VC110 Video Conferencing Endpoint Admin Guide

Version 10.6
Oct. 2015

Copyright

Copyright © 2015 YEALINK NETWORK TECHNOLOGY

Copyright © 2015 Yealink Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

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

Warranty

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

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

Declaration of Conformity

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

CE Mark Warning

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

Part 15 FCC Rules

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

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

Class B Digital Device or Peripheral

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

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

WEEE Warning

To avoid potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. WEEE must not be regarded as unsorted municipal waste and must be collected and disposed of separately by a competent authority.

Customer Feedback

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

About This Guide

Thank you for choosing the Yealink VC110 full HD video conferencing endpoint. It is an all-in-one unit that supports 1080P-full HD video conferencing and includes outstanding features such as good compatibility, easy deployment and intelligent network adaptability. These make it the best choice for SME.

The Yealink VC110 full-HD video conferencing endpoint is designed to help enterprises organize video conferences easily and efficiently. Users can expect to enjoy the high-quality video conferencing experience very cost-effectively.

The guide is intended for administrators who need to configure, customize, manage, and troubleshoot the video conferencing endpoint properly, rather than for end-users. It provides details on the functionality and configuration of the Yealink VC110 endpoint.

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

Documentations

This guide covers the VC110 video conferencing endpoint. In addition to the administrator guide, the following related documents are available:

- Quick Start Guide, which describes how to assemble the endpoint and configure basic network features on the endpoint.
- User Guide, which describes how to configure and use basic features available on the endpoints.
- Video Conference Room Deployment Solution, which describes the conference room layout requirements and how to deploy the endpoints.

You can download the above 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://www.yealink.com/Support.aspx.

Firmware

Common reasons for updating firmware include fixing bugs or adding features to the device. You can download the latest firmware for your product online:
http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage

For more information on how to upgrade the endpoint firmware, refer to Upgrading Firmware on page 193.

In This Guide

This administrator guide includes the following chapters:

- Chapter 1, "VC110 Video Conferencing Endpoint Introduction" describes endpoint components, icons and Indicator LEDs.
- Chapter 2, "Getting Started" describes how to install and start up the endpoint and configuration methods.
- Chapter 3, "Configuring Network" describes how to configure network features on the endpoint.
- Chapter 4, "Configuring Call Preferences" describes how to configure call preferences on the endpoint.
- Chapter 5, "Configuring Endpoint Settings" describes how to configure basic, audio and video features on the endpoint.
- Chapter 6, "Endpoint Management" describes how to manage endpoint contacts and call history.
- Chapter 7, "Configuring Security Features" describes how to configure security features on the endpoint.
- Chapter 8, "Endpoint Maintenance" describes how to upgrade endpoint firmware and reset the endpoint.
- Chapter 9, "Troubleshooting" describes how to troubleshoot the endpoint and provides some common troubleshooting solutions.

Table of Contents

About This Guide v

Documentations v
Firmware v
In This Guide vi

Table of Contents vii

VC110 Video Conferencing Endpoint Introduction 1

VoIP Principles 1
Physical Features of Endpoint 2
Packaging Contents 3
VC110 All-in-one Package 4
VCM60 Package 5
VCP40 Package 6
VCM30 Package 7
Endpoint Component Instructions 7
VC110 All-in-one Unit 7
Cable Hub 11
VCM60 Video Conferencing Wireless Microphone 11
VCP40 Video Conferencing Phone 21
VCM30 Video Conferencing Microphone Array 24
VCR10 Remote Control 27
Icon Instructions 29
Icons on Display Device 29
Icons on the VCP40 Video Conferencing Phone 31
LED Instructions 31
User Interfaces 33
Remote Control 33
Web User Interface 33

Getting Started 35

Endpoint Connection and Installation 35
Connecting the VC110 Video Conferencing Endpoint 36
Installing the VC110 Video Conferencing Endpoint 37
Installing Batteries in the Remote Control 39
Connecting the CPE80 Expansion Microphone 40

Powering the Endpoint On or Off 41
Endpoint Initialization 42
Endpoint Startup 43
Setup Wizard 43
Enabling Communication with Other Endpoints 47
Placing a Test Call from the Yealink VC110 endpoint 47

Configuring Network 49

Preparing the Network 49
Configuring LAN Properties 50
DHCP 50
Configuring Network Settings Manually 55
Configuring Network Speed and Duplex Mode 57
VLAN 59
LLDP 60
Manual Configuration for VLAN 63
DHCP VLAN 65
802.1X Authentication 66
H.323 Tunneling 71
Configuring the Endpoint for Use with a Firewall or NAT 75
Reserved Ports 75
Network Address Translation 78
H.460 Firewall Traversal 88
Intelligent Firewall Traversal 90
Quality of Service 91
VPN 94

Configuring Call Preferences 99

Configuring SIP Settings 99
SIP Account 99
SIP Direct Account 102
Configuring H.323 Settings 105
DTMF 109
Methods of Transmitting DTMF Digit 109
Codecs 112
Call Type 113
Do Not Disturb 114
Auto Answer 116
Call Match 117
History Record 118
Bandwidth 119
Video Size Mode 121
Ringback Timeout 123

Auto Refuse Timeout 123

Configuring Endpoint Settings 125

General Settings 125
Site Name 125
Backlight of the VCP40 Video Conferencing Phone 126
Language 127
Date & Time 128
Automatic Sleep Time 134
Hide IP Address 135
Relog Offtime 136
Key Tone 137
Audio Settings 138
Audio Output Device 138
Audio Input Device 140
Adjusting MTU of Video Packets 143
Dual-Stream Protocol 145
Mix Sending 146
Configuring Camera Settings 147
Far-end Camera Control 151
Camera Control Protocol 153
Tones 154

Endpoint Management 159

Local Directory 159
LDAP 162
Call History 166
Search Source List in Dialing 168
Dual Screen 169

Configuring Security Features 173

User Mode 173
Administrator Password 174
Web Server Type 176
Transport Layer Security 178
Secure Real-Time Transport Protocol 185
H.235 188
Attack Defense in Public Network 189
Abnormal Call Answering 190
Configuring Safe Mode Call 191

Endpoint Maintenance 193

Upgrading Firmware 193
Importing/Exporting Configuration 194
Resetting to Factory 194
SNMP 196

Troubleshooting 201

Troubleshooting Methods 201
Viewing Log Files 201
Capturing Packets 204
Getting Information from Status Indicators 207
Analyzing Configuration Files 207
Viewing Call Statistics 208
Using Diagnostic Methods 208
Troubleshooting Solutions 210
General Issues 211
Camera Issues 213
Video & Audio Issues 214
Endpoint Maintenance 215

Appendix 217

Appendix A: Time Zones 217
Appendix B: Trusted Certificates 220

Index 222

VC110 Video Conferencing Endpoint Introduction

This chapter contains the following information about VC110 video conferencing endpoint:

- VoIP Principles
- Physical Features of Endpoint
- Packaging Contents
- Endpoint Component Instructions
- Icon Instructions
- LED Instructions
- User Interfaces

VoIP Principles

VoIP

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

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

H.323

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

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

SIP

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

Physical Features of Endpoint

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

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

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

VC110 All-in-one Unit User Interface

- 2 x HDMI
- 1x DVI-I
- 1 x Line-in (3.5mm)

- 1 x Line-out (3.5mm)
- 2 x USB2.0 port
- Others: 1 x security lock slot, 1 x reset slot

Cable Hub User Interface

- 1x DVI-I
- 1x 10/100Mb (RJ-45)
- 1x VGA
- 1xRJ-45
- Input：AC 100-240V；Output：12V/2A

Full-HD Camera

- 1920x1080 video resolution
- Pan range: ±100°
- Tilt range: ±30°
- Up to 10 preset positions
- Beauty shot feature

Video Resolution

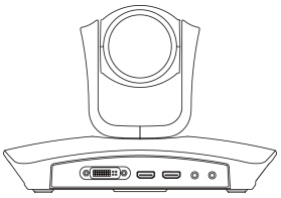
- Full-HD 1080P at 30fps (1920x1080), from 1Mbps
- 720P (1280x720), from 512Kbps
- W448P (768 x 448), WQVGA (400 x 240)
- 4CIF (704×576), CIF (352 x 288)

Packaging Contents

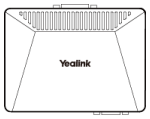
The VC110 all-in-one unit can work with the VCM60, VCP40 or VCM30. You can purchase any combination according to your needs:

VC110 All-in-one Package

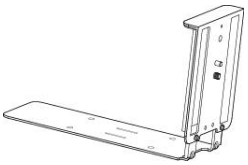
- **VC110 All-in-one Unit**



- **Cable Hub**



- **L-Bracket** (for installing the VC110 one-in-one unit)



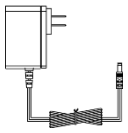
- **Installation Accessories** (for installing the VC110 one-in-one unit)

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

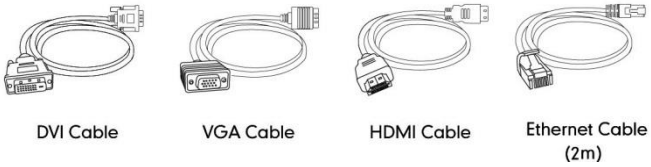
- **VCR10 Remote Control**

- **AAA Batteries×2**

- Power Adapter



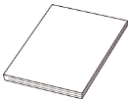
- Cables



- Cable Ties×5

- Velcro×2

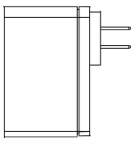
- VC110 Quick Start Guide



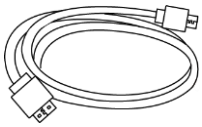
VCM60 Package

- VCM60 Video Conferencing Wireless Microphone

- Power Adapter

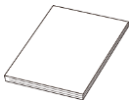


- **USB Cable**



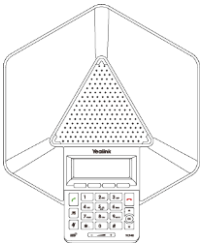
- **Dongle**

- **VCM60 Quick Start Guide**

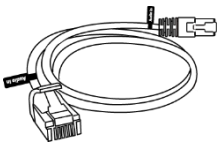


VCP40 Package

- **VCP40 Video Conferencing Phone**



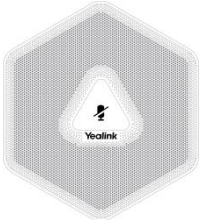
- **Ethernet Cable (7.5m)**



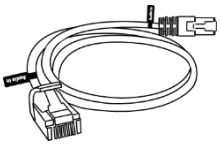
Locate the Audio In port of the cable hub, and connect it to the Audio Out port of the VCP40 with the 7.5m Ethernet cable. VCP40 phone can work as an audio device for the VC110 endpoint. You can also place calls, answer calls or view directory and history on the VCP40 phone.

VCM30 Package

- **VCM30 Video Conferencing Microphone Array**



- **Ethernet Cable (7.5m)**



Locate the Audio In port of the cable hub, and connect it to the Audio Out port of the VCM30 with the 7.5m Ethernet cable. VCM30 video conferencing microphone array can work as the audio input device for the VC110 endpoint. For more information, refer to Audio Input Device on page140.

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

Endpoint Component Instructions

Before installing and using the VC110 video conferencing endpoint, you need to be familiar with the following endpoint components, including:

- VC110 All-in-one Unit
- Cable Hub
- VCM60 Video Conferencing Wireless Microphone
- VCP40 Video Conferencing Phone
- VCM30 Video Conferencing Microphone Array
- VCR10 Remote Control

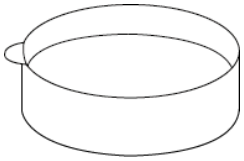
VC110 All-in-one Unit

The VC110 all-in-one unit integrates the camera, the built-in microphone and the codec into a unit. VC110 all-in-one unit compresses outgoing video and audio data, transmits

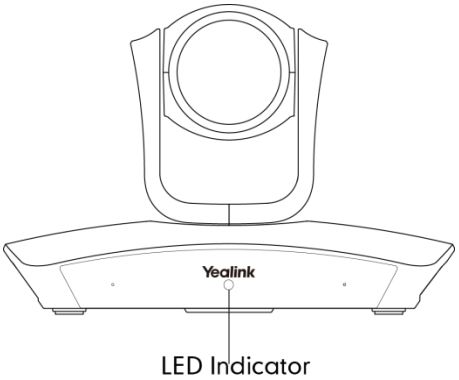
this information to the far end, and decompresses incoming data. It supports 16:9 and 4:3 aspect ratios. It can be compatible with different audio output devices, and can adapt to the display devices automatically.

Lens cover

The lens cover is used for protecting the lens, which shall not receive dust pollution and all possible brush, collision.

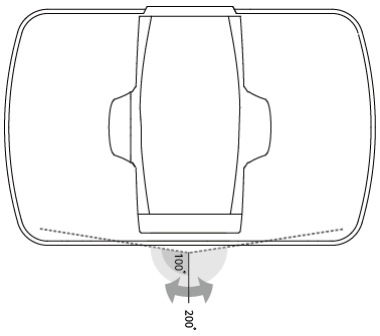


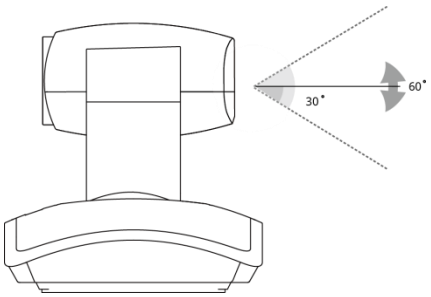
The front of VC110 all-in-one unit



The HD camera supports 4xdigital zoom, white balance and automatic gain. You can place the VC110 all-in-one unit on the table or mount it on a wall. The LED indicator in front of the camera indicates different statuses of the endpoint. For more information, refer to LED Instructions on page 31.

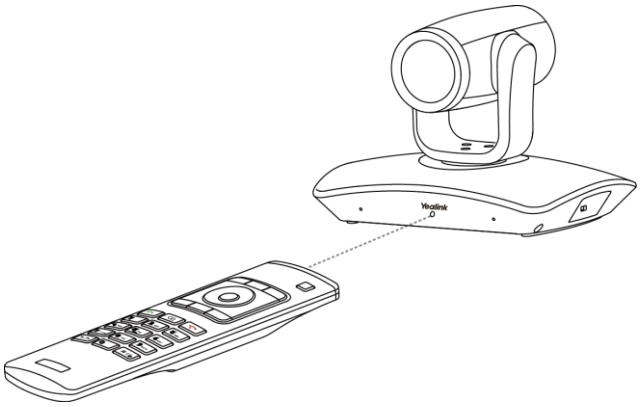
You can use the remote control to adjust the position or focus of the camera. The VC110 camera can be panned (± 100 degrees range), tilted (± 30 degrees range).





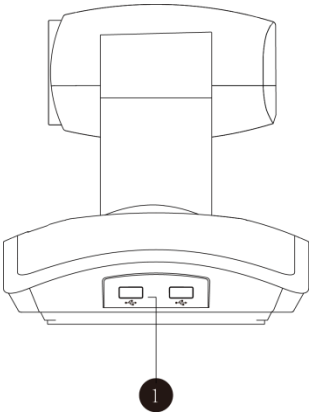
Infrared Sensor

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



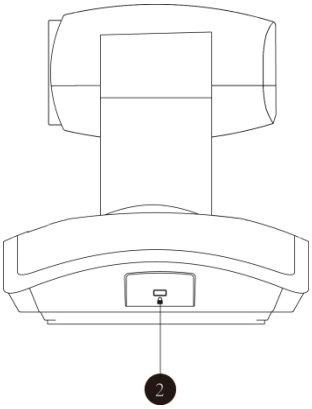
Note When the endpoint is powered on, avoid physically turning the camera. This may cause permanent damage to the camera. Always use the remote control to pan and tilt it.

The right side of the VC110 all-in-one unit



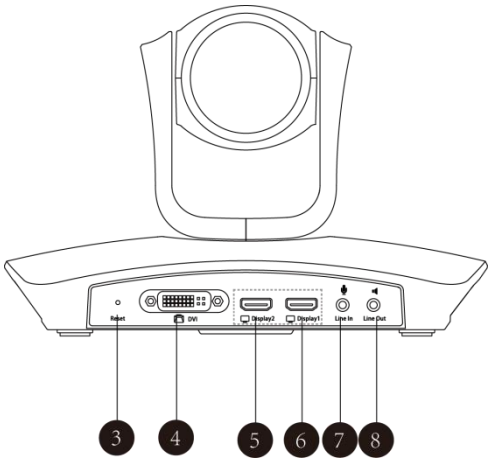
	Port Name	Description
①	USB	Inserts a USB flash drive to one of the two USB ports for storing screenshots and recording videos. Inserts a dongle to one of the two USB ports for connecting the VCM60 video conferencing wireless microphone. **Note**: • The wireless microphone dongle and USB flash drive can work at the same time. • If two USB flash drives are connected, only the latter one can be identified.

The left side of the VC110 all-in-one unit



	Port Name	Description
②	Security Slot	Allows you to connect a universal security cable to VC110 all-in-one unit, so you can lock it down. The endpoint cannot be removed when locked.

