens.	Web user interface Remote control CTP20

Adjusting Camera Angle and Focus

You can pan, tilt and zoom your own camera.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Home** > **Yourself** > 📷 .
   - On your remote control, select the local video.
   - On your CP960 conference phone, tap **Camera**.
   - On your CTP20, tap **Camera**.
2. Use the navigation keys to adjust the camera angle.
3. Use ⊖or ⊕/⊖ or ⊕ to adjust the camera angle.

Adjusting the White Balance

To display the high quality video image, you can adjust the camera white balance.

- *Setting Auto Exposure Mode*
- *Setting Manual Exposure Mode*
- *Configuring the Mode of Shutter Priority*
- *Configuring Aperture Priority*

- *Configuring the Mode of Brightness Priority*
- *Configuring the Mode of WDR-Auto*
- *Configuring WDR-Manual*

Setting Auto Exposure Mode

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **Manual** as the **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configures the value of exposure compensation. The 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. **Valid value**: from -6 to 6. **Default**: 0.	Web user interface Remote control CTP20
Flicker	Configures the value of the camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Remote control CTP20
Gain/Gain Limit	Specifies the value. **Valid value**: 1 - 15. **Default**: 4.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
WDR/Wide Dynamic Range	Specifies the WDR. The value represents the compression degree of the dynamic range. Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Remote control CTP20
Metering	Configures the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Remote control CTP20

Setting Manual Exposure Mode

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **Manual** as the **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Aperture	Configures the value of aperture. • Off • F1.6, F2.0, F2.4, F2.8, F3.4, F4, F4.8, F5.6, F6.8, F8, F9.6, F11, F14 **Default**: F3.4.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Shutter	Configures the value of the shutter. **Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350, 1/500, 1/725 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Remote control CTP20
Gain	Specifies the value. **Valid value**: 1 - 15. **Default**: 2.	Web user interface Remote control CTP20
WDR/Wide Dynamic Range	Specifies the WDR. The value represents the compression degree of the dynamic range. Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Remote control CTP20

Configuring the Mode of Shutter Priority

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **Shutter Priority** as the **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Shutter	Configures the value of the shutter. **Valid Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350/ 1/500, 1/725/, 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Remote control CTP20
Exposure Compensation	Configure the value of exposure compensation. The 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. **Valid value**: from -6 to 6. **Default**: 0.	Web user interface Remote control CTP20
Gain/Gain Limit	Specifies the value. **Valid value**: from 1 to 15. **Default**: 4.	Web user interface Remote control CTP20
WDR/Wide Dynamic Range	Specifies the WDR. The value represents the compression degree of the dynamic range. Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Remote control CTP20
Metering	Configures the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Remote control CTP20

Configuring Aperture Priority

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video&Audio** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **Aperture Priority** in **Exposure Mode** field.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Aperture	Disable aperture or set the desired value. **Value**: F1.6, F2.0, F2.4, F2.8, F3.4, F4.0, F4.8, F5.6, F6.8, F8, F9.6, F11, F14 and off **Default**: F3.4.	Web user interface Remote control CTP20
Exposure Compensation	Configure the value of exposure compensation. The 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. **Valid value**: from -6 to 6. The default value is 0.	Web user interface Remote control CTP20
Flicker	Disable the flicker or configure the value of camera flicker frequency. **Frequency**: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Remote control CTP20
Gain	Specify the value of gain. **Valid value**: 1 - 15. The default value is 4.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
WDR/Wide Dynamic Range	Specify the value of WDR. The value represents the compression degree of the dynamic range. Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Remote control CTP20
Metering	Configure the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Remote control CTP20

Configuring the Mode of Brightness Priority

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **Brightness Priority** as the **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Brightness	Configures the value of brightness. **Note**: the valid value is from 0 to 14 and the default value is 6.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Flicker	Configures the value of camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Remote control CTP20
WDR/Wide Dynamic Range	Specifies the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Remote control CTP20
Metering	Configures the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Remote control CTP20

Configuring the Mode of WDR-Auto

WDR mode is not available to VC200.

Procedure

1. Do one of the following:
    - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
    - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
    - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **WDR-Auto** from the drop-down menu of **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The 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. **Note**: the valid value is from -6 to 6. The default value is 0.	Web user interface Remote control CTP20

Configuring WDR-Manual

WDR-Manual mode is not available to VC200.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Exposure**.
   - On your CTP20, tap **Setting** > **Camera** > **Exposure**.
2. Select **WDR-Auto** from the drop-down menu of **Exposure Mode**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The 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. **Valid value**: from -6 to 6. **Default**: 0.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Exposure Ratio	Configures the value of exposure ratio. **Note**: the valid value is from 1 to 16. The default value is 1. The exposure ratio represents the ratio of long exposure to short exposure. In a backlit environment, the bright part uses a short exposure and the dark part uses a long exposure.	Web user interface Remote control CTP20

Adjusting the White Balance

To display high quality video image, you can adjust camera white balance.

Procedure

1. Do one of the following:
    - On your web user interface, go to **Setting** > **Camera** > **White Balance**.
    - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **White Balance**.
    - For VC200: on your remote control, go to **More** > **Setting** > **Video&Audio** > **White Balance**.
    - On your CTP20, select **Setting** > **Camera** > **White Balance**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
White Balance Mode	Configures the white balance mode of the camera. • **Auto**—Yealink recommends that you use this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. • **InDoor** • **OutDoor** • **OnePush** • **ATW—**automatically adjust the white balance according to the picture took by the camera. • **Auto**—manually adjust the color temperature **Default**: ATW.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Color Temperature (it is only available to VC200/VC500/ VC800/VC880)	Configure the value of the color temperature. **Note**: the value is from 2800K to 6800K. The default value is the color temperature tested in the your current environment. You can set this parameter only when the white balance mode is configured to Manual.	Web user interface Remote control

Adjusting Graphics

To display the high quality video image, you can adjust camera graphics.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Graphic**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Graphics**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Graphics**.
   - On your CTP20, tap **Setting** > **Camera** > **Graphics**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Display Mode	Configures the display mode of the camera. • High Definition • Standard • Mild • Custom **Default**: Standard.	Web user interface Remote control CTP20
Saturation	Configures the saturation of the camera's image. The saturation means the maximum intensity of color in the image. **Note**: the value is from 0 to 100. **Default**: 50.	Web user interface Remote control CTP20

Parameter	Description	Configuration Method
Sharpness	Configures the sharpness of the camera's image. The sharpness is an indicator that reflects the definition of the image plane and the sharpness of image edge. Increasing the sharpness will improve the definition of the image. However, if the sharpness is set too high, the image will look distorted and glaring. **Valid value**: 0 - 100. **Default**: 15.	Web user interface Remote control CTP20
Brightness	Configures the brightness of the camera's image. **Valid value**: 0 - 100. **Default**: 50.	Web user interface Remote control CTP20
Contrast	Configures the contrast of the camera's image. **Valid value**: 0 - 100. **Default**: 49.	Web user interface Remote control CTP20
Noise Reduction (2D)	Specifies the noise reduction (2D) mode. The available modes are described as below: • Off • Low • Middle • High **Default**: Middle.	Web user interface Remote control CTP20
Noise Reduction (3D)	Specifies the noise reduction (3D) mode. It indicates the coefficient of the reduced noise in the image. The higher the coefficient is, the smaller the noise is. **Valid value**: 0 - 22. **Default**: 3.	Web user interface Remote control CTP20

Configuring Other Settings of the Camera

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

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Graphic**.
   - For VC880/VC800/VC500/PVT980/PVT950: on your remote control, go to **More** > **Setting** > **Camera Setting** > **Graphics**.
   - For VC200: on your remote control, go to **More** > **Setting** > **Video & Audio** > **Graphics**.
   - On your CTP20, tap **Setting** > **Camera** > **Other**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hangup Mode	Enables or disables the camera to flip the image view when camera is handed at up-side-down position. If this mode is enabled, the picture took by the camera is upside down. This mode is applicable to install the camera on the meeting room ceiling. **Default**: Off.	Web user interface Remote control CTP20
Camera Pan Direction	Configures the pan direction of the camera. • Normal • Reversed 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. **Default**: Normal.	Web user interface Remote control CTP20
Reset Camera	Resets the camera to factory defaults.	Web user interface Remote control CTP20

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 Near Camera feature.

- *Camera Control Protocol*
- *Configuring the Far Site to Control the Near Camera*

Camera Control Protocol

If the remote wants to control your camera, both the remote and you 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 the H.323 call and enable FECC (SIP) protocol for the SIP call.

- *Configuring FECC (H.323) Protocol*
- *Configuring FECC (SIP) Protocol*

Configuring FECC (H.323) Protocol

FECC(H.323) protocol is used when controlling the far-site camera in H.323 calls. To control the far-site camera, the call parties should enable this protocol 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**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
FECC (H.323)	Enables or disables FECC(H.323). Enables FECC (H.323) protocol, so that the remote can control the near camera. **Default**: On.	Web user interface

Configuring FECC (SIP) Protocol

FECC(SIP) protocol is used when controlling the far-site camera in SIP calls. To control the far-site camera, the call parties should enable this protocol simultaneously.