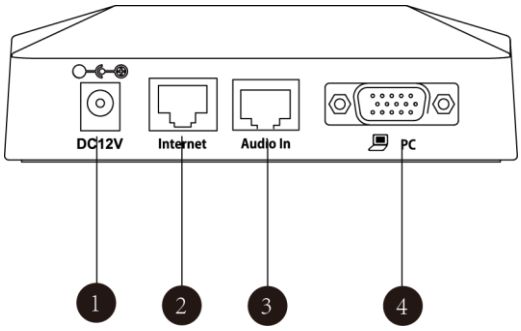
The back of VC110 all-in-one unit



	Port Name	Description
③	Reset Key	Resets the endpoint to factory defaults.
④	DVI Port	Connects to the cable hub.
⑤	Display1	Connects to a display device for displaying video images. When connecting to only one display device, Display1 port on the VC110 all-in-one unit is the only available
⑥	Display 2	Connects to secondary display device for displaying video images.
⑦	Line In	Connects to an audio input device using an audio cable (3.5mm).
⑧	Line Out	Connects to an audio output device using an audio cable (3.5mm).

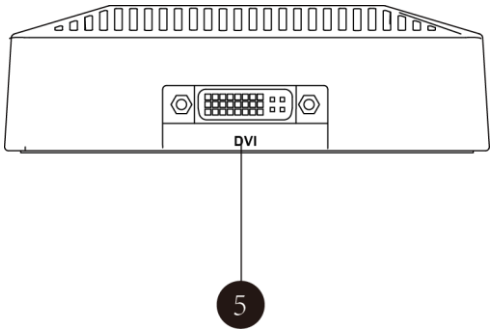
Cable Hub

The front of cable hub:



	Port Name	Description
①	DC12V	Connects to the power source via a power adapter.
②	Internet	Connects to the network device.
③	Audio In	Connects to the VCP40 video conferencing phone or the VCM30 video conferencing microphone array.
④	PC	Connects to a PC for sharing documents or videos during a call.

The back of cable hub:

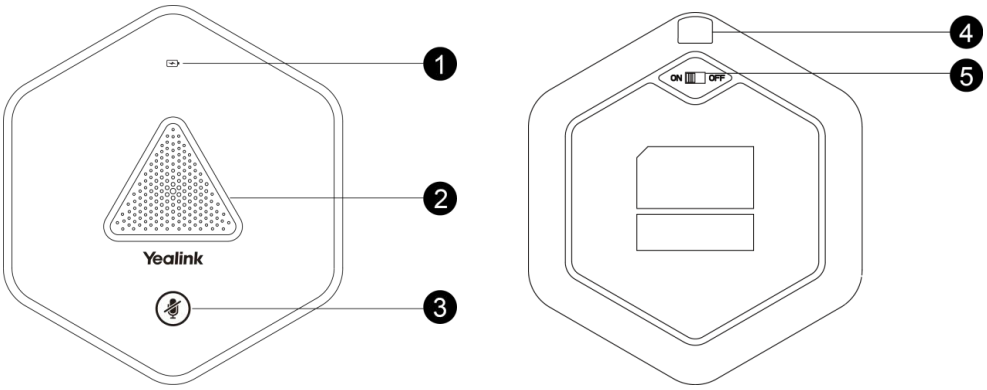


	Port Name	Description
⑤	DVI Port	Connects to the VC110 all-in-one unit.

VCM60 Video Conferencing Wireless Microphone

The VCM60 is a video conferencing wireless microphone which can work as the audio input device for VC110 video conferencing endpoint. It supports 360-degree audio pickup at a radius of up to 2 meters. There are a mute button and a battery indicator LED on its top. You can mute or unmute the VCM60 by tapping the mute button.

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



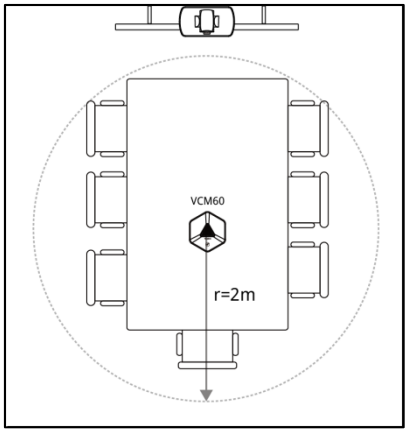
	Name	Description
①	Battery Indicator LED	Indicates the battery information. For more information on the mute indicator LED, refer to LED Instructions on page 31.
②	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 2 meters.
③	Mute Button	• Mutes or unmutes the VCM60. For more information on the mute indicator LED, refer to LED Instructions on page 31. • Activates the VCM60 to search the dongle when it is in the offline standby mode. For more information, refer to Standby Mode on page 31. • Enters registration mode. For more information, refer to Registering and Unregistering the VCM60 on page 17.
④	Charging Interface	Connects the VCM60 to a power adapter or a computer's USB port using a USB cable to charge the VCM60.
⑤	Switch	Turns on or off the VCM60.

Placing the VCM60

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

- For registering to the dongle successfully, make sure the VCM60 video conferencing wireless microphone is less than 30 meters distant from the dongle.

- Place the VCM60 on a stable surface and keep it away from obstacles so that it can effectively pick up sounds.



Turning On or Off the VCM60

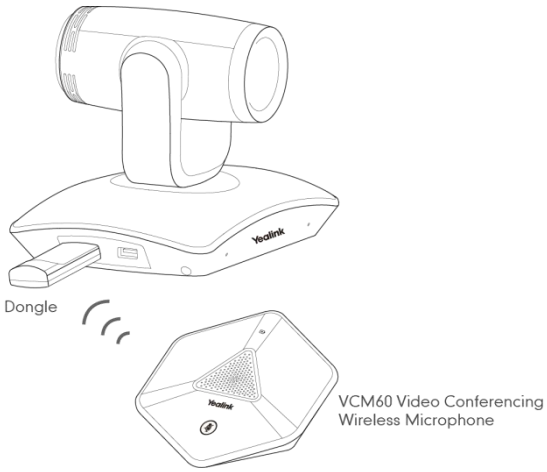
There is a power switch on the bottom of the VCM60. Turn on the power switch to start the VCM60. After the VCM60 starts, it registers with the paired dongle automatically. You can turn off this switch if the VCM60 is not in use for a long period of time.

Connecting VCM60 to the Video Conferencing Endpoint

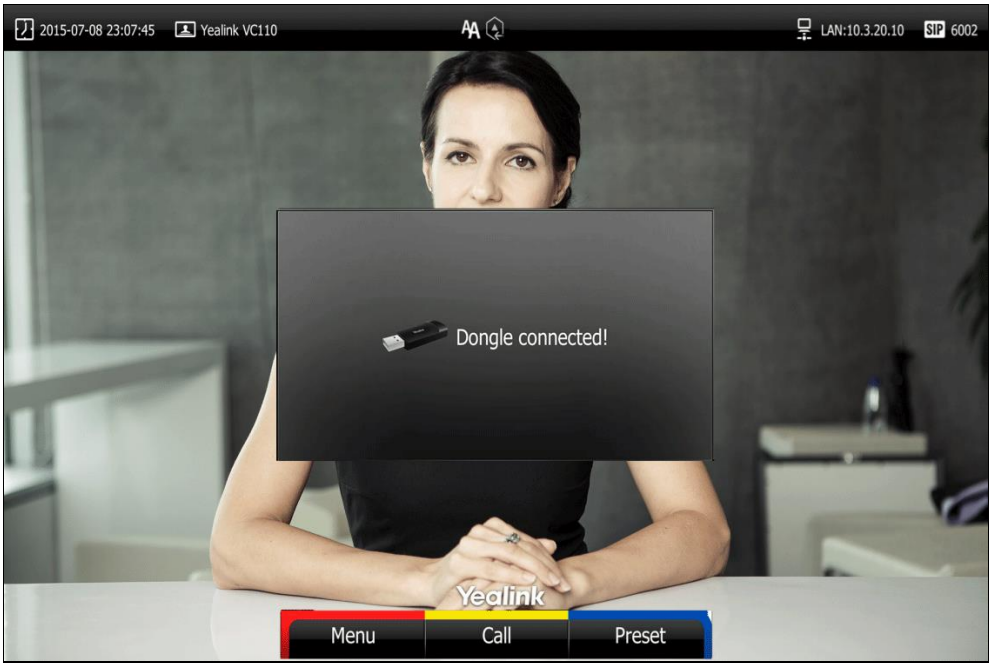
To ensure good voice quality, VCM60 video conferencing wireless microphone can be connected to the VC110 video conferencing endpoint to work as the audio input device.

To connect the VCM60 to the VC110 video conferencing endpoint, do the following:

1. Connect the dongle to one of the USB ports on the VC110 all-in-one unit.

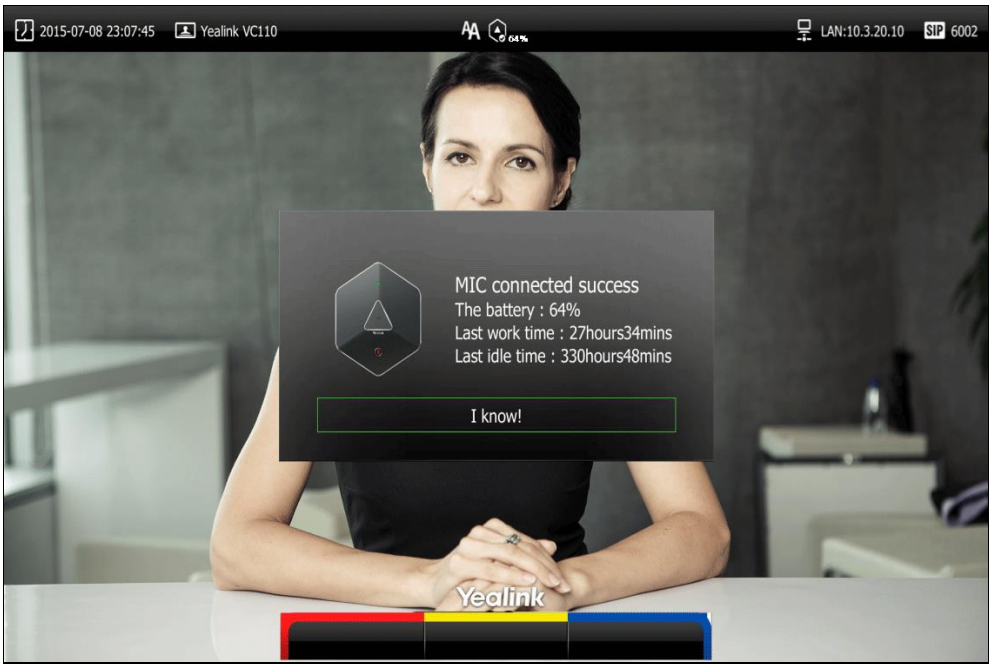


The display device prompts "Dongle connected!", and the (unregistered) icon appears on the status bar.



2. Turn on the VCM60.

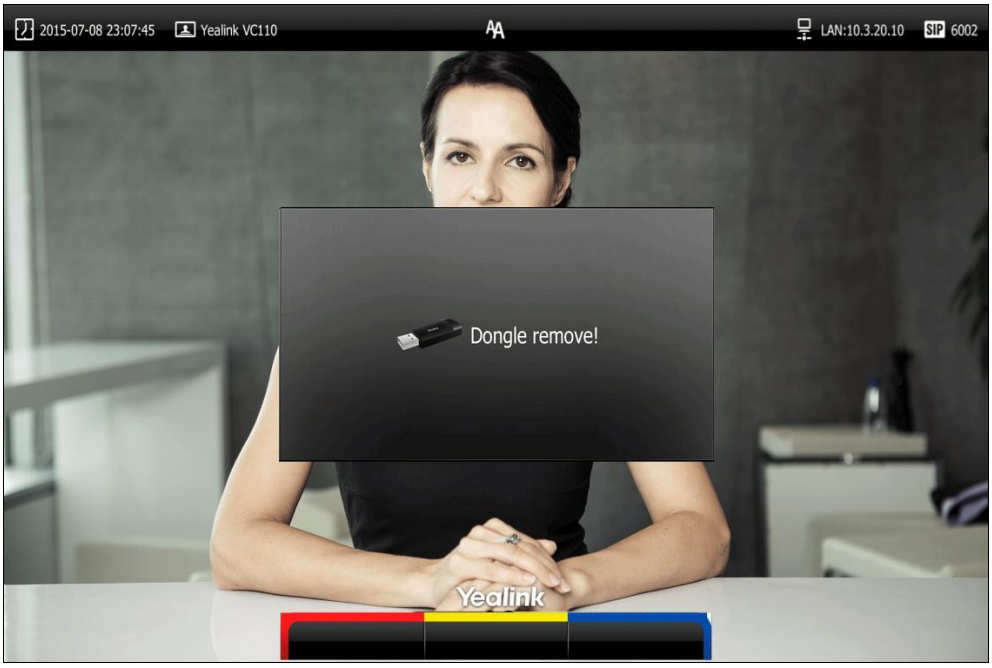
   The VCM60 registers with the dongle automatically. If successful, the (unregistered) icon will change to (registered). Current capacity appears on the right side of the icon. When the standby time is less than 1 hour, please charge the VCM60. For more information, refer to Charging the VCM60 on page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



To remove the VCM60 from the VC110 video conferencing endpoint, do the following:

1. Remove the dongle from the VC110 all-in-one unit.

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



Standby Mode

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

Online standby:

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

Offline standby:

- If VC110 video conferencing endpoint encounters poor signal, wireless interference or is powered off, the VCM60 may lose connection with the dongle. In this case, the VCM60 will search the dongle again, and the mute indicator LED fast flashes green. If dongle cannot be searched in 2 minutes, the VCM60 will enter offline standby mode automatically and the mute indicator LED slowly flashes orange.
- When the VCM60 is in offline standby mode, you need to tap the mute button to activate VCM60 to search dongle again and the mute indicator LED fast flashes green.

Muting or Unmuting the VCM60

There is a mute button on the top of the VCM6. If VCM60 works as the audio input device of the VC110 video conferencing endpoint, you can mute or unmute it in the following scenarios:

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

To mute the VCM60 during a call:

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

To un-mute the VCM60 during a call:

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

Viewing VCM60 Information

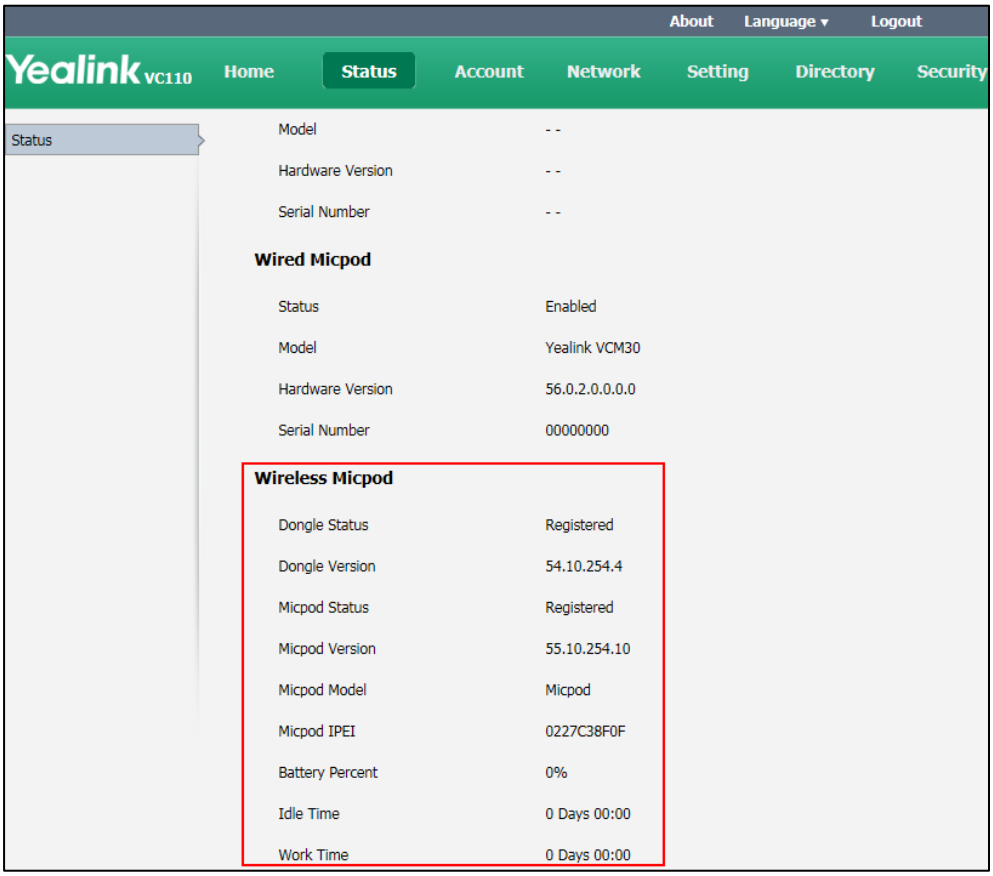
When the dongle is connected to the USB port of the VC110 one-in one unit, you can view VCM60 status via the remote control or web user interface.