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/EasyMeet / Videxio/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
FECC (SIP)	Enables or disables the FECC (SIP) protocol for the far site to control the near camera. **Note:** For Zoom/Pexip/BlueJeans/ EasyMeet/Videxio/Custom and SIP IP call, BFCP is enabled by default. For SIP account, the default value is off.	Web user interface

Configuring the Far Site to Control the Near Camera

You can enable this feature to allow the remote to control your local camera, so that the image captured by the local camera can be displayed properly on the remote monitor.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Video & Audio** > **Far Control Near Camera**.
   - For on your remote control, go to **More** > **Setting** > **Video & Audio**.
   - On your CTP20, tap **Setting** > **Camera** > **Far Control Near Camera**.
2. Configure and save the following settings:

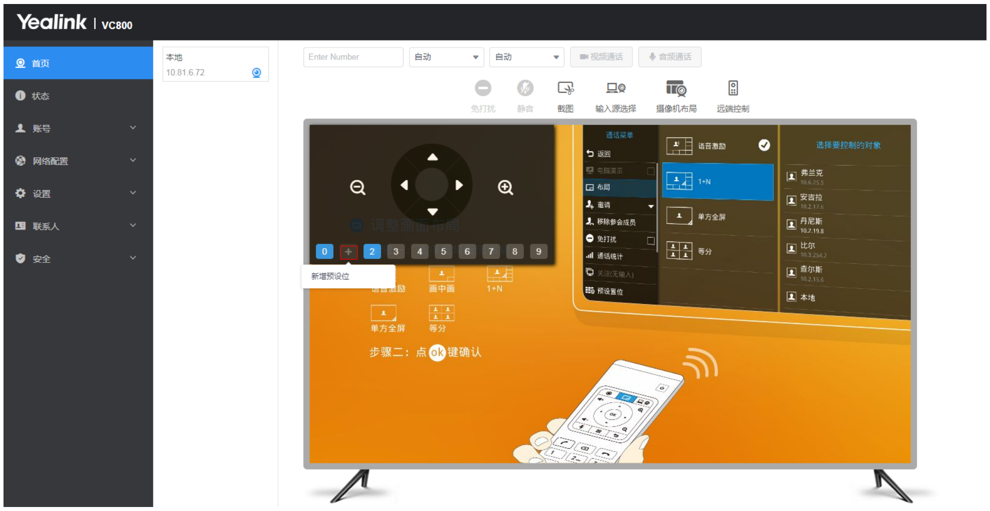
Parameter	Description	Configuration Method
Far Control Near Camera	Enables or disables the far site to control the near-site camera. **Default**: On.	Web user interface Remote control CTP20

Setting the Camera Presets

The camera presets store the setting of the angle and the focal length. The camera presets can help you quickly point a camera at pre-defined locations. The camera presets can remain in effect until you change them.

Procedure

1. On your web user interface, go to **Home** > **Yourself** > 📷.



2. Click any number to configure the camera presets.

   You can add, modify, and delete the preset.

> **Note:** For more information about configuring presets via CP960 conference phone, CTP20 or the remote control, refer to the *Yealink Full HD Video Conferencing System User Guide*.

Configuring Continuous Auto Focus

If you want to make the camera focus on the moving object automatically, you can enable this feature. If you want a fixed focal length for presentation, for example, the class, you can disable this feature. It is not available to VC200/PVT980/PVT950.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Focus**.
   - For VC880/VC800/VC500: on your remote control, go to **More** > **Setting** > **Camera Setting**.
   - On your CTP20, tap **Setting** > **Camera**.
2. Enable or disable **Continuous Auto Focus**.

Call Settings

- *Selecting a Call Protocol*
- *Specifying the Video Call Rate*
- *Account Polling*
- *Configuring Additional Audio Call*
- *Selecting the Multi-party Resources*
- *Search Source List in Dialing*
- *Configuring Call Match*
- *Auto Answer*
- *Do Not Disturb*
- *Enabling Fast Audio Call for CP960*
- *Configuring Ringback Timeout*
- *Configuring the Auto Refuse Timeout*
- *SIP IP Call by Proxy*

Selecting a Call Protocol

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

Procedure

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

Parameter	Description	Configuration Method
Call Protocol	Specifies the desired call protocol for placing calls. The supported types are as follows: • **Auto**—the system automatically uses the available call protocol. The system preferentially uses the H.323 protocol to place calls. 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. **Default**: Auto.	Web user interface Remote control

Specifying the 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.

About this task

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

Procedure

1. 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** > **Setting** > **Call Features** > **Video Call Rate**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Video Call Rate	Specifies the maximum video call rate. **Default**: 2000kb/s.	Web user interface Remote control

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*
- *Configuring the Account Polling*

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**.

Configuring the Account Polling

Procedure

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

Parameter	Description	Configuration Method
Account Polling	Enables or disables the account polling on the system. • **Off**—the system dials a number by using the call type with the highest priority. If you disable this feature, once the dialed number differs from the call type you are using, you cannot place the call. • **On**—the system tries each call type in order to dial a number. **Default**: On.	Web user interface

Example

1. System A is registered with a Yealink Cloud account and a SIP account.
2. Select the call type automatically. 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 (the second highest priority) to call system B.

Related tasks

Placing a Call by Entering a Number

Configuring Additional Audio Call

If you enable this feature, when the number of video calls reaches the limit (except for 24-way video calls) in the call, additional 5 users can still place audio calls to join the call. Otherwise, additional 5 users cannot place audio calls to join the call. This feature is only available to VC200/VC500/VC800/VC880.

About this task

For example, for VC800 with 16-way license, if you disable additional audio call, when you create a call, only 16 participants can place video calls to join your call, the 17th participant cannot join the call.

Procedure

1. On your web user interface, go to **Setting** > **Call Features**.
2. Enable or disable **Additional Audio Call**.

Selecting the Multi-party Resources

If you are during a P2P call, you can invite a third party using its own capacity (built-in MCU) or the server VMR to initiate a conference.

About this task

The systems can select multi-party resources by the following:

Prerequisite	Multiparty Resources	Inviting the third party
VC500/VC200 endpoint uses Cloud account or YMS account to make a P2P call.	**Auto**	Select multi-party resources according to this priority: Server VMR >Endpoint own capacity
VC880/VC800 system (without an imported multipoint license) uses Cloud account or YMS account to make a P2P call.		
VC880/VC800 system (with an imported multipoint license) uses any call type (Cloud/YMS/SIP/H.323/IP) to make a P2P call.		Uses the capacity to initiate a conference call
PVT980/PVT950 system uses any call type (Cloud/YMS/SIP/H.323/IP) to make a P2P call.		Uses the capacity to initiate a conference call
Any call type (Cloud/YMS/SIP/H.323/IP) is used to make a P2P call	**Endpoint Built-in MCU**	Uses the capacity to initiate a conference call
Cloud account or YMS account is used to make a P2P call.	**Server VMR**	Uses server VMR to initiate a conference call

Note: The system uses its own capacity to initiate a conference call in following situations: one is dialing a group to initiate a conference call when the system is idle, the other one is receiving a call when the system is during a P2P call.

Procedure

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

Parameter	Description	Configuration Method
Multiparty Resources	Configures the multiparty resources that the system uses to initiate a conference call. • **Auto**—the available multi-party resources are used automatically. • **Endpoint Built-in MCU** • **Server VMR** **Default**: Auto.	Web user interface

Search Source List in Dialing

The 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. To make the system search a specific list, you need configure the list first.

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 LDAP list, make sure LDAP is already configured, refer to *LDAP* .

- *Configuring Search Source List in Dialing*

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 ›.
3. The selected search source list appears in the Enabled column.
4. Repeat step 2 to add more search source lists to the Enabled column.
5. To remove a list from the Enabled column, select the desired list and then click ‹.
6. To adjust the search priority of the enabled search source lists, select the desired list, and click ˄ or ˅.
7. The list shown on the top has the highest priority.
   The system will search the list with higher priority preferentially.

Configuring Call Match

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

- *Configuring Call Match*

Configuring Call Match

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 settings:

Parameter	Description	Configuration Method
Configuring Call Match	Enables or disables the call match feature on the system. **Default**: On.	Web user interface Remote control

Related information

Configuring Call Match

Auto Answer

You can allow the system to answer incoming calls automatically.

- *Answering a Call Automatically*
- *Answering Multiple Calls Automatically*

Answering a Call Automatically

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

About this task

Attention: Auto answer feature may create security issues, for example, an unexpected caller can view your video conference room randomly.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features** > **Auto Answer**.
   - On your remote control, go to **More** > **Setting** > **Call Features** > **Auto Answer**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap **Setting** > **Basic** > **Auto Answer**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Auto Answer	Enables or disables the auto answer feature on the system. **Default**: On.	Remote control Web user interface CP960 Conference Phone CTP20

Related tasks

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.

Before you begin

Make sure the auto answer is enabled.

About this task

Attention: Auto answer feature may create security issues, for example, an unexpected caller can view your video conference room randomly.

Procedure

1. 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** > **Setting** > **Call Features** > **Auto Answer Multiway**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap **Setting** > **Basic** > **Auto Answer Multiway**.
2. Configure and save the following settings:

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**: Off.	Web user interface Remote control CTP20

Do Not Disturb

You can enable do not disturb feature to reject incoming calls automatically. All calls you reject will be recorded to missed calls list.

- *Enabling DND when Not in a Call*
- *Enabling DND during an Active Call*

Enabling DND when Not in a Call

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features** > **Do Not Disturb**.
   - On your remote control, go to **More** > **Setting** > **Call Features** > **Do Not Disturb**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap **Setting** > **Basic** > **DND**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Do Not Disturb	Enables or disables DND mode on the system. **Default**: Off.	Web user interface Remote control CP960 Conference Phone CTP20

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.

Procedure

Do one of the following during a call:

- On your web user interface, go to **Home** > **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**.
- On your CTP20, tap ⋯ > **DND**.

Enabling Fast Audio Call for CP960

If you enable this feature and users register SIP accounts or H.323 accounts in VCS system, the interface of **Audio Call** will be added to CP960. Users can tap **Audio Call** to place an audio call, and the call is placed via SIP account or H.323 account by default. This feature is only available to VC200/VC500/VC800/VC880.

Procedure

1. On your web user interface, go to **Setting** > **Call Features**.
2. Enable **Fast Audio Call**.

Configuring Ringback Timeout

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

Procedure

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

Parameter	Description	Configuration Method
Ringback Timeout(30-240)	Configures the duration time (in seconds) in the ringback state. **Note:** the valid value is from 30 to 240 and the default value is 180. If it is set to 180, the system will cancel dialing if the call is not answered within 180s.	Web user interface Remote control CTP20

Configuring the Auto Refuse Timeout

The 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 settings:

Parameter	Description	Configuration Method
Auto Refuse Timeout (30-240)	Configures the duration time (in seconds) in the ringing state. **Note**: the value is from 30 to 240. **Note**: the default value id 120. If it is set to 120, the system will stop ringing if the call is not answered within 120s.	Web user interface Remote control CTP20

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 settings:

Parameter	Description	Configuration Method
SIP IP Call by Proxy	Configures the SIP IP call by proxy. • **Off**—when dialing the URI of the far site, the system uses the SIP IP address to establish a connection. • On—when dialing the URI of the far site, the system uses the SIP account to establish a connection. **Default**: Off.	Web user interface

Configuring the 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 Types*
- *Meeting Password*

- *Joining the Meeting*
- *Configuring Voice Activation*
- *Configuring the View Switching*

Conference Types

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/PVT980/PVT950	Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.	For VC880/VC800/ VC500/VC200, up to 1 video call and 5 voice calls. For PVT980, up to 8 video calls and 5 voice calls. For PVT950, up to 4 video calls and 5 voice calls.
VMR Mode	VC800 video conferencing system with a multipoint license	Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.	The total MCU ways of the two virtual meeting rooms are depended on the multipoint license you imported. You can allocate the MCU ways between two virtual meeting rooms respectively.
		Virtual meeting room 2: when participants call the virtual meeting room 2, only participants join the meeting, the moderator does not join the meeting.	

- *Conference of General Mode*
- *VMR Mode Conference*

Related information

Multipoint Licenses

Conference of General Mode

Conference of general mode provides virtual meeting room 1.

- *Selecting Regular Mode Conference*

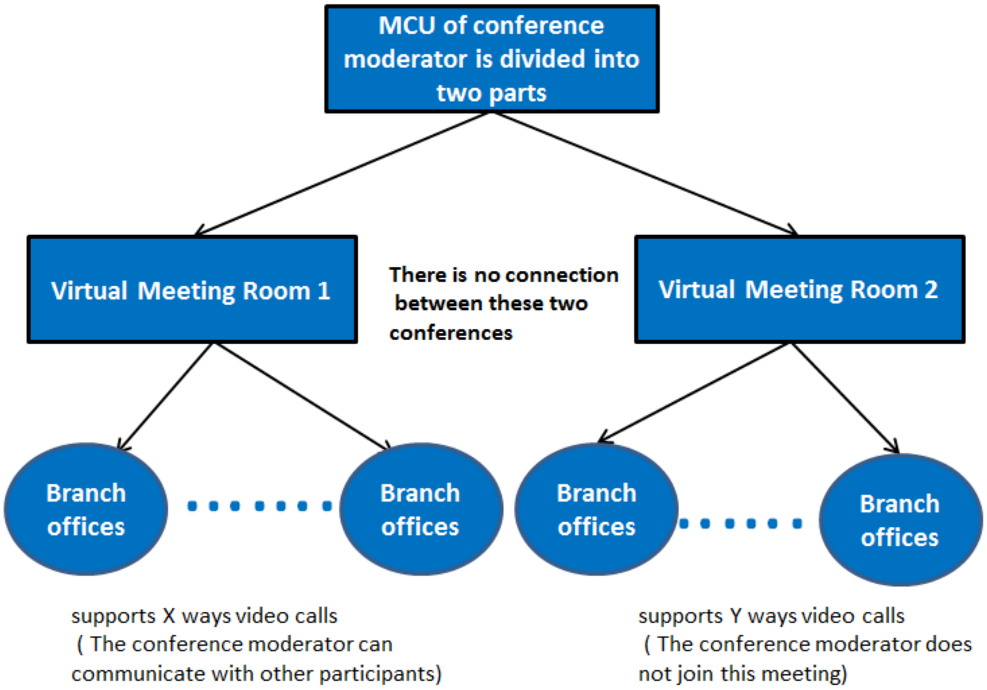
Selecting Regular Mode Conference

Procedure

1. On your web user interface, go to **Setting** > **Buit-in MCU Setting** > **Conference Setting**.
2. Select **Regular Mode** from the drop-down menu of **Conference Type**.

VMR Mode Conference

In VMR mode conference, the MCU of moderator can be used to host two independent conferences (corresponding to virtual meeting room 1 and virtual meeting room 2). The VMR mode conference is only available for VC800.


MCU of conference moderator is divided into two parts
Virtual Meeting Room 1
There is no connection between these two conferences
Virtual Meeting Room 2
Branch offices
Branch offices
Branch offices
Branch offices
supports X ways video calls (The conference moderator can communicate with other participants)
supports Y ways video calls (The conference moderator does not join this meeting)

- If you import an 8 ways multipoint license to the VC800 system, X+Y<=8. Two virtual meeting rooms supports up to 8 ways video calls.
- If you import an 16 ways multipoint license to the VC800 system, X+Y<=16. Two virtual meeting rooms supports up to 16 ways video calls.
- If you import an 24 ways multipoint license to the VC800 system, X+Y<=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 system, virtual meeting room 1 provides additional 5 voice calls.

- *Selecting VMR Mode Conference*

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** > **Buit-in MCU Setting** > **Conference Setting**.
2. Select **VMR Mode** from the drop-down menu 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 the 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*

Configuring Meeting Password

Procedure

1. On your web user interface, go to **Setting** > **Buit-in MCU 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. **Default**: Off.	Web user interface
Virtual Meeting Room 1->Meeting Room 1 Password	Configures the password for virtual meeting room 1. **Valid Value**: 1 to 10, default value: 6.	Web user interface
Virtual Meeting Room 2->Meeting Password	Enables or disables the system to configure a password for virtual meeting room 2. **Note**: the default value is **Off**. Only when the meeting room type is VMR mode can this parameter be configured.	Web user interface
Virtual Meeting Room 2->Meeting Room 2 Password	Configures the password for virtual meeting room 2. **Valid Value**: 1 to 10, default value: blank. Only when the meeting room type is VMR mode can this parameter be configured.	Web user interface

Related information

Joining the Meeting

Conference Types

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.

Example:

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

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 tasks

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. When a new speaker is identified, the image of the previous speaker is replaced by the new speaker. Other video images remain unchanged.

About this task

Note:

Voice activation is only applicable to PVT980/PVT950/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** > **Buit-in MCU Setting** > **Conference Setting**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Voice Activation	Enables or disables the voice activation feature. **Default**: On.	Web user interface
Voice Hold Active Duration	Configures the voice activation interval. **Default**: 1 seconds. If the voice duration of a speaker is greater than 1 second, the video image of this speaker is displayed in largest pane.	Web user interface

Configuring the View Switching

The 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.

- **Average Mode**: Up to 9 video images can be displayed in the Equal N×N layout. When the number of participants exceeds 9, all participants' video images will be switched automatically. The 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 the Speaker View layout and the 1+N 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:

The view switching is only applicable to VC880/VC800/PVT980/PVT950 system with a multipoint license. It is not applicable to VC500/VC200 endpoint.

- *Configuring the Average Mode*
- *Configuring 1+N Mode*

Configuring the 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** > **Buit-in MCU Setting** > **Video Layout** > **Average Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. **Note**: the default value is 30 seconds. 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 1+N layout, up to 8 video images can be displayed. When the number of participants exceeds 8, all participants' video images will be switched automatically. But the video images of active speaker and the content are not be switched.

Procedure

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

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. **Note**: the default value is 30 seconds. The video images will be switched automatically every 30 seconds.	Web user interface
View Round	Configure the number of video images to be switched at a time. **Note**: the default value is 1. **Valid value**: 1 - 7.	Web user interface
Full Screen Round	Switches all video images (except for the active speaker and the content) at a time.	Web user interface

Configuring the Security Features

The following introduces how to configure the security features.

- *User and Administrator*
- *Configuring the Auto Logout Time*
- *Transport Layer Security (TLS)*

User and Administrator

- *Configuring an Administrator Password*
- *Enabling the User Role*

Configuring an Administrator Password

The default administrator name is "admin" and the administrator password is "0000". Only the user with the administrator permission can change the password. For security reasons, you should change them as soon as possible. The administrator password for the system supports ASCII characters 32-126 (0x20-0x7E).

Procedure

1. 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**.
   - On your CTP20, tap **Setting** > **Advanced** > **Password Reset**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
User Type	Select the administrator.	Web user interface

Parameter	Description	Configuration Method
Old Password/Current Password	Enters the old administrator password. **Default**: “0000 ”.	Web user interface Remote control CTP20
New Password	Configures a new administrator password. **Note**: You can leave the password blank.	Web user interface Remote control CTP20
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 CTP20

Enabling the User Role

Procedure

1. On your web user interface, go to **Security** > **Security**.
2. 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**: the system supports ASCII characters 32-126 (0x20-0x7E). You can also leave the password blank.	Web user interface

Configuring the 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. You can change the auto logo time.

Procedure

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

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 minutes.	Web user interface

Transport Layer Security (TLS)

Transport Layer Protocol (TLS) is a commonly-used protocol for ensuring communications privacy and managing the security of the message transmission. When secured by the TLS protocol, the device can transmit the data and communicate safely.

The TLS protocol includes two protocol groups: the TLS handshake protocol and the TLS record protocol. The TLS handshake protocol allows the server and the client to authenticate with each other before negotiating about the data, the encryption algorithms and the encrypted keys. The TLS Record Protocol completes the actual data transmission and ensures the data integrity and confidentiality. The TLS protocol uses an asymmetric encryption algorithm to exchange keys, a symmetric encryption algorithm to ensure data confidentiality, and the MAC algorithms to ensure data integrity.