Available information of VCM60 includes:

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

To view the VCM60 information via web user interface:

1. Click on **Status**.



To view the VCM60 information via the remote control:

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

Registering and Unregistering the VCM60

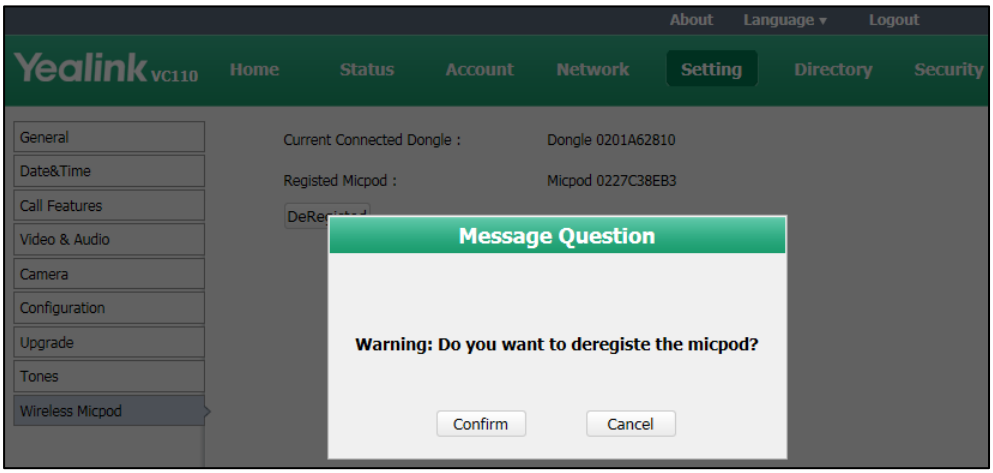
The VCM60 video conferencing wireless microphone and dongle are automatically "paired" at the factory. But In following cases, you may need to deregister or register the VCM60 video conferencing wireless microphone manually.

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

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

To deregister the VCM60 via web user interface:

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

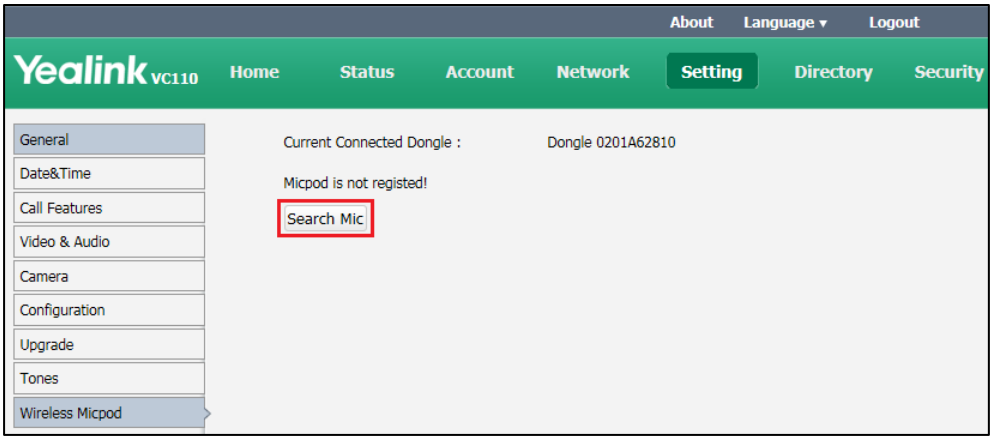


3. Click **Confirm** to deregister the video conferencing wireless microphone.

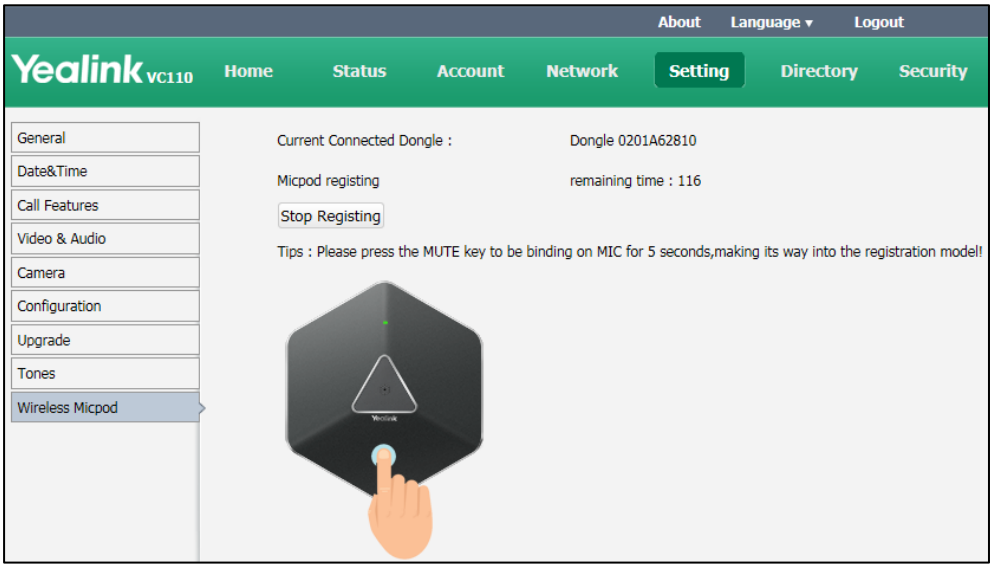
   The paired information will be cleared. The VCM60 video conferencing wireless microphone will enter offline standby mode and the mute indicator LED slowly flashes orange.

To register the VCM60 via web user interface:

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



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



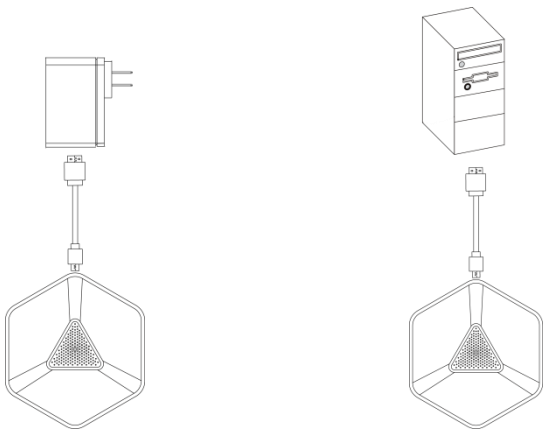
3. Tap and hold the mute button on the VCM60 video conferencing wireless microphone for 5 seconds until the mute indicator LED flashes orange.

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

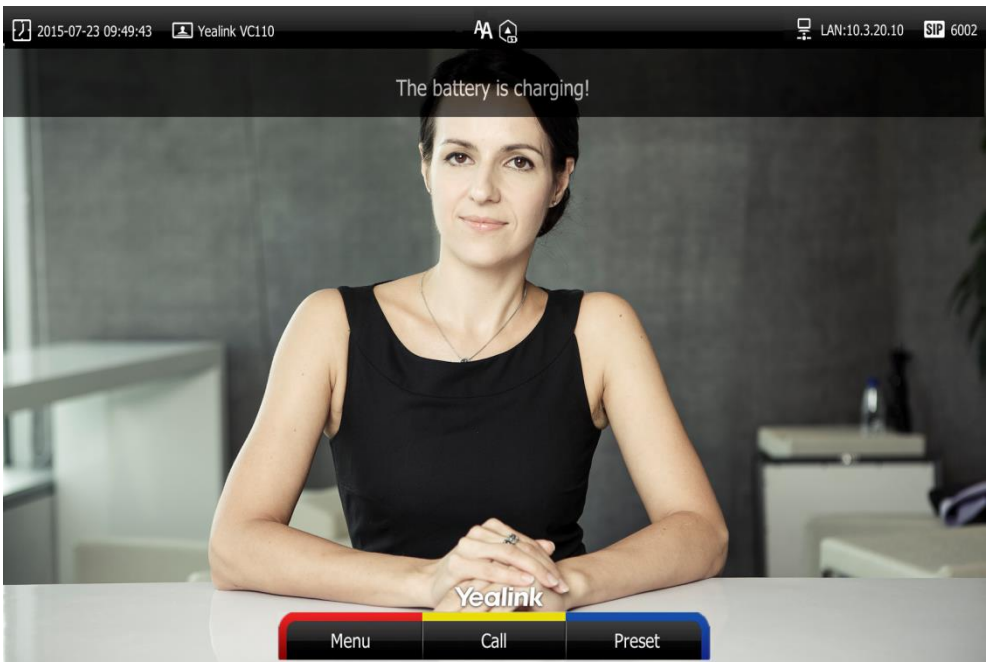
Charging the VCM60

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

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



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



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

VCM60 Working Frequency

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

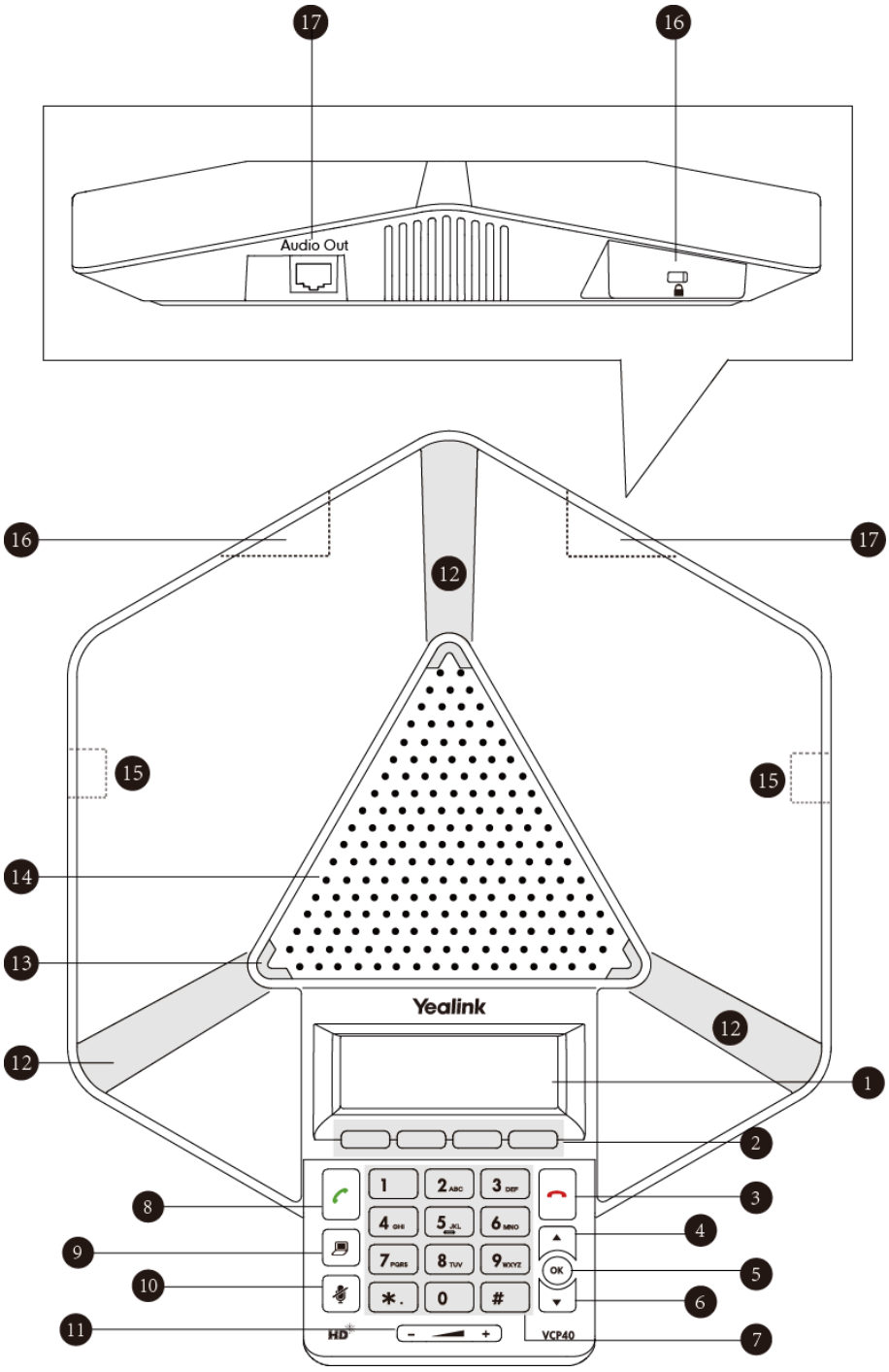
Freq (MHz)	RF Carrier Index (DECT tester Numbering)						
	EU	Taiwan	US	LA	Korea	Brazil	Japan
1881.792	9	9					
1883.520	8	8					
1885.248	7	7					
1886.976	6	6					
1888.704	5	5					
1890.432	4	4					
1892.160	3	3					
1893.888	2	2					
1895.616	1						4(F1)
1897.344	0						3(F2)

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

VCP40 Video Conferencing Phone

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

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

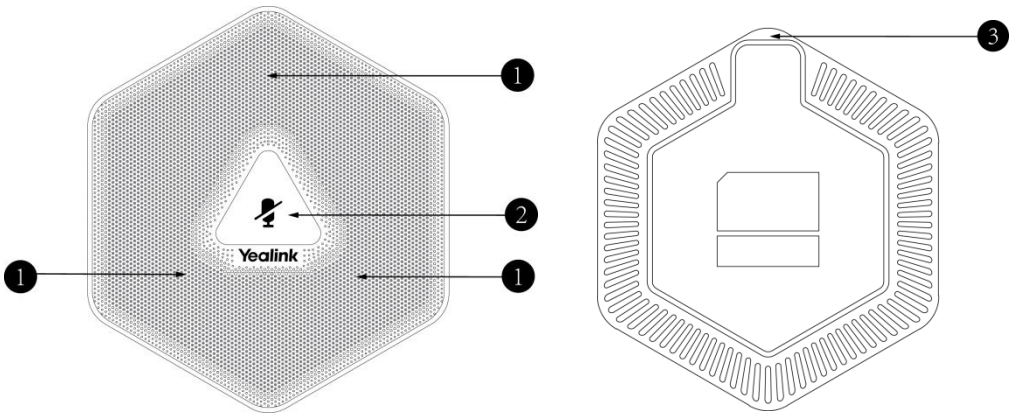


Component instructions for the VCP40 phone are:

	Item	Description
①	LCD Screen	Shows information about calls, messages, soft keys, time, date and other relevant data: • Call information—call duration • Icons (for example,) • Missed call information • Time and date
②	Soft Keys	Label automatically to identity their context-sensitive features.
③	On-hook Key	Rejects or ends a call or returns to the previous screen.
④		Scrolls upwards through the displayed information.
⑤	OK	Enters list or answers incoming calls.
⑥		Scrolls downwards through the displayed information.
⑦	Keypad	Generates the digits and special characters ".", "*", "#".
⑧	Off-hook Key	Initiates a call or answers a call.
⑨	Presentation Key	Enables or disables presentation.
⑩	Mute Key	Toggles the mute feature.
⑪	Volume Key	Adjusts the volume of the speakerphone and ringer.
⑫	Microphone	Picks up voice.
⑬	LED Indicators	Indicate phone and call statuses.
⑭	Speakerphone	Provides ringer and hands-free (speakerphone) audio output.
⑮	MIC Port	Connects a CPE80 expansion microphone to one of two MIC ports.
⑯	Security Slot	Allows you to connect a universal security cable to lock down your phone. The phone cannot be removed when locked.
⑰	Audio Out Port	Connects to the VCP40 phone using the7.5m Ethernet cable labeled Audio In. Provides the power supply for the VCP40 phone.

VCM30 Video Conferencing Microphone Array

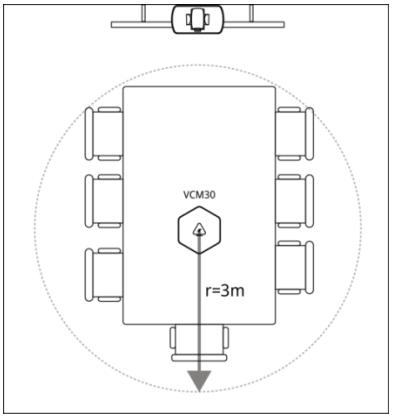
The VCM30 is a video conferencing microphone array which can work as the audio input device for VC110 video conferencing endpoint. It has 3 built-in microphones which support 360-degree audio pickup at a radius of up to 3 meters. There is a mute button on its top. You can mute or unmute the VCM30 by tapping the mute button during a call.



	Name	Description
①	Built-in Microphones	Support 360-degree audio pickup at a radius of up to 3 meters.
②	Mute Button	Mutes or unmutes the VCM30. For more information on the mute indicator LED, refer to LED Instructions on page 31.
③	Audio Out Port	Connects to the Audio In port of cable hub using the 7.5m Ethernet cable labeled Audio In. Provides the power supply for the VCM30.