- *Supported Cipher Suites*
- *TLS Transport Protocol*
- *Managing the Trusted Certificates List*
- *Managing the Server Certificates*
- *Secure Real-Time Transport Protocol (SRTP)*
- *H.235*
- *Defending against Attacks*

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 by 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 via 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/EasyMeet / Videxio/Custom**.
    - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **Transport**.
    - On your remote control, go to **More** > **Setting** > **Advanced** > **SIP account/SIP IP Call** > **Transport**.
    - On your CTP20, tap **Setting** > **Advanced** > **SIP account/SIP IP Call** > **Transport**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Transport	Configures the transport protocol for SIP signaling. The supported protocols are as follows: • **UDP—**it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Note**: • Yealink Cloud Platform and StarLeaf Cloud platform cannot be configured. • The default value of the Zoom/Pexip/BlueJeans/Videxio/Custom Cloud platform is TCP. • The default value of EasyMeet Cloud platform is TLS. • The default value of the SIP account is UDP. • If you use TLS, you need to upload the CA certificate to the server for the devices.	Web user interface Remote control CTP20

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.

About this task

The trusted certificates list contains the default and the custom certificates.

- **Default Certificates**: The system has 36 built-in trusted certificates.
- **Custom Certificates**: You can upload up to 10 trusted certificates with the size no more than 5M to the system. The format of the CA 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	Enables or disables the system to only trust the server certificates in the trusted certificates list. **Note**: the default value is **On**. If it is disabled, the system can connect to the server no matter whether the certificate send by the system is valid or not. 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. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Common Name Validation	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*. **Note**: the default value is **Off**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
CA Certificates	Configures the certificate type in the Trusted Certificates list for the system to authenticate for the TLS connection. • **Default Certificates**—the device authenticates whether the server is reliable via the built-in CA certificates. • **Custom Certificates**—the device authenticates whether the server is reliable via the uploaded CA certificates. • **All Certificates**—the device authenticates whether the server is reliable via both the built-in and the uploaded CA certificates. **Note**: the default value is Default Certificates. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Upload Trusted Certificate File	Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Note**: The format of the certificate must be in *.pem, *.crt, *.cer or *.der. You can upload up to 10 CA certificates.	Web user interface

- *Default Certificates List*

Default Certificates List

The following introduces 36 most common used CA Certificates built in Yealink video conferencing system.

- 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:

The most common used CA Certificates are built in Yealink phones. Due to memory constraints, we cannot ensure a complete set of certificates. If there is no the desired certificate in the above list, contact your distributor for the desired one. After that, you can upload the certificate into your phone. For more information on uploading custom CA certificate, refer to *Transport Layer Security (TLS)* .

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.

About this task

The server certificate contains the default and the custom certificates.

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

  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 or .cer, and the size should be less than 5M.

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. • **Default Certificates** • **Custom Certificates** **Default**: Default Certificates 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**: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. Only one server certificate can be uploaded to the system.	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 RTP and the RTP stream in a call are encrypted by AES algorithm which is compliant with RFC3711. The data in the RTP stream cannot be understood even though it is captured or intercepted. Only the receiver has the key to restore the data. To use SRTP, 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 by the systems. This negotiation process is compliant with RFC 4568.

When you place a call that enables SRTP, the system sends an INVITE message with the RTP encryption algorithm to the destination system.

The rules of SRTP for media encryption in SIP calls are described as below:

Far Local	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish a call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish a call	RTP Call	RTP Call

Example of the INVITE message carried with the RTP encryption algorithm in the SDP is described as below:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
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 replying the 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the 200 message carried with the RTP encryption algorithm in the SDP is described as below:

```
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:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

Note:

If you enable SRTP and you can also enable TLS, which can ensure the security of SRTP encryption. For more information about TLS, refer to *TLS Transport Protocol* .

- *Configuring SRTP*

Configuring SRTP

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/EasyMeet/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **SRTP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
SRTP	Specify the SRTP type. The supported types are as follows: • **Disabled**—the 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**: Off.	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 system provides the identity authentication, the data encryption, and the integration. H.235 encrypts the RTP during H.323 calls to avoid interception and eavesdropping.

The H.235 is supported by the systems. 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 are described as below:

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

- *H.235 Configuration*

H.235 Configuration

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 settings:

Parameter	Description	Configuration Method
H.235 Encryption	Configures the H.235 encryption. The supported types are as follows: • **Disabled**—the encrypted calls are not supported. • **Optional**—both the encrypted and the unencrypted calls are supported. The secure calls are supported only if the far end supports encryption. • **Compulsory**—unencrypted calls are not supported. **Default**: Off.	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 may receive calls from unknown caller, and the calls may be unable to answer. For the communication security, VCS supports the features of defending against attacks. You can configure the abnormal call answering feature to handle the abnormal SIP incoming call or configure the safe mode call feature to verify the H.323 incoming call.

- *Abnormal Call Answering*
- *Configuring the Safe Mode Call*

Abnormal Call Answering

When the destination address of the incoming SIP call does not match the local address, the call is considered to be an abnormal call. You can deal with them by setting them as the abnormal SIP incoming call. You can reject the abnormal SIP incoming call, or answer it by 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 settings:

Parameter	Description	Configuration Method
Abnormal Call Answering	Specifies the account type for answering abnormal SIP incoming calls. The supported types are as follows: • **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. **Default**: IP Call Answer.	Web user interface

Configuring the Safe Mode Call

The safe mode call feature is used to verify whether the incoming H.323 call is coming from an H.323 endpoint.

Procedure

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

Parameter	Description	Configuration Method
Safe Mode Call	Enables or disables the safe mode call feature. The supported types are as follows: • **Off**—Answer incoming H.323 calls directly without validation. • **On**—Verify whether the incoming H.323 call is coming from an H.323 endpoint. If it is, the system will answer it. If not, the incoming call will be rejected. **Default**: Off.	Web user interface

Managing the Directory

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*
- *Cloud Directory*

- *Enterprise Directory*
- *LDAP*
- *Searching for Contacts*
- *Placing Calls to Contacts*
- *Meeting Whitelist*
- *Meeting Blacklist*

Local Directory

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

- *Adding Local Contacts and Conference Contacts*
- *Importing a Local Contact List*
- *Exporting Local Contact List*
- *Editing Local Contacts*
- *Deleting Local Contacts*

Adding Local Contacts and Conference Contacts

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

- *Adding a Local Contact*
- *Adding a Conference Contact*

Adding a Local Contact

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

Procedure

1. Do one of the following:
    - On your web user interface, go to **Directory** > **Local Directory** > **New Contact**.

      If you import the multipoint license to the device, on your web user interface, click **Directory** > **Local Directory** > **New Contact** > **Local**.
    - On your remote control, go to **Dial** > **Directory** > **Local** > **New Contact**.
    - On your CTP20, go to **Dial** > 👤+ .

      Select **Add Local Contact** from the pop-up dialog if the multipoint license is imported to the device.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Name	Configures the contact name.	Web user interface Remote control CTP20
Number	Configures the contact number.	Web user interface Remote control CTP20
Add New Number	You can add up to 3 numbers for the local contact.	Remote control CTP20

Parameter	**Description**	**Configuration Method**
Bandwidth	Select the desired bandwidth from drop-down menu of **Call bandwidth**. The default value is Auto, which means the system will select the appropriate bandwidth automatically. **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 *Specifying the Video Call Rate* .	Web user interface Remote control CTP20

Adding a Conference Contact

You can add 100 conference contacts at most.

About this task

Note: Adding Conference contact is only applicable to VC880/VC800/PVT980/PVT950 system with a multipoint license. It is not applicable to VC500/VC200.

Procedure

1. Do one of the following:
   - If you import the multipoint license to the device, on your web user interface, click **Directory** > **Local Directory**.

     Select the checkboxes of desired local contacts, click **New Contact** > **Conf**.
   - On your remote control, go to **Dial** > **Directory**.

     Select **Conference Contacts** from the drop-down menu.

     Select **New Conference**.
   - On your CTP20, tap **Dial** > 👤+ , and select **Add Conference Contact** from pop-up dialog.
2. Enter the conference name.
3. 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-point license to your VC880/VC800, up to 24 local contacts can be added to a conference contact. For more information the MCU certificate, contact the system administrator.

Related tasks

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**.
2. Click **Import**.
3. Click the import box, and upload the contact file from your computer.
4. Click **Import**.
5. 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. • 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. • Check—delete the old contacts. • Uncheck—do not delete the old contacts.	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 Contact List

You can export a local contact list in XML format from your system. Therefore, you can share it with other systems.

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Click **Export** > **XML/CSV**.

Editing Local Contacts

Procedure

1. Do one of the following:
   - On your web user interface, go to **Directory** > **Local Directory**.

     Hover your cursor over the desired local contact, and click ✎.
   - On your remote control, go to **Dial** > **Directory**.

     Select the desired contact and then press the right key.

     Select **Edit**.
   - On your CP960 conference phone, tap **Directory**.

     Tap ⓘ after the desired contact.
   - On your CTP20, go to **Dial** > **Directory**.

     Tap ⓘ after the desired contact.
2. Edit the contact information.

Deleting Local Contacts

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

- *Deleting a Local Contact*
- *Deleting Multiple Local Contacts*
- *Deleting All Local Contacts*

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 desired local contact, and click 🗑.
   - 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**.
   - On your CTP20, go to **Dial** > **Directory**.

     Tap ⓘ beside the contact, tap 🗑 in the top-right corner, and then tap **Delete Contact**.

   The page prompts whether or not you are sure to delete. There is no prompts on CTP20 when you delete the contact, so the contact is deleted directly.

2. Click **OK**.

Deleting Multiple Local Contacts

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Select the checkboxes of desired local contacts.
3. Click **Delete Contacts**, and select **Selected**.

   The page prompts that whether or not you sure to delete.
4. Click **OK**.

Deleting All Local Contacts

Procedure

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

   It prompts that whether you are sure to delete.
3. Click **OK**.

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 and managed by the 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 four types of Yealink Cloud 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. The enterprise administrator can determine whether to synchronize the permanent VMR to your system or not.

Related tasks

Registering a Yealink Cloud Account

Enterprise Directory

The enterprise directory appears only when you log into the Yealink Meeting Server. The enterprise directory includes all YMS contacts which are created and managed 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 with 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 or not.

Related tasks

Registering a YMS Account

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)

The biggest advantage of LDAP is that users can quickly find contacts from the LDAP server rather than maintaining the local directory. The contact information returned by the LDAP server is read-only, and the user can call an LDAP contact, but cannot add, edit, or delete the LDAP contact. The administrator can configure the filtering conditions of the LDAP request on the devices, such as the number of displayed contacts, the returned information, and how to sort contacts.

The method about how the devices search for contacts on LDAP is described as below:

- Enter the content you want to search in the Dialing interface (ensure that the callee has enabled the LDAP in the matching list).
- In the Contact interface, select the “Colleague” group to go to the LDAP search interface and enter the desired content.

The device sends a search request to the LDAP server, and the LDAP server will search all contacts according to the input content and the filtering condition, and then return the matched result to the device.

- *LDAP Attributes*
- *Configuring LDAP*

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	The unique identifier for each entry
dc	dc	The domain component
-	company	The company or the organization name
-	telephoneNumber	The office phone number
mobile	mobilephoneNumber	The mobile or cellular phone number
ipPhone	IPphoneNumber	The 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**: Off.	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 the system. • **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 the IP address of the LDAP server.	Web user interface
Port	Configure the LDAP server port. **Default**: 389.	Web user interface

Parameter	Description	Configuration Method
LDAP User Name	Configure the user name used to log into the LDAP server. **Note**: The user name is provided by the LDAP server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user name to access the LDAP server.	Web user interface
LDAP Password	Configure the password to log into the LDAP server. **Note**: The password is provided by the LDAP server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the 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.Hits	Configures the maximum number of search results returned by the LDAP server. **Valid Value**: 1 to 32000, **default value**: 50.	Web user interface
LDAP Name Attributes	Configure the name attributes of each record returned by the LDAP server. **Note**: multiple name attributes should be separated by spaces. **Example**: cn sn	Web user interface
LDAP Number Attributes	Configure the number attributes of each record returned by the LDAP server. **Note**: multiple number attributes should be separated by spaces. **Example**: telephoneNumber mobile	Web user interface

Parameter	Description	Configuration Method
LDAP Display Name	Configures the contact attributes displayed on the LCD screen. **Note**: multiple contact 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. If the match is successful, the system will display the caller name when receiving an incoming call. **Default**: Off.	Web user interface
Match Outgoing Call	Enables or disables the system to match outgoing call numbers with LDAP contacts. If the match is successful, the system will display the contact name when placing a call. **Default**: Off.	Web user interface
LDAP Sorting Results	Enables or disables the system to sort the search results in alphabetical order or numerical order. **Default**: Off.	Web user interface

For more information about the string display method of the LDAP search filter, refer to *http://www.ietf.org/rfc/rfc2254*.

Searching for Contacts

You can enter search criteria to find desired contact quickly.

Procedure

1. 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 🔍.
   - On your CTP20, go to **Dial** > 🔍 .

2. Enter a few or all characters of the contact name or numbers in the **Search** field.

   The research result is displayed on the screen.

Placing Calls to Contacts

Procedure

Do one of the following:

- On your web user interface, go to **Directory** > **Local Directory**.

  Click › on the right.

  Click 🎥 or 🎤 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.

  Select **Video Call** or **Voice Call**.
- On your CP960 conference phone, tap **Directory**.

  Tap ⓘ after the desired contact.

  Tap **Video Call** or **Voice Call**.