Placing the VCM30

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



Muting or Unmuting the VCM30

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

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

To mute the VCM30 during a call:

1. Tap to mute the call.

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

To un-mute the VCM30 during a call:

1. Tap again to un-mute the call.

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

Viewing VCM30 Information

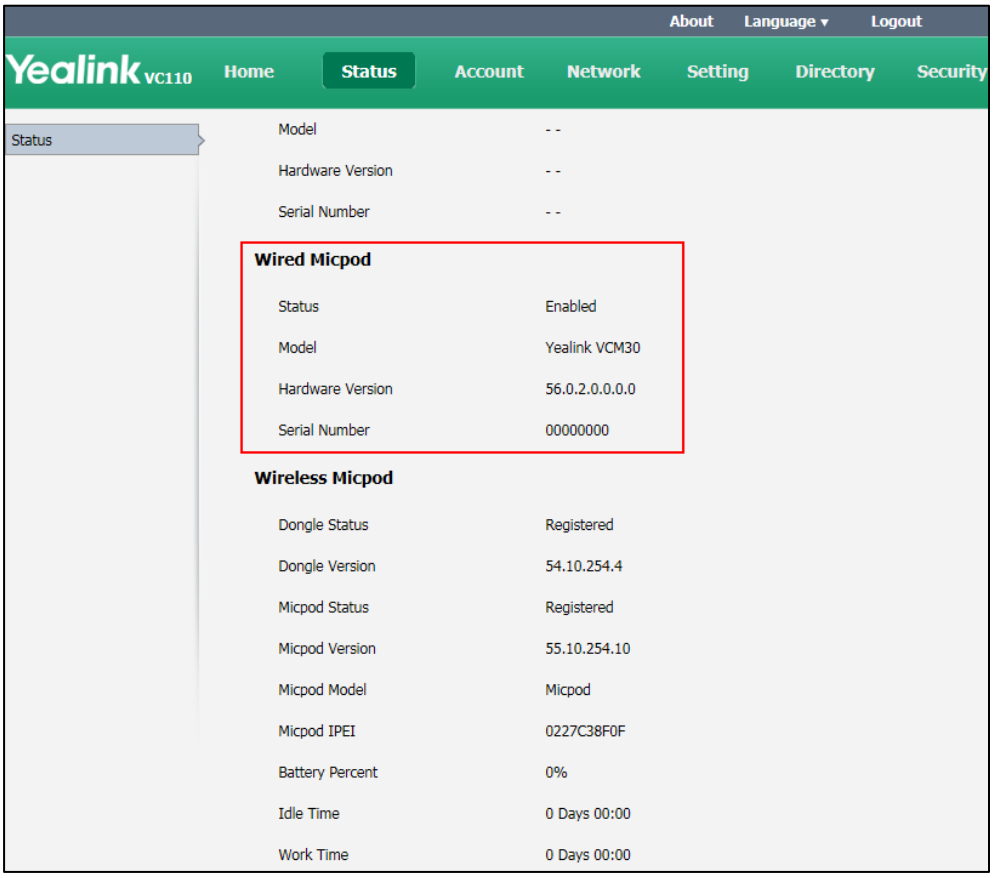
When the VCM30 is connected to the Audio In port of cable hub, you can view VCM30 status via the remote control or web user interface.

Available information of VCM30 includes:

- Status
- Model
- Hardware Version
- Serial Number

To view the VCM30 information via the web user interface

1. Click **Status**.

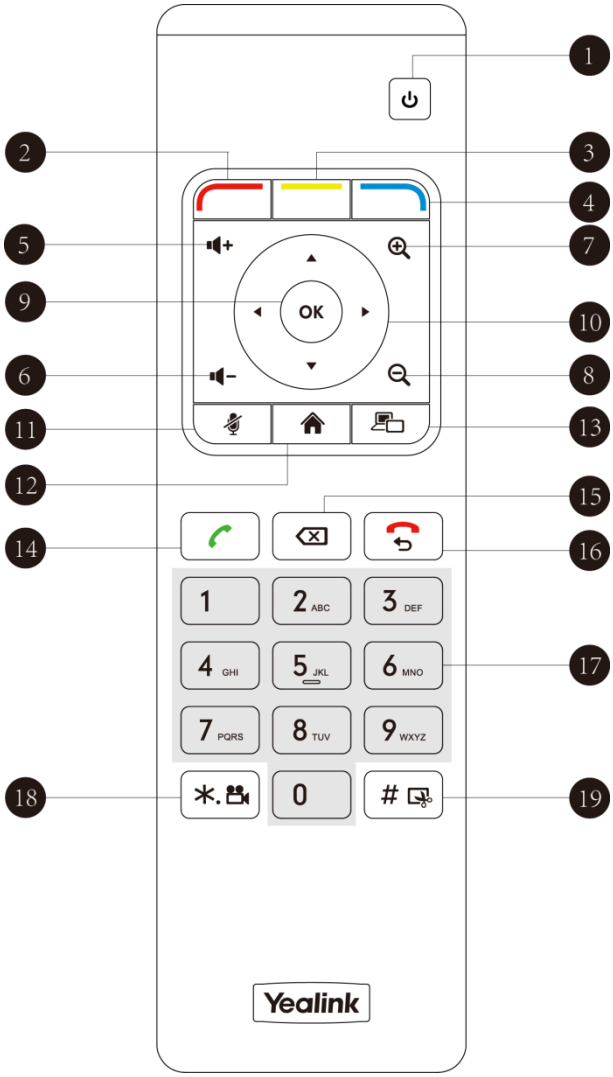


To view the VCM30 information via the remote control:

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

VCR10 Remote Control

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



Hardware components of the remote control:

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

	Item	Description
④	Blue Shortcut Key	Located at the bottom right of the screen. Label identifies context-sensitive features. In the idle screen, this is used to save and check the camera preset position, and corresponds to the Preset soft key.
⑤	Vol+	Increases the endpoint volume.
⑥	Vol-	Decreases the endpoint volume.
⑦	Zoom out Key	• Decreases the camera zoom or the captured image magnifications. • Behaves as page up in a multiple page list.
⑧	Zoom in Key	• Increase the camera zoom or the captured image magnifications. • Behaves as page up in a multiple page list.
⑨	OK Key	Confirms actions or answers incoming calls.
⑩	Navigation Key	• In the menu screen, press ◀ or ▶ to change menus, press ▲ or ▼ to select items. • In the idle screen, pan and tilt the camera to adjust the viewing angle.
⑪	Mute Key	Toggles the mute feature.
⑫	Home Key	• Returns to the idle screen when in the menu screen. • Enters the pre-dialing screen during a call.
⑬	Video Source Key	Switches the input source between Camera, Camera-PC, or PC.
⑭	Off-hook Key	• Enters the pre-dialing screen. • Places a call. • Answers a call.
⑮	Delete key	Deletes one character at a time.
⑯	On-hook Key	• Ends a call or exits from a conference call. • Returns to the previous screen when not in a call.
⑰	Keypad	• Enters digits. • Enters the pre-dialing screen. • Stores the preset position of the camera.

	Item	Description
⑱	Video Recording Key	• Generates a special characters ".". • Starts/Stops recording video.
⑲	Snapshot Key	• Generates a pound key (#). • Captures the image from the camera.

Icon Instructions

Icons on Display Device

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

Icon	Description
(flashing)	Network is disconnected
	Network is available
	Packet loss
SIP	SIP account is registered
H323	H.323 account is registered
abc	Lowercase letters input mode of the on-screen keyboard
ABC	Uppercase letters input mode of the on-screen keyboard
@#%	Character input mode of the on-screen keyboard
AA	Auto answer
	Missed calls
	Volume is 0
	Do not disturb
	Do not disturb during a call

Icon	Description
	Call mute
	Call encryption
	The content of the local camera
	Focus content
	Camera position
	Record a video
	Dialed calls
	Received calls
	Missed calls
	Dongle is connected, while the VCM60 is unregistered
	Dongle is connected, and the VCM60 is registered
	The VCM60 is charging
	The standby time of VCM60 is less than one hour
	Dual screen mode
	Dual video sources (when a PC is connected to the PC port on the cable hub)
	A USB flash drive is inserted to the USB port of the VC110 all-in-one unit
	Local contact
VPN	VPN is enabled

Icons on the VCP40 Video Conferencing Phone

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

Icon	Description
(Flashing)	Network is unavailable
SIP	SIP account is registered (the icon flashes when the SIP account is not registered successfully)
H323	H.323 account is registered (the icon flashes when the H.323 account is not registered successfully)
AA	Auto answer
DND	Do not disturb
	Call is muted
	Volume is 0
USB	A USB flash drive is inserted to the port of the VC110 all-in-one unit
	Record a video
	Local contact
	Conference call
	Received calls
	Dialed calls
	Missed calls

LED Instructions

Indicator LED on the VC110 all-in-one unit:

LED Status	Description
Solid green	The VC110 is powered on.
Solid red	The VC110 is in sleep mode.
Solid orange	The VC110 is abnormal (e.g., network unavailable, update failure).
Flashing green	Press the key on the remote control.

LED Status	Description
Off	The VC110 is powered off.

Indicator LED on the VCP40 phone:

LED Status	Description
Solid red	The phone is initializing. The VCP40 is muted when the VC110 is during a call.
Flashing red	The phone is ringing.
Solid green	The phone is placing a call. There is an active call on the phone.
Off	The phone is not connected to the cable hub. The phone is idle.

Battery indicator LED on the VCM60 video conferencing wireless microphone:

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

Mute indicator LED on the VCM60 video conferencing wireless microphone:

LED Status	Description
Fast flashing green	The VCM60 is searching the dongle.
Green and in breathing state	The VCM60 registers with the dongle, and then enters the online standby mode.
Solid green	The VC110 is placing a call. The VC110 is in a call.
Solid red	The VC110 is muted during a call.
Fast flashing orange	The VCM60 enters registration mode.
Slowly flashing orange	The VCM60 fails to search the dongle, and then enters the offline standby mode.
Off	The VCM60 is turned off. The VCM60 runs out of battery.

Mute Indicator LED on the VCM30 video conferencing microphone array

LED Status	Description
Solid red	The VCM30 is muted when the VC110 is during a call.
Flashing red	The VC110 is ringing.
Solid green	The VCM30 is connected to the cable hub within the first 5 seconds. The VC110 is placing a call. The VCM30 is unmuted when the VC110 is during a call.
Off	The VCM30 is not connected to the cable hub. The VCM30 is idle.

User Interfaces

Three are two ways to customize the configurations of your endpoint:

- Remote Control
- Web User Interface

The following describes how to configure the VC110 video conferencing endpoint via the two methods above.

Detailed operation steps will be introduced in the feature section.

Remote Control

You can use the remote control and display device to configure and use the VC110 video conferencing endpoint.

For more information on the function of each key on the remote control, refer to VCR10 Remote Control on page 27. The Advanced option is only accessible to the user with the administrator's permission. The default administrator password is "0000".

Web User Interface

You can customize your endpoint via the web user interface. To access the web user interface, you need to know the user name and the administrator's password. The default user name is "admin" (case-sensitive), and the default password is "0000". You can also access the web user interface with user credential, which is disabled by default. For more information on how to enable the user credential, refer to User Mode on page173.

The endpoint uses the HTTPS protocol to access the web user interface by default. For more information on the access protocol for web user interface access, refer to Web

Server Type on page 176.

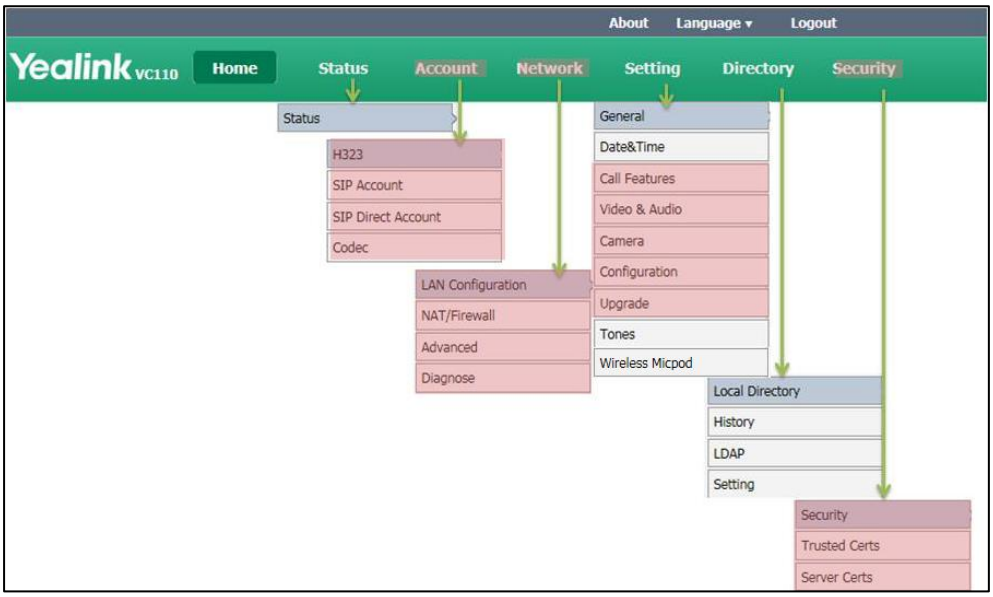
Log into the web user interface of the endpoint:

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

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

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

The web structure tree of VC110 is shown as below, (the red highlight is hidden for users with user credentials):



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

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

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

Getting Started

This chapter provides basic information and installation instructions for Yealink VC110 endpoints in the following sections:

- Endpoint Connection and Installation
- Powering the Endpoint On or Off
- Endpoint Initialization
- Endpoint Startup
- Setup Wizard
- Enabling Communication with Other Endpoints
- Placing a Test Call from the Yealink VC110 endpoint

Endpoint Connection and Installation

Placing the Endpoint

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

Endpoint Components Installation

This section introduces the following:

- Connecting the VC110 video conferencing endpoint
- Installing the VC110 video conferencing endpoint
- Installing batteries in the remote control
- Connecting the CPE80 expansion microphone

Note

Up to two display devices can be connected to the VC110 all-in-one unit. Because the display device is not included in the package, you need to purchase it separately if required. Ensure that the purchased display device supports HDMI input.

When connecting only one display device to the VC110 all-in-one unit, Display1 port is the only available port. If dual screen mode is required, you can connect secondary display device to the Display2 port.

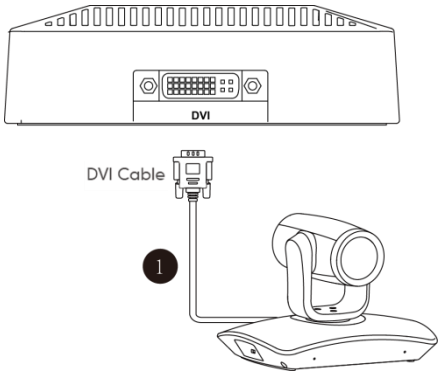
Because DVI cable is tailor-made, please use the Yealink-supplied DVI cable.

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

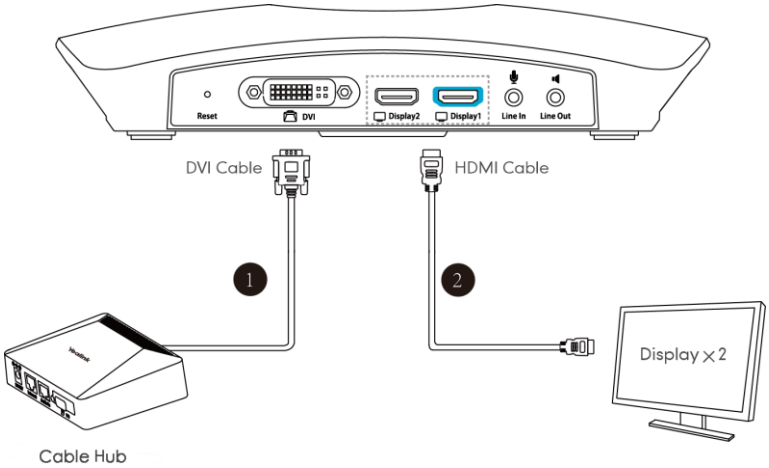
Connecting the VC110 Video Conferencing Endpoint

Do the following:

1. Locate the DVI port on the back of the VC110 all-in-one unit, and connect it to the DVI port of the cable hub with the supplied DVI cable.

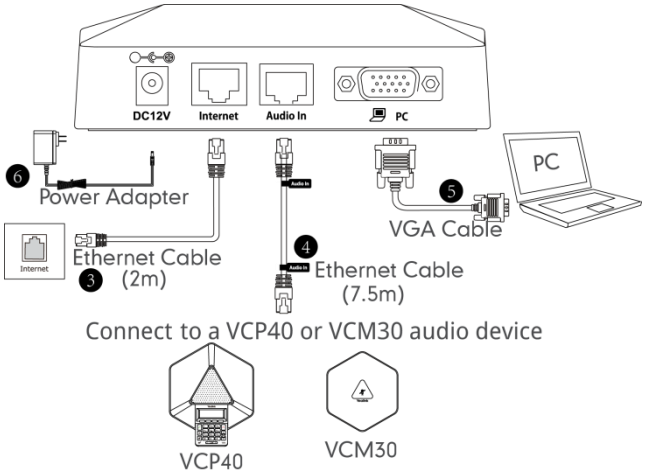


2. Locate the Display1 port of the VC110 all-in-one unit, and connect it to the HDMI port on the display device with the supplied HDMI cable (Make sure the display device is powered on).