- On your CTP20, tap **Dial** > **Local**.

  Tap the desired contact.

  If you want to place a voice call, tap ⓘ beside the desired contact, and then select 🎤.

Meeting Whitelist

You can add meeting whitelist. The 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.

- *Adding Meeting Whitelist*
- *Deleting the Meeting Whitelist*

Adding Meeting Whitelist

The users in the whitelist can call you without the password.

Procedure

1. On your web user interface, go to **Directory** > **Meeting Whitelist**.
2. Enter the desired number.

   The value can be the IP address, the account number, or the domain name.
3. Click **Add**.

   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.

Deleting the Meeting Whitelist

Procedure

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

   It prompts whether you are sure to delete the whitelist.
3. Click **OK**.

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*
- *Deleting the Meeting Blacklist*

Adding Meeting Blacklist

Your system will refuse incoming calls from the blacklist automatically.

Procedure

1. On your web user interface, go to **Directory** > **Meeting Blacklist**.
2. Enter the desired number.

   The value can be the IP address, the account number, or the domain name.
3. Click **Add**.

Deleting the Meeting Blacklist

Procedure

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

   It prompts whether you are sure to delete the blacklist.
3. Click **OK**.

Managing the Call Log

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*
- *Adding a History Record to the Local Directory*
- *Deleting History Records*
- *Placing Calls from Call History*

Saving History Record

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

Procedure

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

Parameter	Description	Configuration Method
Saving History Record	Enable or disable the system to log the call history (missed calls, placed calls, and received calls) in the call lists. **Default**: On.	Web user interface Remote control

Adding a History Record to the Local Directory

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 **Add to Contact**.
    - On your CP960 conference phone, tap **History**.

      Tap ⓘ beside the desired history record, and then tap **Delete**.
    - On your CTP20, go to **Dial**.

      Select the type of history record, tap ⓘ beside the desired history record, and then tap **Delete**.
2. Edit the corresponding information and save the information.

Deleting History Records

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

- *Deleting a History Record*
- *Deleting Multiple History Records*
- *Deleting All History Records*

Deleting a History Record

Procedure

1. Do one of the following:
    - On your remote control, go to **Dial** > **Directory**.

      Select the desired entry 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**.

- On your CTP20, go to **Dial**.

  Select the desired history record, tap ⓘ beside the desired entry, and tap 🗑 in the top-right corner, and then tap **Delete**.

  The page prompts whether or not you sure to delete. There is no prompts on CTP20 when you delete the entry, so the entry is deleted directly.

2. Click **OK**.

Deleting Multiple History Records

Procedure

1. On your web user interface, go to **Directory** > **History**.
2. Select the checkboxes of desired history records.
3. Click **Delete Contacts**, and select **Selected**.

Deleting All History Records

Procedure

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 drop-down menu of **All Calls**.

  Select **Delete**.
- On your CTP20, go to **Dial**.

  Select the desired type of history record, tap **Clear** at the bottom, and tap **Clear All** from the poo-up box.

Placing Calls from Call History

Procedure

Do one of the following:

- On your web user interface, go to **Directory** > **History**.

  Click 📹 or 🎙 beside the desired entry to place a video or audio call.
- On your remote control, go to **Dial** > **History**.

  Select the desired history record and then press the right pan key to select **Video Call** or **Voice Call**.
- On your CP960 conference phone, tap **History**.

  Tap ⓘ beside the desired history record and then tap **Video Call** or **Voice Call**.
- On your CTP20, go to **Dial**.

  Select the desired call type and tap the desired entry.

  If you want to place a voice call, tap ⓘ beside the desired contact, and then select 🎙.

Placing a Call

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

- *Placing a Call by Entering a Number*
- *Placing a Call from the Search Result*
- *Placing a Call from the Search Result by CTP20*
- *Editing Numbers Before Calling*
- *Editing Numbers before Calling by CTP20*

Placing a Call by Entering a Number

You can place a call by using the web user interface, the remote control or the CP960 conference phone.

About this task

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

Do one of the following:

- On your web user interface, go to **Home**.

  Enter the number in the **Enter Number** field.

  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**.

  Select the desired call type from the drop-down menu of **Call Type**.

  Enter the number.

  Press the right navigation key to select 📹 (video call) or 🎤 (voice call).
- On your CP960 conference phone, tap **Dial**.

  Tap **Auto**, and select the desired call type from the drop-down menu.

  Enter the number.

  Tap **Send** to place a video call.
- On your CTP20, tap **Dial**.

  In the bottom-right corner, tap **Auto** and select the desired call type from the drop-down menu.

  Enter the number.

  Tap ☎.

Related tasks

Specifying the Video Call Rate

Related information

Account Polling

Placing a Call from the Search Result

You can enter the 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 You can place a call from the search result by using the web user interface, the remote control or the CP960 conference phone.

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 from the drop-down menu of **Call Type**.
3. Enter a few or all characters of the contact name or numbers in the Search field.
4. Select the desired search result and dial.

Related information

Search Source List in Dialing

Configuring Call Match

Placing a Call from the Search Result by CTP20

Procedure

1. On your CTP20, tap **Dial**.
2. Optional: In the bottom-right corner, tap **Auto** and select the desired call type from the drop-down menu.
3. Enter the contact name or number in the **Dial/Search** box.
4. Select the desired contact form the search result to call.

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 entry and then press the right navigation key.

     Select **Edit before calling.**
   - On your CP960 conference phone, tap **Dial** or tap **History**.

     Tap ⓘ after the desired history record.

     Tap **Edit before calling**.
2. Edit the number and dial out.

Editing Numbers before Calling by CTP20

Procedure

1. On your CTP20, tap **Dial**.

2. Select the desired call type.
3. Tap ⓘ after the desired call history.
4. Tap **Edit before calling**.
   The selected call history will be filled in the dialing input box automatically.
5. Edit the number and dial out.

Accessories with Your System

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*
- *Using the CPW90-BT Bluetooth Wireless Microphones with VCS*
- *Using CTP20*
- *Using VCM34*

Using the VCC22 Video Conferencing Cameras

You can connect up to 9 VCC22 video conferencing cameras to the VC880/PVT980 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/PVT950 video conferencing endpoint.

- *Controlling VCC22 Camera*
- *Configuring Multi-Camera Default Layout*
- *Adjusting the Camera Layout During a Call*

Controlling VCC22 Camera

When the system is idle, you can choose the desired camera to capture video images, and adjust the camera angle and focal length.

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 go to the cameras list.
   - On your CP960 conference phone, tap **Camera** > **The current control camera**.
   - On your CTP20, tap **Camera**.
2. Select the desired camera and then adjust the angle and the focus.

Configuring Multi-Camera Default Layout

During a call, if you connect VCC22, all the local video streams are synthesized to one video stream, and sent to the far site. You can configure the default layout when you connect multiple cameras.

Procedure

1. On your web user interface, go to **Setting** > **Camera** > **Camera** > **Multi-camera Default Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Multi-camera Default Layout/ Camera Layout	Configures the camera layout during a video call. • **1+N**: the selected camera is given prominence in the largest pane, and other cameras are displayed in small panes. • **Selected Speaker**: the selected camera is displayed in the full screen. • **Equal N×N**: every camera is displayed in equal panes. **Default**: 1+N.	Web user interface Remote control CP960 Conference Phone CTP20

Adjusting the Camera Layout During a Call

During a call, all video streams captured from the connected 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 during a call, on your web user interface, go to **Home** > **Camera Layout**.
   - When the system is during a call, on your remote control, press ≡ or OK key to open Talk Menu, and select **Layout Adjustment** > **Camera Layout**.
   - When the system is during a call, on your CP960 conference phone, tap **Layout**.
   - When the system is during a call, on your CP960 conference phone, tap **Layout** > **Camera Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Camera Layout	Configures the camera layout during a video call. • **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. **Default**: 1+N.	Web user interface Remote control CP960 Conference Phone CTP20

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-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. For more information, refer to *CPW90-BT Bluetooth Wireless Microphones Quick Start Guide*.

- *Registering CPW90-BT with VCS*
- *Deregistering CPW90 from VCS*
- *Viewing the Information of Bluetooth Wireless Microphones*
- *Finding the Registered CPW90-BT*

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 video conferencing system is VC500/VC800/VC880/PVT980/PVT950, 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 **Setting** > **Wireless Microphone** > **Search Mic**.
   - On your remote control, go to **More** > **Setting** > **Video & Audio** > **Wireless Microphone** > **Add Wireless Microphone**.
   - On your CTP20, tap **Setting** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.
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.

   Note: Up to 2 Bluetooth wireless microphones can be connected to one video conferencing system.

Deregistering CPW90 from VCS

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Wireless Microphone** > **Deregistration**.
   - On your remote control, go to **More** > **Setting** > **Video & Audio** > **Wireless Microphone**.

     Select a wireless microphone and then select **Unbind**.
   - On your CTP20, tap **Setting** > **Audio** > **Wireless Microphone**.

     Select a wireless microphone and then select **Unbind**.

   The page prompts whether or not you are sure to unbind.
2. Click **OK**.

Viewing the Information of Bluetooth Wireless Microphones

Procedure

1. Do one of the following:

- On your web user interface, go to **Setting** > **Wireless Microphone**.
- On your remote control, go to **More** > **Setting** > **Video & Audio** > **Wireless Microphone**, and select the desired wireless microphone.
- On your CTP20, go to **Setting** > **Audio** > **Wireless Microphone**, and select the desired wireless microphone.

2. Select a desired microphone to view the information.

Finding the Registered CPW90-BT

Procedure

1. Do one of the following:

- On your web user interface, go to **Setting** > **Wireless Microphone**.
- On your remote control, go to **More** > **Setting** > **Video & Audio** > **Wireless Microphone**.
- On your CTP20, tap **Setting** > **Audio** > **Wireless Microphone**.

2. Select a wireless microphone and then select **Find**.

The mute indicator LED on the CPW90-BT flashes red and green alternately.

Using CTP20

- *Wired Connection to CTP20*
- *Wireless Connection to CTP20*
- *Using Multiple CTP20s for Collaboration*

Wired Connection to CTP20

After connected to the VC Hub/Phone port via the network cable, CTP20 will be connected to the VCS automatically. For more information, refer to *Yealink_CTP20_Quick_Start_Guide*.

Wireless Connection to CTP20

If the VC Hub/Phone port of the VCS codec is used, you can connect the CTP20 to the PoE switch for power supply, also to the wireless access point provided by the VCS codec.

Before you begin

Make sure the Wireless AP is enabled and the codec is connected to WF50.

About this task

If the codec connects to the wireless network and the Wireless AP is disabled, the CTP20 cannot use the wireless connection.

Procedure

1. Enable **Wi-Fi**.

2. Select the Wi-Fi supplied by the VCS codec.

3. Enter the password and tap **OK**.
After connecting to the wireless network, you can use the CTP20 to work with VCS codec.

Related tasks

Enabling the Wireless Access Point

Configuring Wireless Access Point

Using Multiple CTP20s for Collaboration

In a meeting room, you can use multiple CTP20s for whiteboard collaboration or presentation. Up to 4 CTP20s can be connected to a VCS codec simultaneously.

The collaboration methods are as below:

- **Status Synchronizing**: The status of the VCS codec can be synchronized to all connected CTP20s.
- **Configuration Synchronizing**: in idle state, you can configure the VCS codec via each CTP20, and the new configuration will cover the old configuration and take effect immediately.
- **Whiteboard Collaboration**: you can use each CTP20 to initiate the whiteboard collaboration which can be received by other CTP20s simultaneously, but the editing and noting on each CTP20 are independent. If you close the whiteboard of one CTP20 connected to a VCS codec, the whiteboards of other connected CTP20s are closed simultaneously.
- **Presentation Collaboration:** if you enable the feature of auto-presentation on devices, after you start presenting on the local computer/Apple devices, the presentation will be synchronized to all the CTP20s, but the editing and noting on each CTP20 are independent. If you do not enable the feature of auto-presentation on devices, you can initiate the presentation on any CTP20 and the presentation will be synchronized to all the CTP20s, but the editing and noting on each CTP20 are independent. If you close the presentation on one CTP20 connected to a VCS codec, the presentation on other connected CTP20s are closed simultaneously.

Note: If multiple CTP20s are wired to the VCS codec, you need a multi-port switch.

Related information

Controlling the Shared Content by CTP20

Using the Whiteboard Feature of CTP20

Using VCM34

To further improve the sound quality, you can connect VCM34 to the VCS codec. If you need to expand the pickup range, you can connect to multiple VCM34s in cascade (up to 4 VCM34s). For more information, refer to *Yealink_VCM34_Quick_Start_Guide*.

System Maintenance

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*
- *Rebooting the System*
- *Resetting the SD Card*
- *Resetting the System*
- *Exporting Log Files*
- *Capturing Packets*
- *System Firmware*
- *Licenses*

Exporting or Importing Configuration Files

You can export the configuration files to check the current configuration of the system and to troubleshoot if necessary. You can also import configuration files for a quick and easy configuration. The format of the imported configuration file must be “*.bin”.

- *Exporting BIN Files from the System*
- *Importing BIN Files to the System*

Exporting BIN Files from the System

Procedure

1. On your web user interface, go to **Setting** > **Configurations** > **Configuration** > **Export Configuration**.
2. Click Export.

Importing BIN Files to the System

Procedure

1. On your web user interface, go to **Setting** > **Configurations** > **Configuration** > **Import 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

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**.
- On your CTP20, tap **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

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**.
- On your CTP20, tap **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.

- *Resetting the System via Configuration Methods*
- *Resetting the System by using Reset Button*

Resetting the System via Configuration Methods

If you use configuration methods to reset your system, the system, the connected CP960 conference phone and the connected VCC22 video conferencing camera are reset simultaneously.

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**.
   - On your remote control, go to **Setting** > **Advanced** > **Reboot & Reset** > **Reset**.

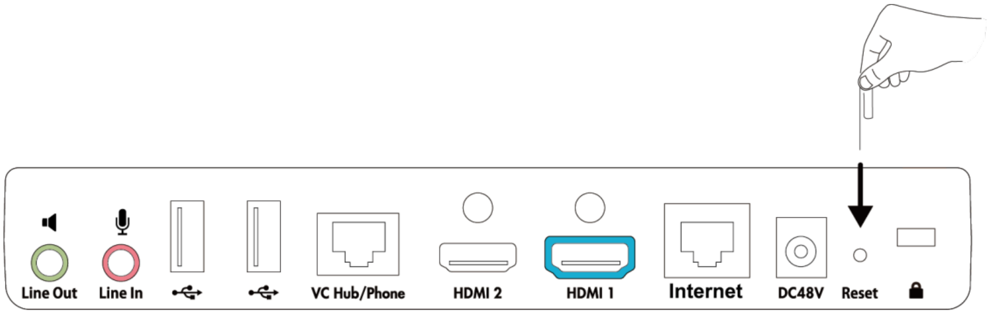
   It prompts whether or not you are sure to reset.
2. Select **OK**.

Resetting the System by using Reset Button

If you use the reset button to reset your system, the system, the CP960 conference phone (if connected) or VCC22 video conferencing camera (if connected) are reset synchronously.

Procedure

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.



Attention:

Do not power off the system when resetting to the factory settings.

Exporting Log Files

Log files are essential when troubleshooting the phone issues. Log files contain information about phone activities and the phone configuration profile. You can also export the log to the local PC or to a specific syslog server.

- *Setting the Severity Level of the Local log*
- *Setting Severity Level of the Module log*
- *Exporting the Log Files to a Local PC*
- *Exporting the Log Files to a USB Flash Drive*
- *Exporting the Log Files to a Syslog Server*

Setting the Severity Level of the Local log

Procedure

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

Parameter	Description	Configuration Method
Local Log	Specify the local 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 **6**-informational **Note**: the default value is 6. The smaller the number is, the higher the priority is. Higher value indicates more detailed content.	Web user interface
Max Log File Size	Limit the maximum size (kb) of local log files. **Default**: 20480.	Web user interface

Setting Severity Level of the Module log

You can configure severity level of each module of the system.

Procedure

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

Parameter	Description	Configuration Method
Module Log Level	Specify the module log level. • All—all modules • Driver • System • Service • Connectivity • Video & Audio • Protocol • Deploy • Web • App • Talk The available levels are as below: • 0 • 1 • 2 • 3 • 4 • 5 • 6 **Default**: all, 6. If you set the log level for a specified module and then set the log level for all modules, the log level of a specified module will be overwritten by the log level of all modules.	Web user interface

Exporting the Log Files to a Local PC

You can export local log to your computer.

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. In the **Enable Local Log** field, select **On**.
3. Reproduce the issue.
4. In the **Export Local Log** field, click **Export**.

Note:

The severity level of the exported Module Log will not be greater than the local Log Level. For example: If you set Local Log Level to 3 and set Talk log Level to 6, the exported Talk log Level will still be 3 in your exported local log. If you set Local Log Level to 5 and set Talk log Level to 4, the exported Talk log Level will be 4 in your exported local log.

Exporting the Log Files to a USB Flash Drive

You can export local log to the connected USB flash drive.

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. In the **Enable Local Log** field, select **On**.
3. In the **USB Auto Exporting Syslog** field, select **On**.
4. Reproduce the issue.

   A folder named yealink.debug appears in your USB flash drive, which includes the log files.

   Note:

   The severity level of the exported Module Log will not be greater than the local Log Level. For example: If you set Local Log Level to 3 and set Talk log Level to 6, the exported Talk log Level will still be 3 in your exported local log. If you set Local Log Level to 5 and set Talk log Level to 4, the exported Talk log Level will be 4 in your exported local log.

Exporting the Log Files to a Syslog Server

You can also configure the phone to send syslog messages to a syslog server in real time.

Procedure

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

Parameter	Description	Configuration Method
Enable Syslog	Select **On** to enable the system to upload log messages to the syslog server. **Default**: On.	Web user interface
Syslog Server	Configures the IP address or the domain name of the syslog server.	Web user interface
Port	Configures the port of the syslog server.	Web user interface
Syslog Transport Type	Configures the transport protocol that the device uses when exporting log messages to the syslog server. • UDP • TCP • TLS **Default**: UDP.	Web user interface

Parameter	Description	Configuration Method
Syslog Level	Specifies the level of syslog information that displayed in the syslog. **0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational **Note**: the default value is 6. Higher value indicates more detailed content.	Web user interface
Syslog Facility	Configures the facility that generates the log messages. **Default**: Local Use 0.	Web user interface
Syslog Prepend Mac	Configures whether or not the uploaded log messages include the phone MAC address. **Default**: Off.	Web user interface

Note:

The severity level of the exported Module Log will not be greater than the Syslog Level. For example, if you set Syslog Level as 3 and set Talk log Level as 6, the exported Talk log Level will still be 3. If you set Local Log Level as 5 and set Talk log Level as 4, the exported Talk log Level will be 4.

Capturing Packets

You can capture packets in three ways: capturing the packets via web user interface, on the remote control or using the Ethernet software. You can analyze the packet captured for troubleshooting.

- *Capturing the Packets via Web User Interface*
- *Capturing the Packets via Remote Control*
- *Capturing the Packets via Ethernet Software*

Capturing the Packets via Web User Interface

You can capture the packets via the web user interface. You can also download the captured packets to your computer. The video conferencing system supports the following two modes for capturing packets:

- **Enhanced**: directly exporting the packets file to local PC while capturing.
- **Normal**: manually exporting the packets file to local PC after stopping capturing.

- *Capturing the Packets in Enhanced Way*

- *Capturing the Packets in Normal Way*

Capturing the Packets in Enhanced Way

You can capture more packets in enhanced way than normal mode.

Procedure

1. On your web user interface, go to **Setting** > **Configuration**.
2. Select **Enhanced** from the drop-menu of **Pcap Type**.
3. In the **Pcap Feature** field, click **Star**t to start capturing enhanced packets.
4. Reproduce the issue to get stack traces.
5. Click **Stop** to stop capturing.

Capturing the Packets in Normal Way

Procedure

1. On your web user interface, go to **Setting** > **Configuration**.
2. Select **Normal** from the drop-menu of **Pcap Type**.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Packet Capture Device	Configures the port where you want to capture packets: • **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 Count	Configures the count of the number of packets to capture. **Default**: 5.	Web user interface
Packet Capture Clip KB	Configures the number of bytes (in kb) of the packet to capture. **Default**: 1024.	Web user interface

Parameter	Description	Configuration Method
Pcap Filter Type	Configures the filter type of the packet to capture. The supported types are as follows: • **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. For more information, refer to *Capturing Packet Filter String* . **Note:** the default value id blank. It works only when you set the Pcap Filter Type to Custom.	Web user interface

4. Click **Confirm**.
5. In the **Pcap Feature** field, click **Star**t to start capturing enhanced packets.
6. Reproduce the issue.
7. Click **Stop** to stop capturing.
8. Click **Export** to open the file download window, and then save the file to your local system.

- *Capturing Packet Filter String*

Capturing Packet Filter String

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 If no protocol is specified, all the protocols are used. Note that the application-level protocol, such as http, dns and sip are not supported.
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".

Syntax	Description
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 the source IP address 10.4.1.12 or the source network 10.6.0.0/16, and the result is 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 the remote control, and store the packets to the USB flash drive.

Before you begin

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

Procedure

1. On the idle screen or during a call, long press ⌫.

   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 drive.

Related tasks

Configuring USB Storage

Capturing the Packets via Ethernet Software

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. Therefore, 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).

Device model	Firmware Name	Example
VC200 video conferencing system	80.x.x.x.rom	80.40.0.10.rom
VC880 video conferencing system	63.x.x.x.rom	63.40.0.10.rom
VC800 video conferencing system		
VC500 video conferencing system		
Hardware of VCC22 Video Conferencing Camera		
PVT980 video conferencing system	1345.x.x.x.rom	1345.32.0.40
PVT950 video conferencing system		
CP960 Conference Phone	73.x.x.x.rom	73.83.0.45.rom
Hardware of WPP20 Wireless Presentation Pod	81.x.x.x.rom	81.40.0.10.rom
CTP20 Touch Panel	85.x.x.x.rom	85.40.0.10.rom

You can download the latest firmware online: *http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage*.

- *Upgrading the Firmware*

Upgrading the Firmware

You can upgrade firmware for the system and accessories.

About this task

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. Click the white box beside the desired firmware.
3. Click **Upgrade** to upgrade the firmware.

   Note: If you connect multiple CTP20s to the VCS codec, all the firmware of CTP20s will be updated simultaneously.

Licenses

- *Importing Device Type License*
- *Viewing Device Type*
- *Multipoint Licenses*
- *Viewing Multipoint License Status*

Importing Device Type License

About this task

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. You can get the device type license from Yealink technical support. After changing to a normal machine, the system supports 1 video call and 5 voice calls (1 conference creator and 6 participants).

Procedure

1. On your web user interface, go to **Security** > **License**.
2. Click the **Load License File** filed.
3. Select the device type license from your local system.

   The file format must be *.dat.
4. Click **Upload** to import the device type license.

Viewing Device Type

You can view the device type.

Procedure

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** > **License**.
- On your CTP20, tap **Setting** > **Host Status** > **System**.

Parameter	Description	Configuration Method
Device Type	Indicate the device type. • Demo machine • Normal Machine	Web user interface Remote control CP960 Conference Phone CTP20

Multipoint Licenses

Only VC880/VC800/PVT980/PVT950 supports multipoint licenses. In additional, because PVT980 has built-in-8-way multipoint license and PVT950 has built-in-4-way multipoint license, the user do not need to import the license again. Only after importing multipoint license can VC880/VC800 be used to initiate multi-party video conferences.