3. Locate the Internet port on the cable hub, and connect it to the port on the in-line power switch/hub with the supplied 2m Ethernet cable.
4. (Optional) Locate the Audio In port of the cable hub, and do one of the following:
   - Connect it to the Audio Out port of the VCP40 video conferencing phone with the 7.5m Ethernet cable labeled Audio In.
   - Connect it to the Audio Out port of the VCM30 video conferencing microphone array with the 7.5m Ethernet cable labeled Audio In.
5. (Optional) Locate the VGA output port of the PC, and connect it to the PC port of cable hub with the supplied VGA cable for sharing content.
6. Locate the DC19V port of the VC110 all-in-one unit, and connect it to an AC power outlet with the supplied power adapter and power cord.

The cable hub also can be powered from a PoE-compliant switch or hub. For more information, refer to on Power over Ethernet on page 41.

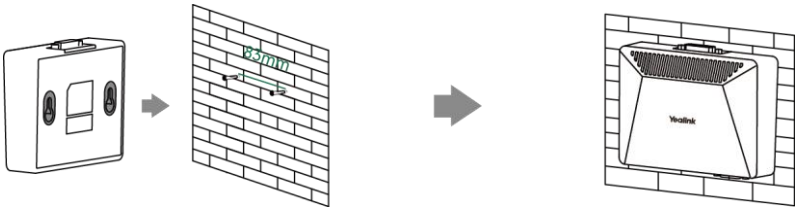


You can fasten all cables with cable ties after all devices are connected.

Installing the VC110 Video Conferencing Endpoint

Installing the Cable Hub

You can hang the cable hub on the wall. To use this method, you need to purchase the screws (specification: T4×30) separately.

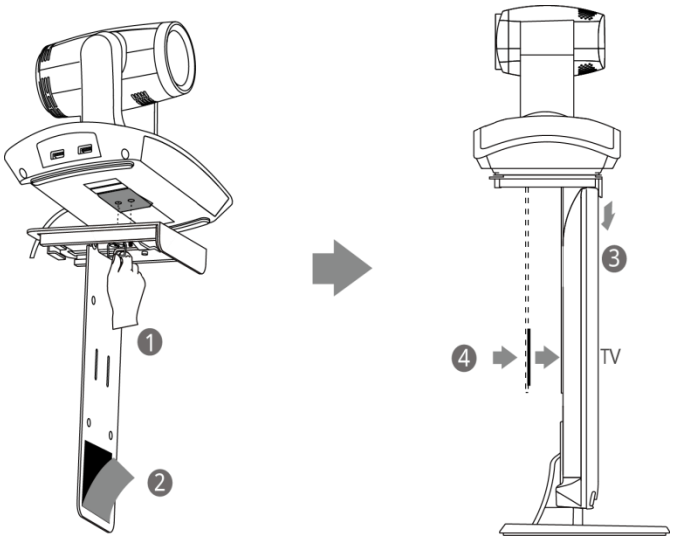


Installing the VC110 All-in-one Unit

You can choose to mount the VC110 all-in-one unit on your TV or a wall, depending on your actual needs.

a) Mounting the VC110 all-in-one unit on a TV

When the thickness of your TV is between 35-120 mm, you can mount the VC110 all-in-one unit on your TV.



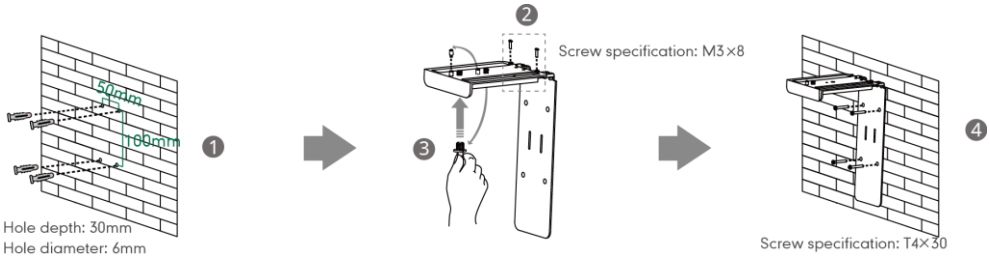
Do the following:

1. Lock the VC110 all-in-one unit to the L-bracket.
2. Remove the protection of the Velcro.
3. Put the L-bracket on the top of the TV.
4. Adjust the L-bracket to ensure close adhesion to the back of the TV.

b) Mounting the VC110 all-in-one unit on a wall

You can also mount the VC110 all-in-one unit on a wall. The recommended height for VC110 all-in-one unit positioning is 1.5m-1.8m above the ground.

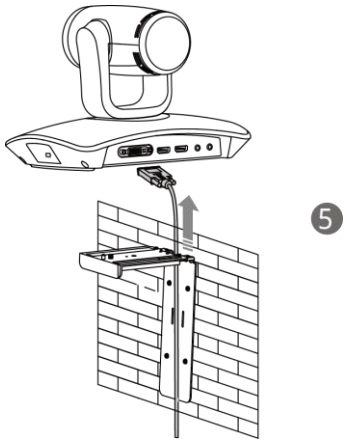
Do the following:



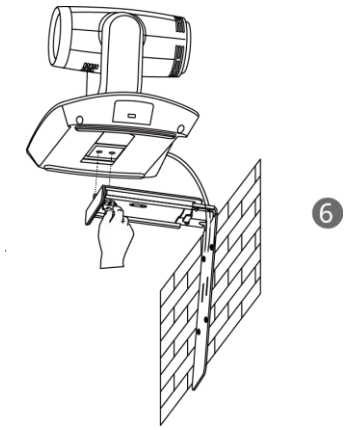
1. Punch holes into the wall and then insert the expansion bolts.

   Installation location for the expansion bolts and punching requirement are shown above.
2. Lock the L-bracket with the M3×8 screws.
3. Move the setscrews on the L-bracket to the left holes.
4. Lock the L-bracket to the wall with T4×30 screws.

5. Connect one end of the DVI cable to the VC110 all-in-one unit and put the other end of the DVI cable through the L-bracket.



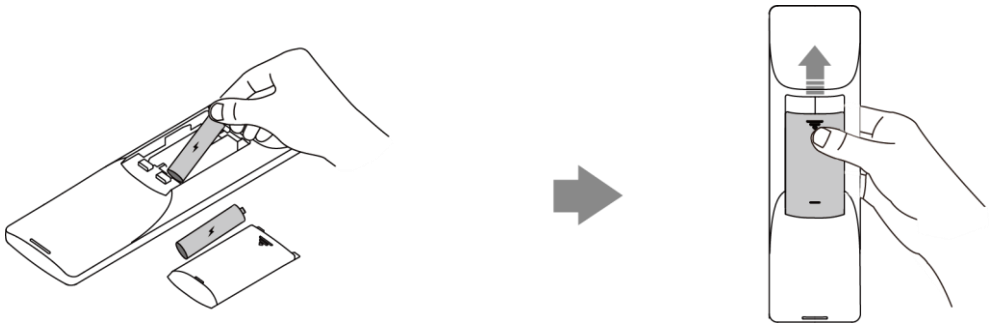
6. Lock the VC110 all-in-one unit to the L-bracket, and then connect the other end of the DVI cable to the cable hub.



Installing Batteries in the Remote Control

Do the following:

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



Remote Control Battery Safety Information

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

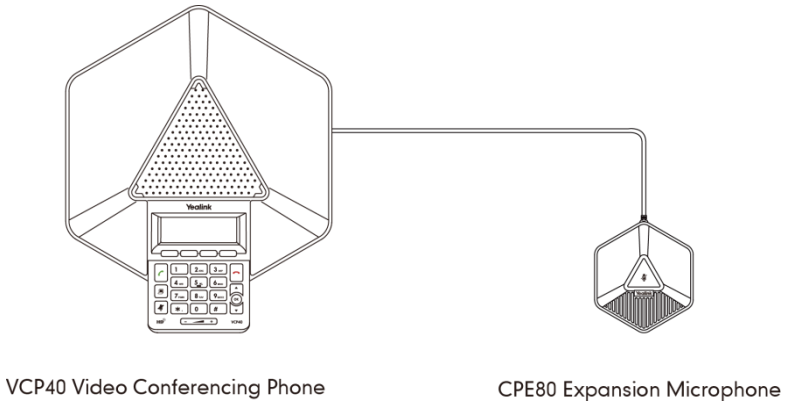
Connecting the CPE80 Expansion Microphone

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

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

To connect the expansion microphone:

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



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

Powering the Endpoint On or Off

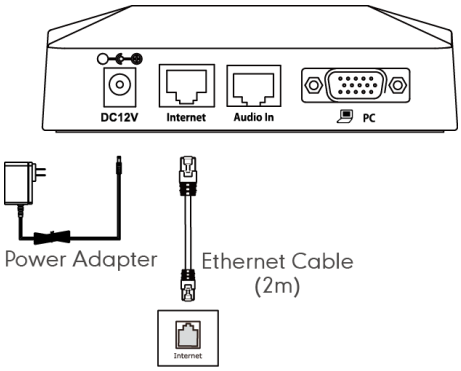
You have two options for power and network connections. Your system administrator will advise you which one to use.

- AC power (Optional)
- Power over Ethernet (PoE)

AC Power (Optional)

To connect the AC power:

1. Locate the DV12V port on the cable hub, and connect it to the electrical power outlet with the supplied power adapter.
2. Locate the Internet port on the cable hub, and connect it to the internet port on the wall or on the switch/hub device with the supplied 2m Ethernet cable.



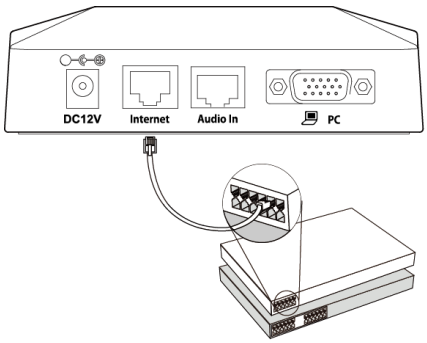
Note The VC110 video conferencing endpoint should be used with Yealink original power adapter (12V/2A) only.

Power over Ethernet

With the included or a regular Ethernet cable, the VC110 video conferencing endpoint can be powered from a PoE-compliant switch or hub.

To connect the PoE:

1. Locate the Internet port on the cable hub, and connect it to the port on the in-line power switch/hub with the Ethernet cable.



IEEE 802.3af compliant
PoE Hub/Switch

Note

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

Important! Do not remove power from the cable hub while it is updating firmware and configurations.

Remove power to power off the endpoint if long time no use.

Endpoint Initialization

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

During the initialization process, the following events take place:

Loading the ROM file

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

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The endpoint is capable of querying a DHCP server. DHCP is enabled on the endpoint by default. The following network settings can be obtained from the DHCP server during initialization:

- IP Address
- Subnet Mask

- Gateway
- Primary DNS (Domain Name Server)
- Secondary DNS

You need to configure the network settings of the endpoint manually if any of them are not provided by the DHCP server. For more information on configuring network settings manually, refer to Configuring Network Settings Manually on page 55.

Endpoint Startup

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

1. The LED indicator on the VC110 all-in-one unit illuminates solid green.
2. The display device displays the boot up screen.
3. The camera pans to the middle position automatically.
4. The display device displays the setup wizard (when you first start up, or reset the endpoint, the display device will display the setup wizard)

   For more information on how to complete the setup wizard, refer to Setup Wizard on page 43.
5. After completing the setup wizard, the display device displays the main screen.

   The main screen displays the following:

   - Time and date
   - Endpoint IP address and site name
   - Status icon
   - Soft key labels
   - Video image
6. The VCP40 conferencing phone starts up normally. The phone's LCD screen displays the site name, status icon, soft keys, time and date.

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

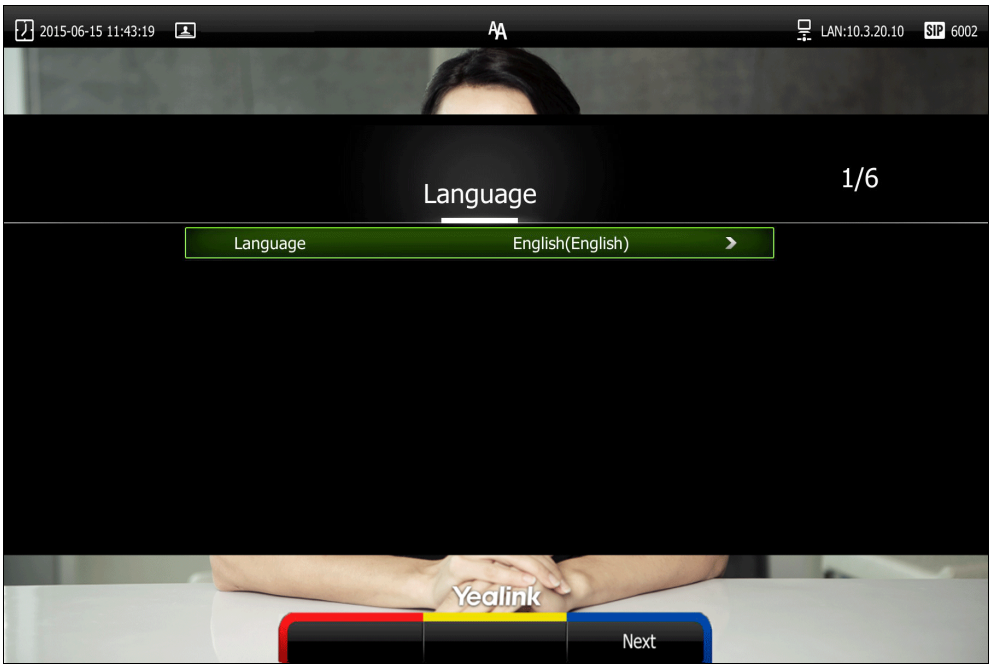
Setup Wizard

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

To complete the setup wizard via the remote control:

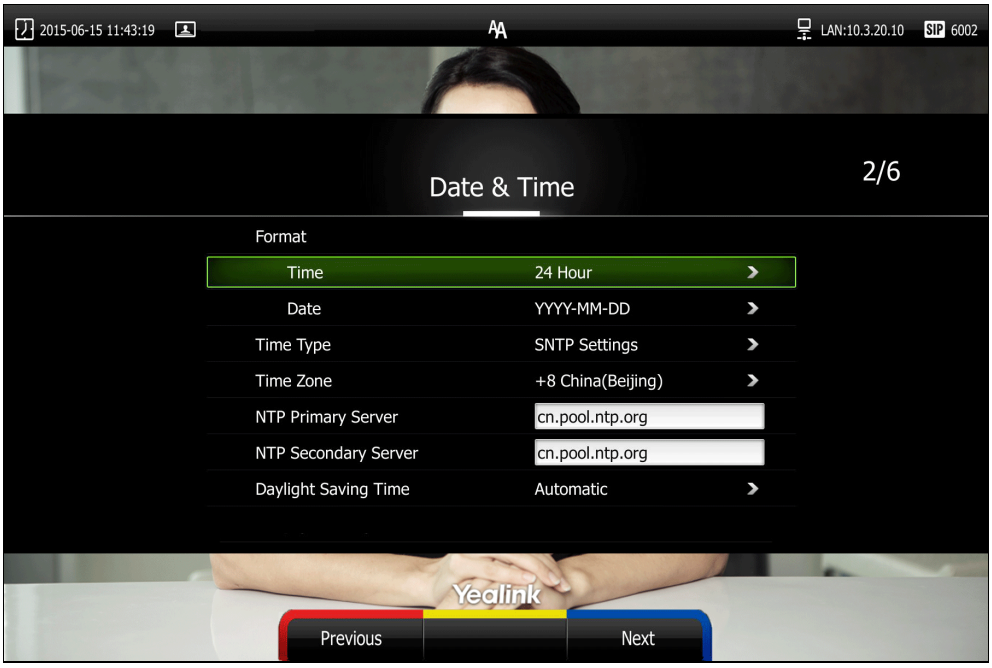
1. Set the language displayed on the display device.

The default language is English.



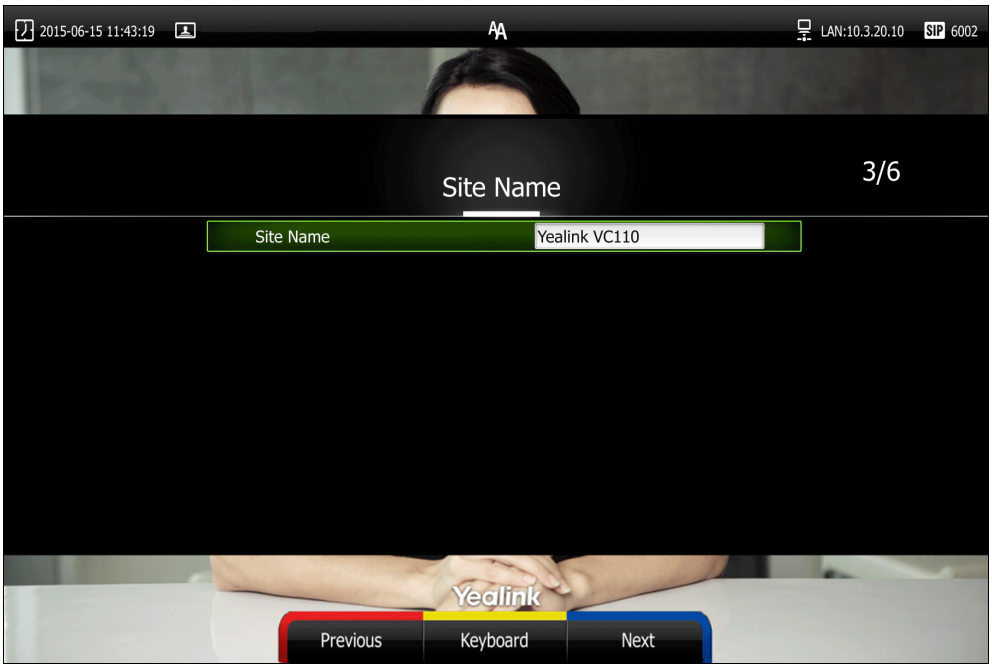
2. Press (**Next** soft key) to continue.
3. Set the date and time (e.g., set the time zone, time format, date format and the type of the daylight saving time).

   The endpoint obtains the time and date from the NTP server automatically by default. You can also configure the time and date manually. For more information, refer to on Date & Time page 128.



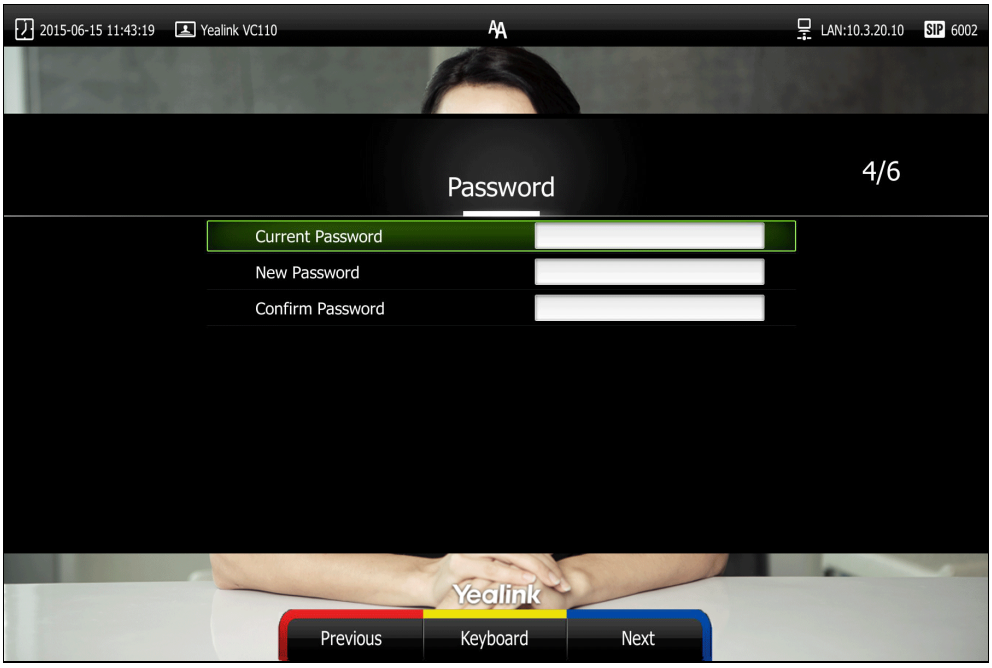
4. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
5. Edit the site name.

The default site name is "Yealink VC110".



6. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
7. Change the administrator password.

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



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

For more information, refer to Resetting to Factory on page 194.

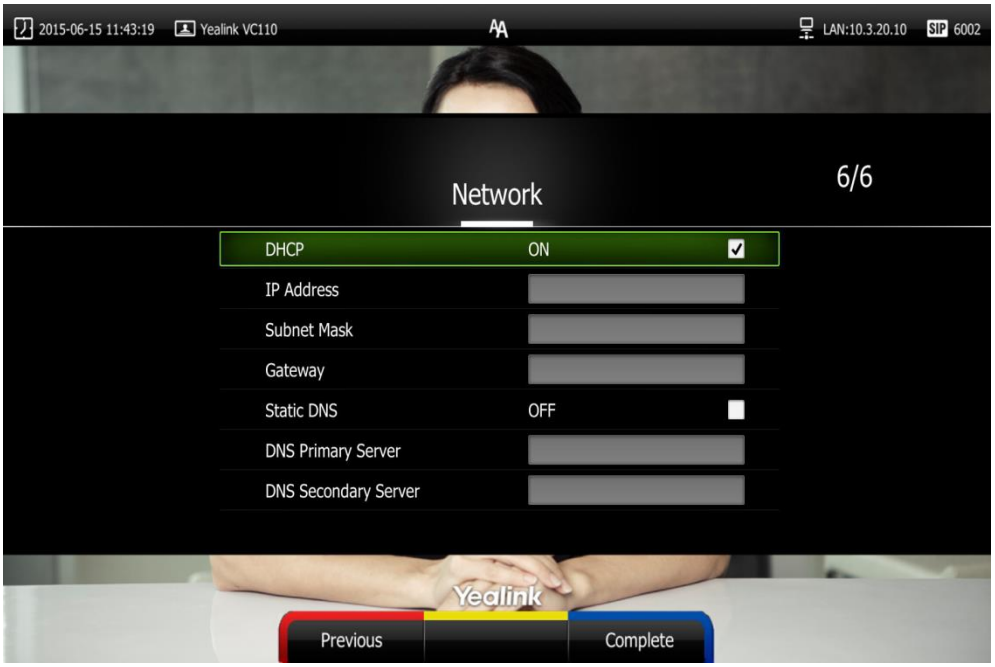
8. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.

   The display device displays firewall port mapping information.

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

10. Configure network settings.

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



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

Enabling Communication with Other Endpoints

- If you use Network Address Translation (NAT) to assign a public IP address to your VC110 endpoint for communication with devices outside your private network, you must enable NAT on your VC110 endpoint before placing calls. For more information, refer to Network Address Translation on page 78.
- If your VC110 endpoint communicates with other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to theVC110 endpoint through the reserved ports specified in Reserved Ports on page 75. And the required ports specified in Configuring the Endpoint for Use with a Firewall or NAT on page 75. Users placing calls through a firewall to endpoints may experience one-way audio or video if the firewall is not properly configured.
- If you are using Session Initiation Protocol (SIP) servers in your environment to place calls using the SIP protocol, refer to Configuring SIP Settings on page 99.
- If you are using H.323 gatekeepers in your environment and want to place calls using a name or extension with the H.323 protocol, refer to Configuring H.323 Settings on page 105.

Placing a Test Call from the Yealink VC110 endpoint

Yealink Demo1 to Yealink Demo3 are three default contacts stored in the local directory.

You can place a test call to the default contact, and the test call will be routed to the Yealink demo video conferencing endpoint. Yealink demo contacts can help users to test quickly whether the endpoint is normal after installation.

Configuring Network

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

This chapter provides the following sections:

- Preparing the Network
- Configuring LAN Properties
- Configuring Network Speed and Duplex Mode
- LLDP
- VLAN
- 802.1X Authentication
- H.323 Tunneling
- Configuring the Endpoint for Use with a Firewall or NAT
- Intelligent Firewall Traversal
- Quality of Service
- VPN

Preparing the Network

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

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

Type	Network Information
Type of endpoint	DHCP
	Static IP Address • IP address • Subnet mask • Gateway
DNS Server	IP address of DNS server
Call Type	Register information of SIP account
	Register information of H.323 account

Type	Network Information
802.1X	Authentication information

Configuring LAN Properties

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. The endpoint complies with the DHCP specifications documented in RFC 2131. DHCP by default, which allows the endpoint connected to the network to become operational by obtaining IP addresses and additional network parameters from the DHCP server.

DHCP Option

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

DHCP can be initiated by simply connecting the endpoint to the network. The endpoint broadcasts DISCOVER messages to request network information carried in DHCP options. The DHCP server responds with the specific values in the corresponding options.

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

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

Parameter	DHCP Option	Description
Domain Server	15	Specifies the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specifies the broadcast address in use on the client's subnet.
Network Time Protocol Servers	42	Specifies a list of the NTP servers available to the client by IP address.
Vendor-Specific Information	43	Identifies the vendor-specific information.
Vendor Class Identifier	60	Identifies the vendor type.
TFTP Server Name	66	Identifies a TFTP server when the 'name' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identifies a bootfile when the 'file' field in the DHCP header has been used for DHCP options.

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

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

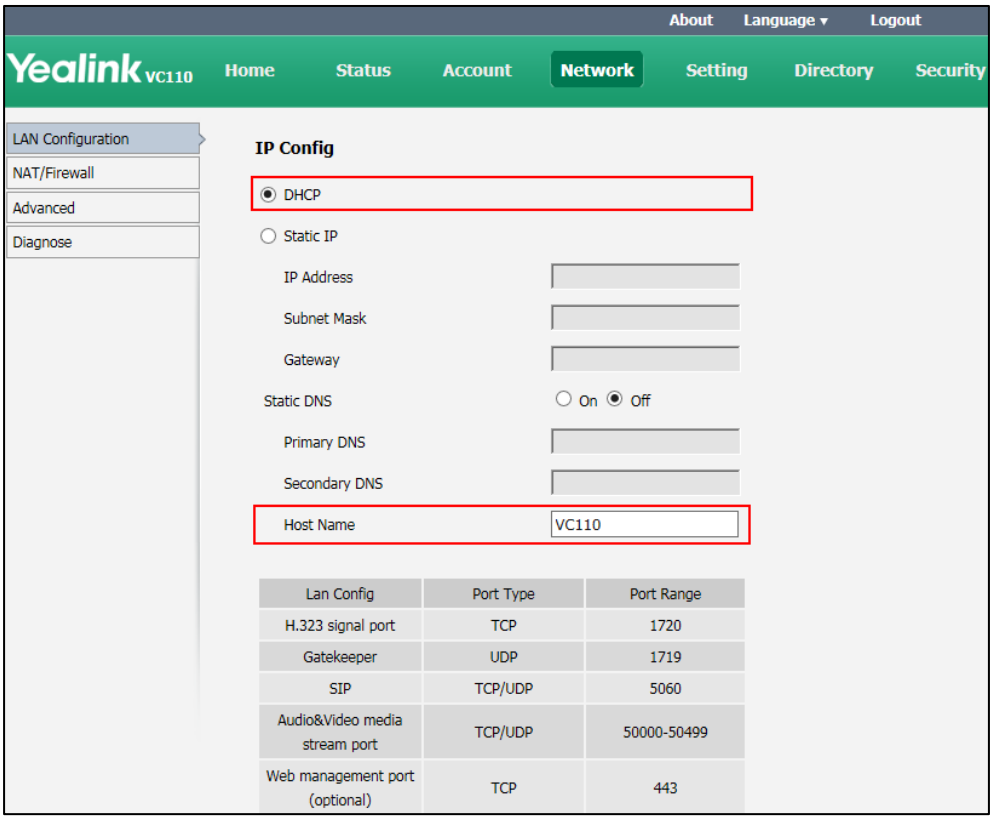
DHCP feature parameters on the endpoint are described below:

Parameter	Description	Configuration Method
DHCP	Enables or disables the endpoint to obtain network settings from the DHCP server. **Default:** Enabled **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Remote Control Web User Interface
Host Name	Configures the host name of the endpoint. **Default:** Blank **Note**: When the endpoint	Web User Interface

Parameter	Description	Configuration Method
	broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12. Host name is optional, so it is not a mandatory configuration item. For more information, contact your network administrator. If you change this parameter, the endpoint will reboot to make the change take effect.	

To configure DHCP via the web user interface:

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



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

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

To configure DHCP via the remote control:

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

Static DNS

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

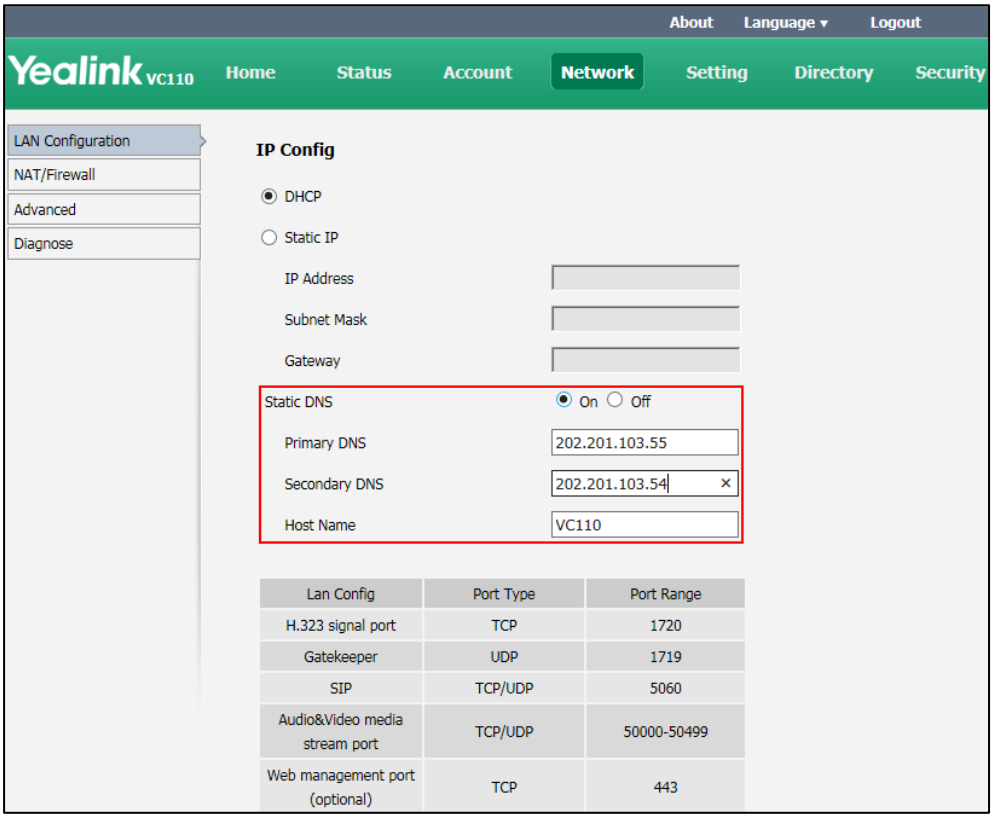
Parameters of static DNS on the endpoint are described below:

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

Parameter	Description	Configuration Method
	the "Static DNS" is set to On. If you change this parameter, the endpoint will reboot to make the change take effect.	

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

1. Click on **Network->LAN Configuration**.
2. In the **IP Config** block, mark the **DHCP** radio box.
3. In the **Static DNS** block, mark the **On** radio box.
4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.



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

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

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

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

1. Select **Menu->Advanced** (default password: 0000) **->LAN Configuration**.
2. Check the **DHCP** checkbox.
3. Check the **Static DNS** checkbox.
4. Enter the desired values in the **DNS Primary Server** and **DNS Secondary Server** fields respectively.

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

   The display device prompts "Reboot now?".

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

Configuring Network Settings Manually

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

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

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

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

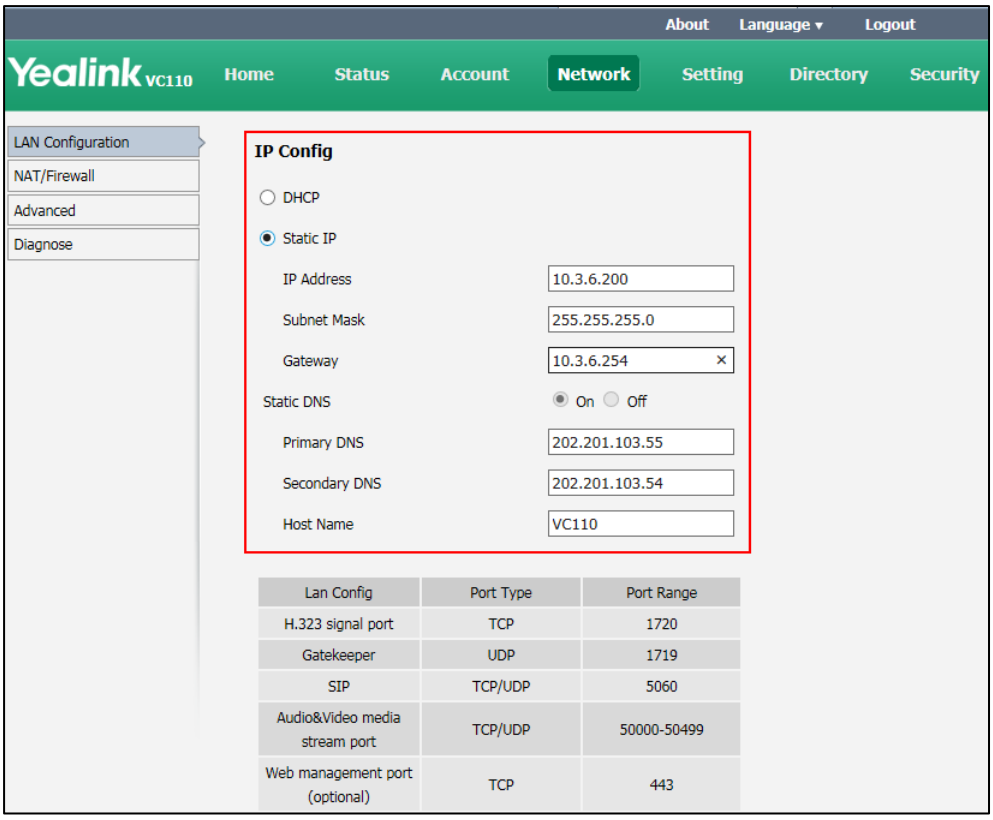
Parameter	Description	Configuration Method
Static IP	Enables or disables the endpoint to use manually configured network settings. **Default**: Disabled **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
IP Address	Configures the IP address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

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

To configure network settings manually via the web user interface:

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

3. Enter the IP address, subnet mask, default gateway, primary DNS and secondary DNS in the corresponding fields.



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

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

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

To configure network settings manually via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**LAN Configuration**.
2. Uncheck the **DHCP** checkbox.
3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **DNS Primary Server** and **DNS Secondary Server** fields respectively.
4. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

5. Select **OK** to reboot the endpoint immediately.

Configuring Network Speed and Duplex Mode

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

- Auto

- 10 Mbps Half Duplex
- 100 Mbps Half Duplex
- 10 Mbps Full Duplex
- 100 Mbps Full Duplex

Auto is configured on the endpoint by default.