Multipoint licenses are described as below:

Multipoint License Type	Maximum Connections	Description
VC880/VC800/VC500/VC200 without a multipoint license	One video call with a presentation and 5-way voice calls (a conference moderator and 6 participants).	Multipoint video conferences are unsupported.

Multipoint License Type	Maximum Connections	Description
PVT980 with an 8-way multipoint license	8-way video call with a presentation and 5-way voice call (a conference moderator and 13 participants).	Multipoint video conferences are supported.
PVT950 with built-in-4-way multipoint license	4-way video call with a presentation and 5-way voice call (a conference moderator and 9 participants).	Multipoint video conferences are supported.
VC880/VC800 with a trial multipoint license	24-way video call with a presentation (a conference moderator and 24 participants)	**Period of validity**: 15-day free trial. VC880/VC800 share this trial multipoint license. You can download it from the Yealink website.
VC880/VC800 with a 8-way multipoint license	8-way video call with a presentation and 5-way voice call (a conference moderator and 13 participants).	**Period of validity**: eternal. One unique worldwide license for every VC880/VC800, which cannot be used by other devices. You can purchase the license from the Yealink by providing the MAC address of your VC880/VC800.
VC880/VC800 with a 16-way multipoint license	16-way video call with a presentation and 5-way call (a conference moderator and 21 participants).	
VC880/VC800 with a 24-way multipoint license	24-way video call with a presentation (a conference moderator and 24 participants)	

- *Importing Multipoint License*

Importing Multipoint License

Procedure

1. On your web user interface, go to **Security** > **License**.
2. Click **Load License File** filed 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** > **License**.
   - On your CTP20, tap **Setting** > **Host System**.
2. The multipoint licenses status is described as below:

Parameter	Description	Configuration Method
Multipoint Status	Indicates whether or not a multipoint license has been imported to the system. • Active • Inactive (without a multipoint license or the imported multipoint license has expired)	Web user interface Remote control CP960 Conference Phone CTP20
Multipoint Ways	Indicates that the multipoint license is imported to the system. • Unsupported • 8 points • 16 points • 24 points	Web user interface Remote control CP960 Conference Phone CTP20
Period of validity/Period	Indicates the validity period of the imported multipoint license. • Unsupported • X~Y Available • Eternal	Web user interface Remote control CP960 Conference Phone CTP20

Note:

Upgrading the system or performing a factory reset will not affect the imported multipoint license.

If you import a trial multipoint license to the system and the license has not expired, and then you import a permanent multipoint license to the system, the trial multipoint license will be overwritten. On the contrary, 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.

Troubleshooting

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, and the cables are loose and the connections are correct or not. All these are common issues.

- *General Issues*
- *Call Issues*
- *Audio Issues*
- *Video Issues*
- *Placing a Test Call*
- *System Diagnostics*
- *System Status*
- *Viewing Call Statistics*

General Issues

Situation	Cause	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 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 the remote control.
You forget the administrator password for the system	You cannot access the advanced settings.	Reset your system.
Time and date are wrong	The system fails to obtain the time and date from the SNTP server automatically.	Contact your network administrator.
		Configure the time and date manually.
You cannot adjust the camera angle and the 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 the 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

Situation	Reason	Solution
You cannot receive calls.	The network is unavailable.	Connect the network administrator.

Situation	Reason	Solution
	Your system cannot receive calls when the far site dials your account.	Check whether your account is registered.
	DND (Do Not Disturb) mode is enabled.	Disable DND.
You fail to call far site.	The far site enables DND (Do Not Disturb) mode.	Contact the far site to disable DND.
	The account is not registered	Check whether the call parties register the accounts.
	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. Connect the network administrator.
	The far site system is powered off.	Contact the far site to power on the system.
	The call protocol(SIP/H.323) that far site uses is different from yours.	Both sites use the same call protocol (SIP/H.323).
	Encryption negotiation (SRTP/H.235) fails.	If one site uses encryption, ensure that the other site enables the encryption too.
	The firewall blocks the traffics.	Open necessary ports on the firewall.
	Your monitor prompts: Call Fail Busy Here. • 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. Far site rejects your H.323 call • 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.

Situation	Reason	Solution
	Your monitor prompts: Maximum number of sessions reached.	The maximum sessions is depend on the multipoint license imported to the system.

Audio Issues

Symptom	Reason	Solution
You cannot hear the audio during a call.	The volume is set to 0.	Adjust the volume.
	The far site mutes the microphone.	Contact the far site to check whether the microphone is unmuted.
You cannot hear the audio clearly during a call.	The speaker volume is too low.	Adjust the volume.
	The 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.
	Dust and debris may cause the 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.
	The speaker of the far site is obscured or damaged.	Ensure that speaker is not obscured or damaged. Do not stack items on top of the CP960 conference phone.
	Your microphone is muted	Unmute the microphone.
	The volume of the far site is set to 0.	Contact the far site to adjust the volume.
You may experience poor voice quality during a call, such as intermittent voice, echo or other noise.	The users sit too far from or near to the microphone.	Adjust the 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.

Symptom	Reason	Solution
You cannot hear the ring tone when receiving a call.	The volume is set to 0.	Adjust the volume.

Video Issues

Situation	Reason	Solution
Picture is blank on the monitor.	The system is in sleep mode.	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.	Make sure that the monitor is connected correctly according to the Quick Start Guide.
The video quality is poor.	Unsuitable monitor resolution.	Unsuitable monitor resolution.
	The packet is lost.	View the call statistics to check whether the packet is lost and contact the network administrator.
	Unsuitable camera parameters.	Adjust the camera parameters, such as the brightness and the white balance.
	High-intensity indoor light or direct sunlight on the camera.	Avoid those situations.
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.	• 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.

Situation	Reason	Solution
The far site displays black screen when you share contents.	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.	You can configure network address adapter to let the content send to the actual public IP address. Procedure: • On your web user interface, go to **Setting->Call Features**. • Select the desired value from the drop-down menu of **Network Address Adapter**: • **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. If you fail to establish a call with Yealink Demo site, contact your network administrator to check whether or not the intranet works.

System Diagnostics

You can diagnose the audio, camera and network.

- *Diagnosing the Audio*
- *Diagnosing the Camera*
- *Diagnosing the Network*

Diagnosing the Audio

You can check whether the speaker connected to your system can pick up voice and play audio normally.

Procedure

1. Do one of the following:
   - On your remote control, go to **More** > **Setting** > **Diagnose** > **Audio Diagnose**.
   - For VC200: on your remote control, go to **More** > **Diagnose** > **Audio Diagnose**.
   - On your CTP20, tap **Setting** > **Diagnose** > **Audio Diagnose**.
2. Speak to the microphone.
3. Check whether or not the microphone can pick up the sound properly.

4. If the microphone can pick up the sound properly and play it, the audio can work.
5. For the remote control, press OK key/for CTP20, tap **Stop** to stop diagnosing.

Diagnosing the Camera

You can check whether the camera can pan and change the focus normally.

Procedure

1. Do one of the following:
    - On your remote control, go to **More** > **Setting** > **Diagnose** > **Camera Diagnose**.
    - For VC200: on your remote control, go to **More** > **Diagnose** > **Camera Diagnose**.
    - On your CTP20, tap **Setting** > **Diagnose** > **Camera Diagnose**.
2. Tap the navigation keys to adjust the camera angle.
3. Press ⊖ or ⊕/⊖ or ⊕ to zoom out or zoom in.
4. If the camera can move and zoom normally, it means that the camera is working well.
5. On your remote control, press ↩ to stop diagnosing.

    On your CTP20, tap **Diagnose** to stop diagnosing.

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*
- *Checking the Network Using "Trace Route" Method*

Checking the Network Using "Ping" Method

The Ping method can help you check whether the system can be connected to the IP address of the remote device.

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **Diagnose**, and select **Ping** from the drop-down menu of **Command**.
    - On your remote control, go to **More** > **Setting** > **Diagnose** > **Ping**.
    - For VC200: on your remote control, go to **More** > **Diagnose** > **Ping**.
    - On your CTP20, tap **Setting** > **Diagnose** > **Ping**.
2. Select **Start**.
3. You can also ping other IP addresses.
4. Select **Stop**.

Checking the Network Using "Trace Route" Method

You can use the 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 the congestion happens by viewing the time cost among the hops.

Procedure

1. Do one of the following:
    - On your web user interface, go to **Network** > **Diagnose**, and select **Trace Route** from the drop-down menu of **Command**.

- On your remote control, go to **More** > **Setting** > **Diagnose** > **Trace Route**.
- For VC200: on your remote control, go to **More** > **Diagnose** > **Trace Route**.
- On your CTP20, tap **Setting** > **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*
- *Viewing System Status*

System Status List

The available status is listed below:

Parameter	Description	Method
System	• System model • Firmware version • Hardware version • Product ID	Web user interface Remote control CP960 Conference Phone
	• Uptime	Web user interface
Touch Panel	• System model • Firmware version • Hardware version	Web user interface Remote control CTP20 Touch Panel
VCP960 Conference Phone	• System model • Firmware version • Hardware version • Device model • IP address • MAC address	Web user interface Remote control (The firmware version is available on CP960)
WPP20 Status (WPP20 is connected to the codec)	• Firmware version	Web user interface
Network	• Network type • Internet Port/IP Mode	Web user interface Remote control CTP20 Touch Panel

Parameter	Description	Method
IPv4	• Internet port type • IP address • Subnet mask • Gateway • DNS server	Web user interface Remote control CP960 Conference Phone CTP20 Touch Panel
Network Common	• Public IP address • MAC address • Wi-Fi MAC Address	Web user interface Remote control CTP20 Touch Panel
AP Status (if Wi-Fi AP is enabled)	• AP enabled • AP name • Security mode • Password • Network sharing • Band • Channel	Web user interface Remote control CTP20
Account status	• The registration status of the Cloud platform • The registration status of the SIP account • The registration status of the H.323 account • The registration status of the PSTN account	Web user interface Remote control CP960 Conference Phone CTP20
Camera	• Status • Device model • Specification • Hardware version	Web user interface Remote control CP960 Conference Phone CTP20
Audio	• Active microphone • Active speaker	Web user interface Remote control CP960 Conference Phone CTP20
VCS Phone	• Status	Remote control
	• Serial number • Firmware version • Hardware version • Device model • IP address • MAC	Web user interface Remote control CTP20

Parameter	Description	Method
License	• Device Type • Multipoint Status • Multipoint Ways • Period of validity	Web user interface Remote control CP960 Conference Phone CTP20

Viewing System Status

Procedure

1. 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**.
   - On your CTP20, tap **Setting**.
2. Select the desired list to view the status.

   For CTP20, you can view the corresponding status in the module of **Collaboration Touch Panel** or **Host Status**.

Viewing Call Statistics

About this task

If voice quality is poor during a call, you can view call statistics to find out the reason. The call statistics includes:

- **Bandwidth**: the received and the sent bandwidth.
- **Video**: the definition, the codec, the bandwidth, the frame rate, the jitter, the packet and its loss rate.
- The protocol used to placing calls.
- The device information.
- **Audio**: the codec, the bandwidth, the sample rate, the frame rate, the jitter, the packet and its loss rate.
- **Content**: the codec, the bandwidth, the definition and the frame rate.

Procedure

Do one of the following during a call:

- On your web user interface, go to **Home**.

  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.
- On your CTP20, tap ⋯ > **Call Statistics**.

  If you are having a conference, tap **Participant**, and tap **Call Statistics** beside the desired participant.