Auto

Auto means that the switch will negotiate the network speed and duplex mode for the endpoints to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both endpoints.

Half-duplex

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

Full-duplex

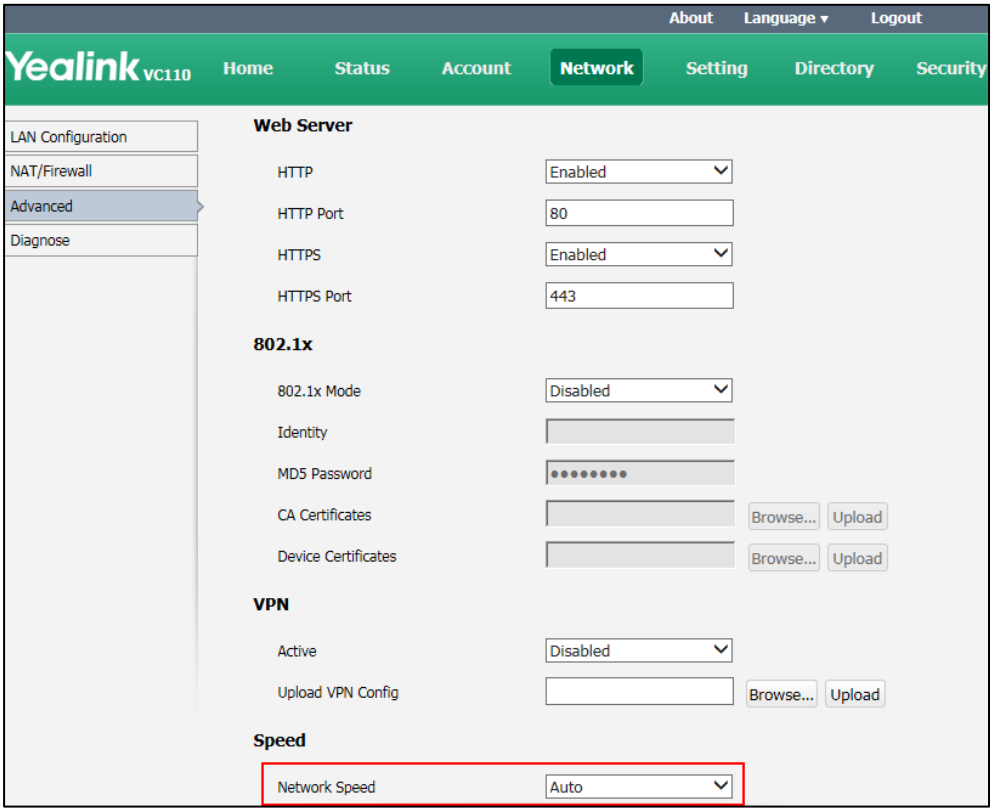
Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one endpoint can send data on the line while also receiving data.

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

Parameter	Description	Configuration Method
Network Speed	Specifies the network speed and duplex mode for the endpoint to use. **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 endpoint will reboot to make the change take effect.	Web User Interface

To configure the network speed via the web user interface:

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



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

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

VLAN

VLAN (Virtual Local Area Network) is used to divide a physical network logically into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

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

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

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

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the endpoint to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for the endpoint:

- Capabilities Discovery -- allows LLDP-MED endpoint to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify the endpoint which VLAN to use and QoS-related configuration for voice data. It provides a "plug and play" network environment.
- Power Management -- provides information related to how the endpoint is powered, power priority, and how much power the endpoint needs.
- Inventory Management -- provides a means to effectively manage the endpoint and its attributes, such as model number, serial number and software revision.

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

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the endpoint.
	Port ID	The MAC address of the endpoint.
	Time To Live	Seconds until data unit expires. The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the endpoint. The default value is "VC110".

TLV Type	TLV Name	Description
	System Description	Description of the endpoint. Description includes firmware version of the endpoint.
	System Capabilities	The supported and enabled endpoint capabilities. The Telephone capability is supported and enabled by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the endpoint. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the endpoint and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the endpoint.
	Inventory – Firmware Revision	Firmware revision of the endpoint.
	Inventory – Software Revision	Software revision of the endpoint.
	Inventory – Serial	Serial number of the endpoint.

TLV Type	TLV Name	Description
	Number	
	Inventory – Manufacturer Name	Manufacturer name of the endpoint. The default value is "IP_Phone".
	Inventory – Model Name	Model name of the endpoint. The default value is "VC110".
	Asset ID	Assertion identifier of the endpoint.

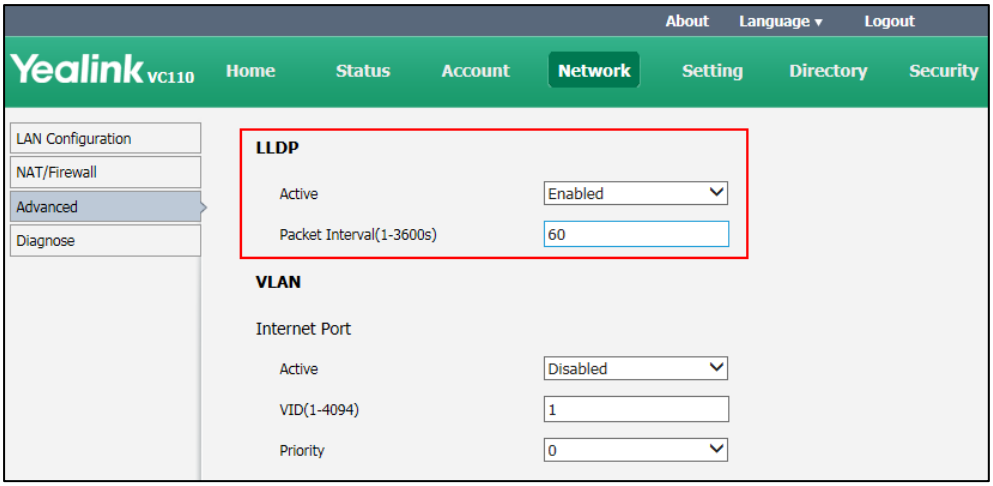
Parameters of LLDP feature on the endpoint are described below.

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

To configure LLDP via the web user interface:

1. Click on **Network->Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.

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



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

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

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

To configure LLDP via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **LLDP** block, check the **Active** checkbox.
3. Enter the desired value in the **Packet Interval (1-3600s)** field.
4. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

5. Select **OK** to reboot the endpoint immediately.

Manual Configuration for VLAN

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

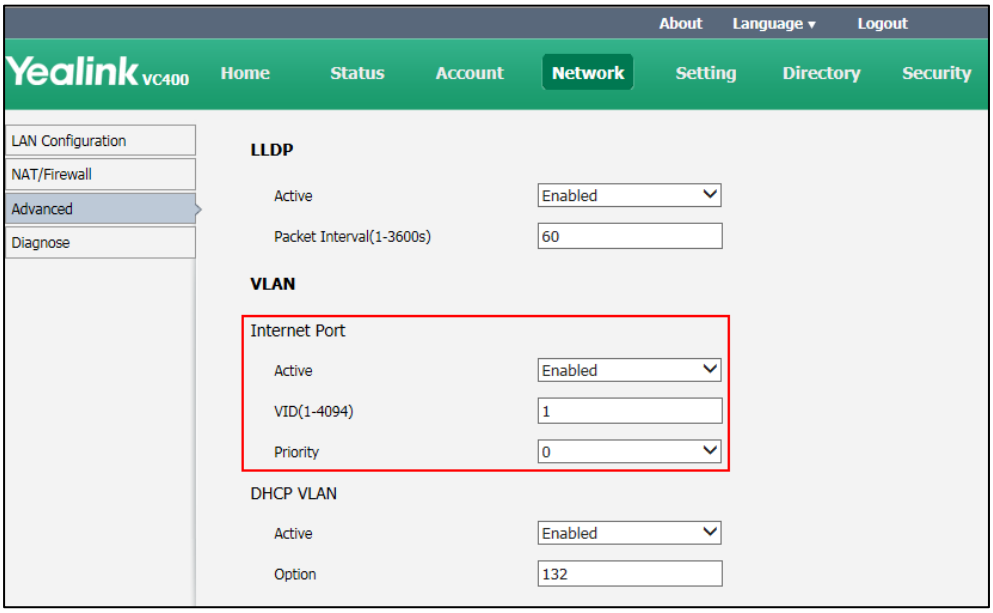
Parameters of manual VLAN on the endpoint are described below.

Parameter	Description	Configuration Method
Internet Port->Active	Enables or disables VLAN for the Internet (WAN) port. **Default:** Disabled **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Remote Control Web User Interface

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

To configure VLAN for Internet port via web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **Internet Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **Priority**.



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

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

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

To configure VLAN via the remote control:

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

   The display device prompts "Reboot now?".

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

DHCP VLAN

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

Parameters of VLAN feature on the endpoint are described below.

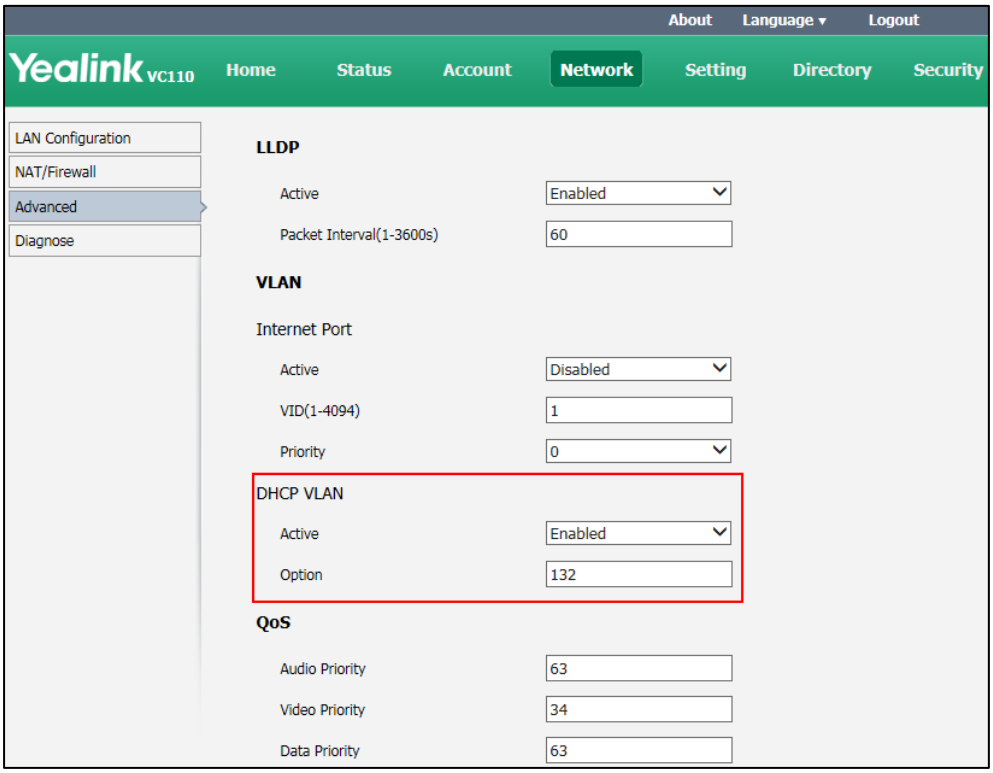
Parameter	Description	Configuration Method
DHCP VLAN->Active	Enables or disables the DHCP VLAN discovery feature on the endpoint. **Default:** Enabled **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
Option	Configures the DHCP option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

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

To configure DHCP VLAN discovery via the web user interface:

1. Click on **Network->Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **DHCP VLAN Active**.
3. Enter the desired option in the **Option** field.

   The default option is 132.



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

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

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN. The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the endpoint that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the endpoint provides credentials, such as user name and

default password, for the authenticator. The authenticator then forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the endpoint is allowed to access resources located on the protected side of the network.

The endpoint supports the authentication protocols EAP-MD5, EAP-TLS, PEAP-MSCHAPv2 and EAP-TTLS/EAP-MSCHAPv2 for 802.1X authentication.

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

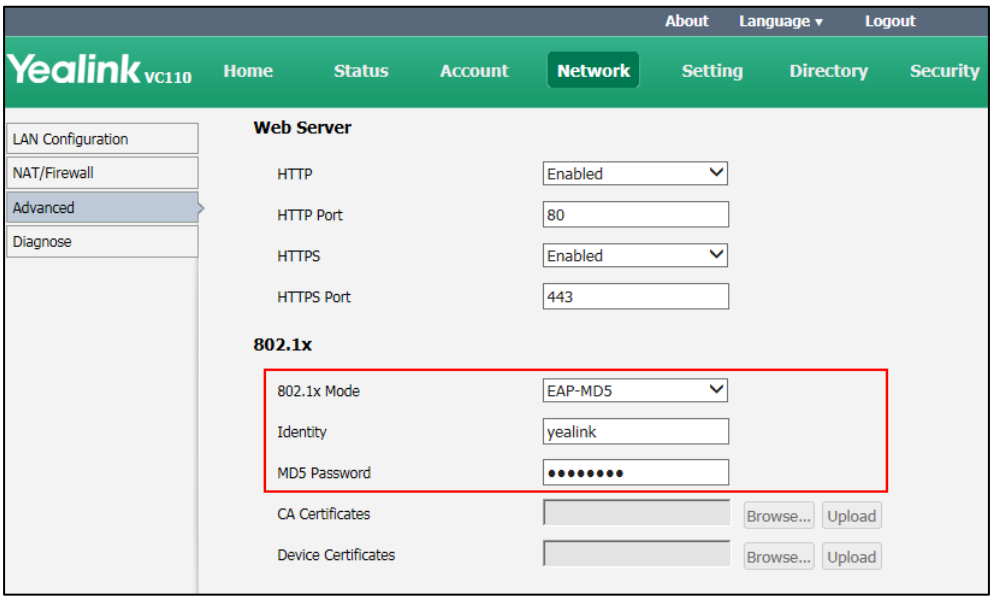
802.1X feature parameters on the endpoint are described below:

Parameter	Description	Configuration Method
802.1x Mode	Specifies the 802.1x authentication mode. • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 **Default:** Disabled **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Remote Control Web User Interface
Identity	Configures the user name for 802.1x authentication. **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
MD5 Password	Configures the password for 802.1x authentication. **Note**: If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the access URL of the CA certificate when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPV2 or	Web User Interface

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

To configure 802.1X via the web user interface:

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

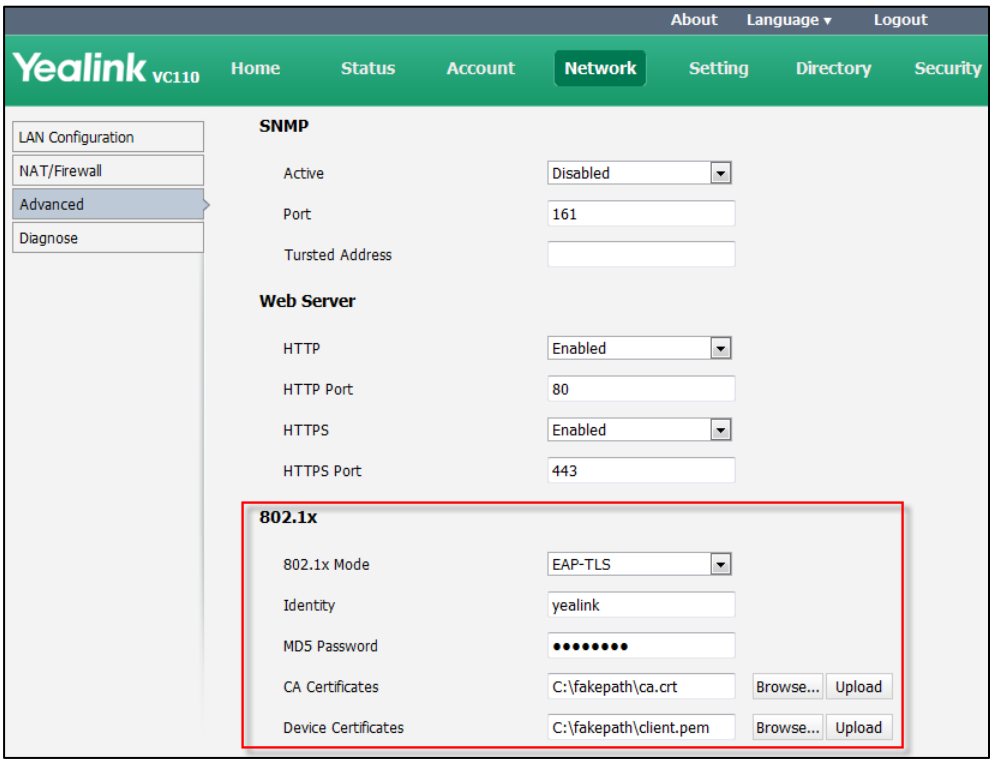


   b) If you select **EAP-TLS**:
      1) Enter the user name for authentication in the **Identity** field.
      2) Leave the **MD5 Password** field blank.

3) In the **CA Certificates** field, click **Browse** to locate the desired CA certificate (*.pem,*.crt, *.cer or *.der) from your local endpoint.

4) In the **Device Certificates** field, click **Browse** to locate the desired client certificate (*.pem or *.cer) from your local endpoint.

5) Click **Upload** to upload the certificates.



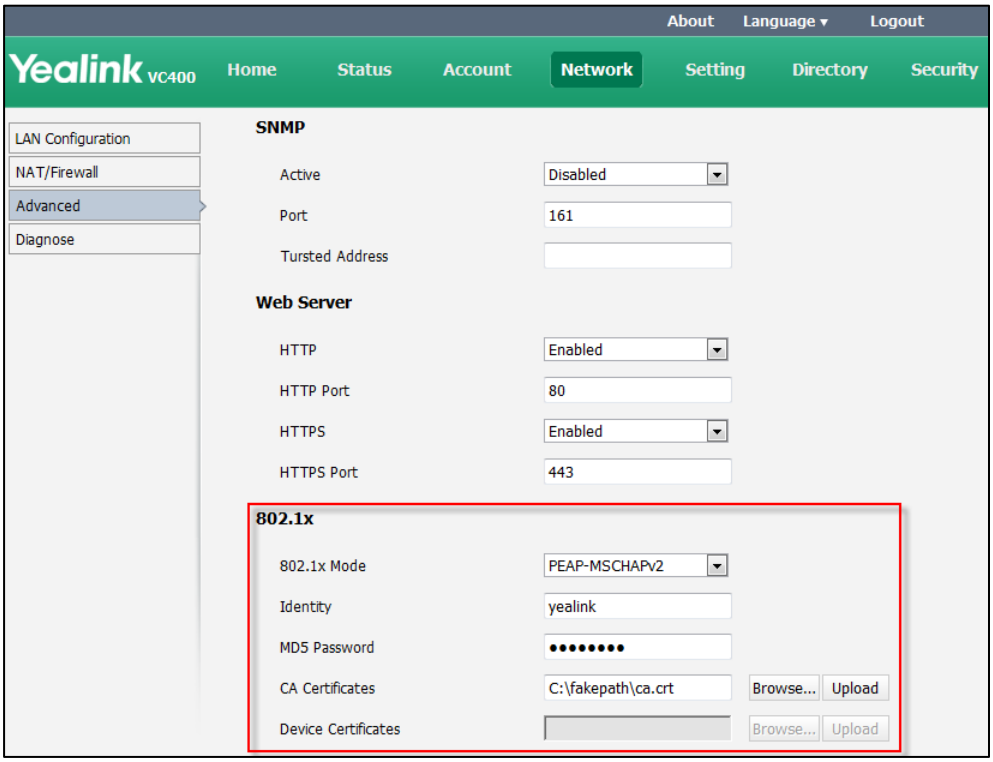
c) If you select **PEAP-MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.

2) Enter the password for authentication in the **MD5 Password** field.

3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem,*.crt, *.cer or *.der) from your local endpoint.

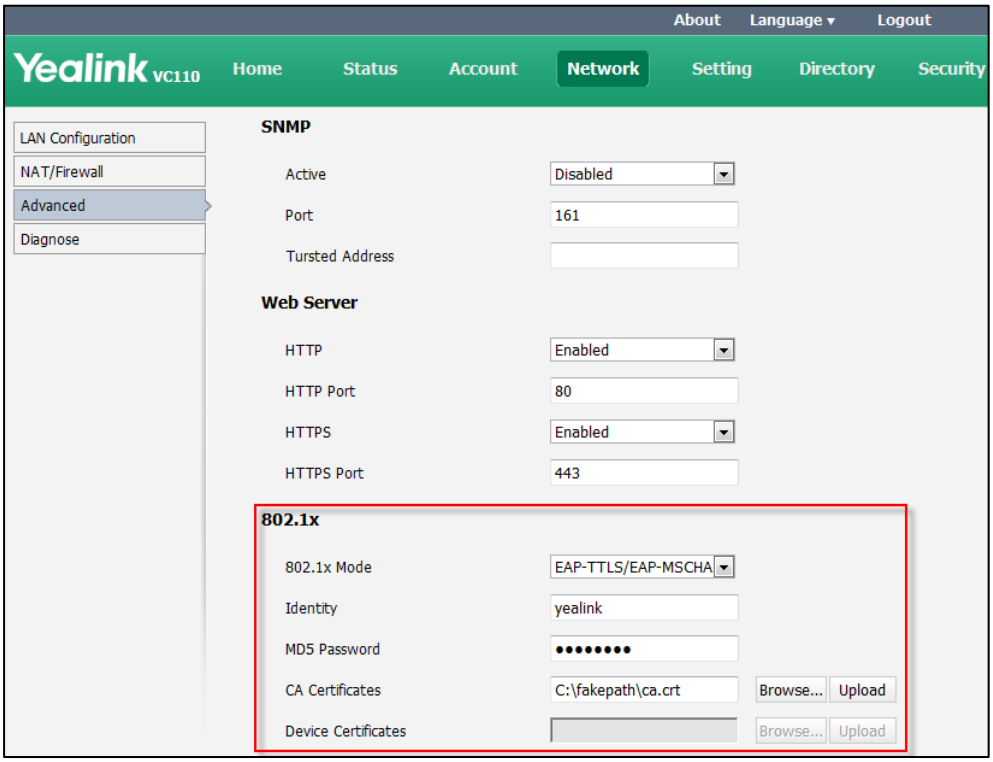
4) Click **Upload** to upload the certificate.



d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.
2) Enter the password for authentication in the **MD5 Password** field.
3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem,*.crt, *.cer or *.der) from your local endpoint.

4) Click **Upload** to upload the certificate.



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

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

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

To configure the 802.1X via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired mode from the pull-down list of **802.1x Mode**.
3. Press the **Save** soft key to accept the change.

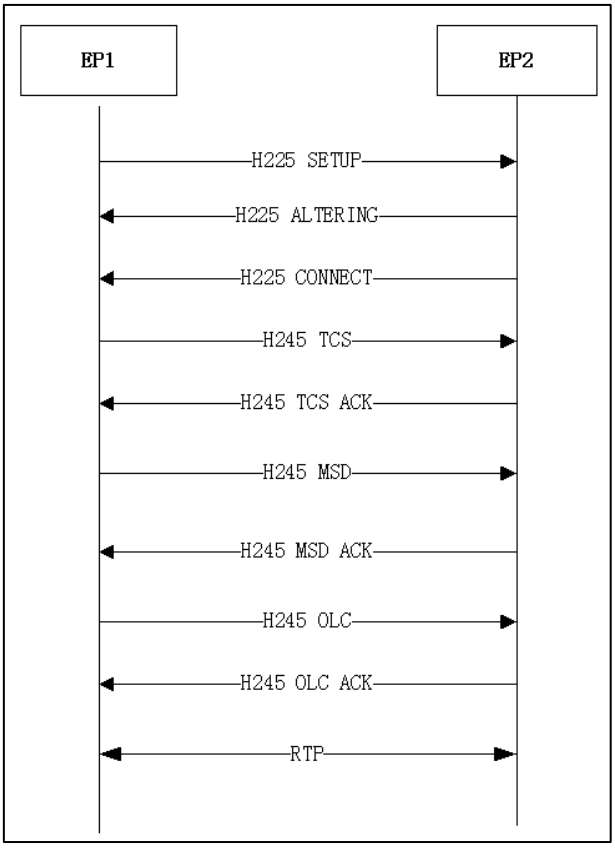
   The display device prompts "Reboot now?".

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

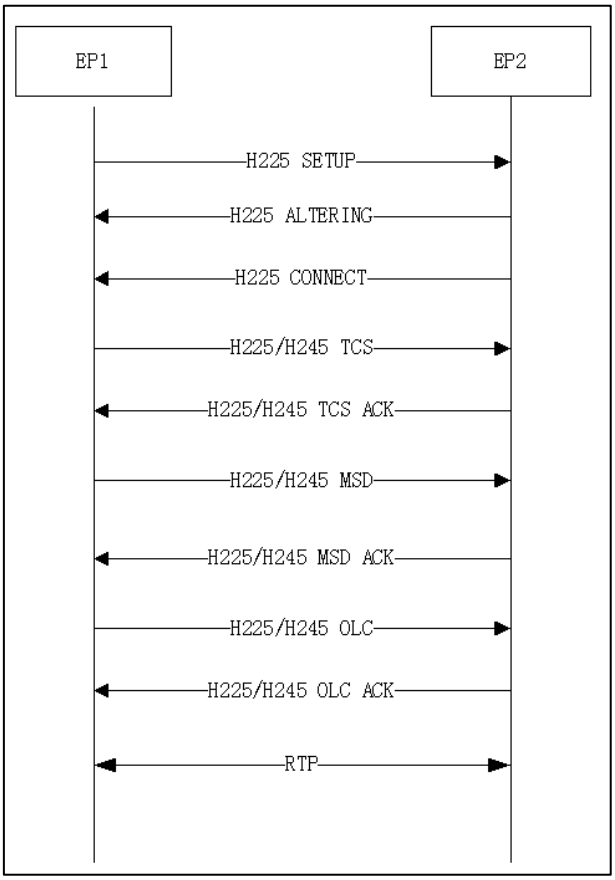
H.323 Tunneling

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

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



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

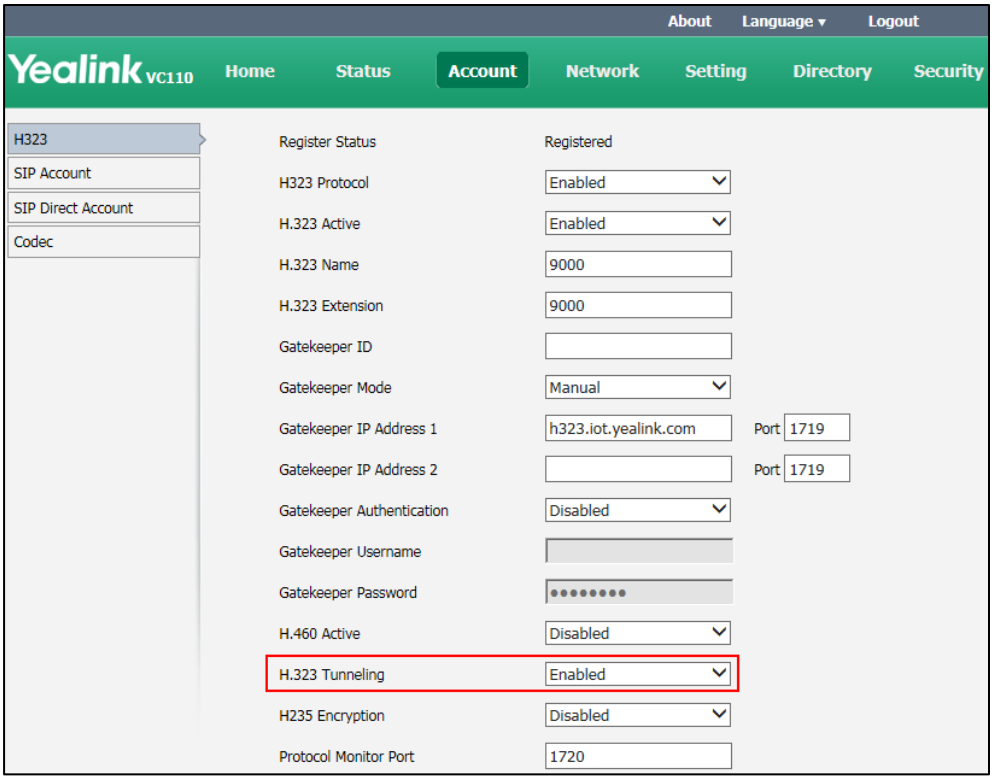


The parameter of the H.323 tunneling feature on the endpoint is described below:

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

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

1. Click on **Account**->**H323**.
2. Select the desired value from the pull-down list of **H.323 Tunneling**.



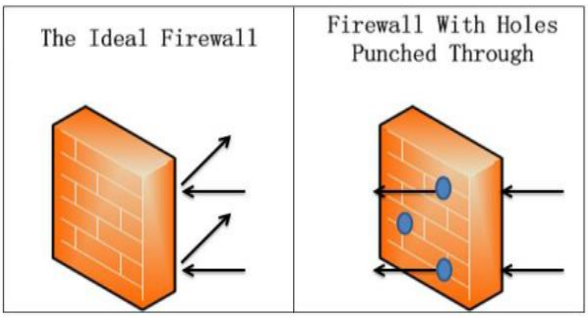
3. Click **Confirm** to accept the change.

To configure H.323 tunneling via the remote control:

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

Configuring the Endpoint for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with video conferencing equipment, you must configure the firewall to allow incoming and outgoing traffic to the VC110 endpoint through the reserved ports. Users placing calls through a firewall to endpoints may experience one-way audio or video if the firewall is not properly configured.



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

Description	Port Range	Port Type
Gatekeeper	1719	UDP
H.323 signal port	1720	TCP
SIP (default transport protocol)	5060	UDP
SIP (when selecting the TCP transport protocol)	5060	TCP
SIP (when selecting the TLS transport protocol)	5061	TCP
Reserved ports of the endpoint. For more information, refer to Reserved Ports on page 75.	50000-50499 (default range)	TCP/UDP
Web management port (optional)	443	TCP

Reserved Ports

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

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

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

Call Type	Number of Required Ports
Video	8 UDP ports (6 if presentation is disabled) 2 TCP ports
Voice	2 UDP ports 2 TCP ports

Required ports for a SIP two-way call:

Call Type	Number of Required Ports
Video	8 UDP ports (6 if presentation is disabled)
Voice	2 UDP ports

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

Endpoint	Maximum Connections	Required Ports for an H.323 Call		Required Ports for a SIP Call	
VC110	Two-way video call and a presentation and an audio call	10 UDP 4 TCP	50000-50009 50000-50003	10 UDP	50000-50009

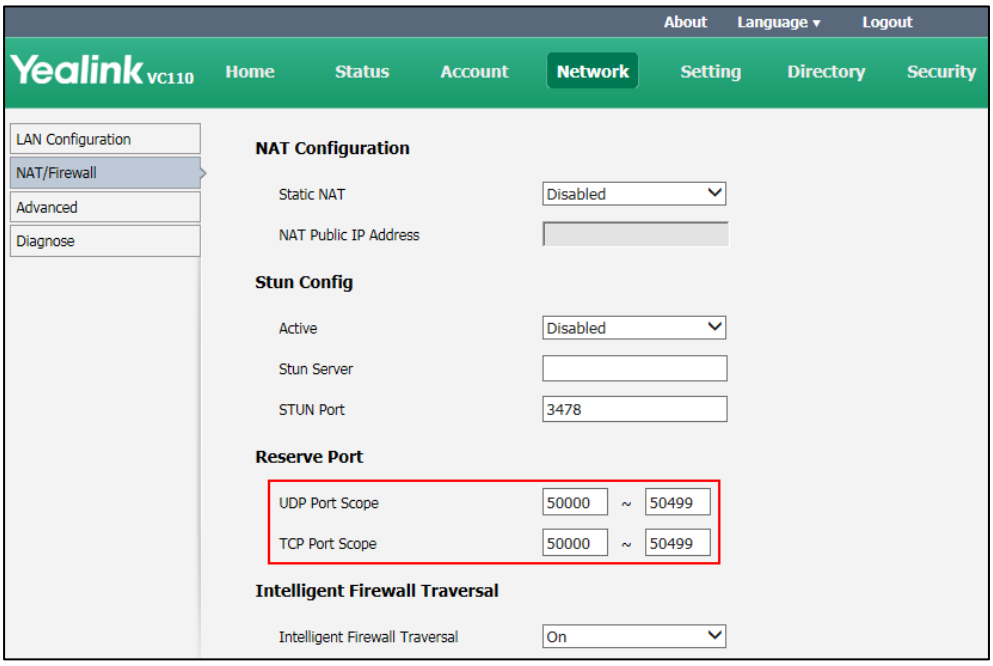
Parameters for reserved ports on the endpoint are described below:

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

Parameter	Description	Configuration Method
	the configured ports. If you change this parameter, the endpoint will reboot to make the change take effect.	

To configure reserved ports via the web user interface:

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



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

   A dialog box pops up to prompt that the settings will be implemented after a reboot.
5. Click **Confirm** to reboot the endpoint immediately.

To configure reserved ports via the remote control:

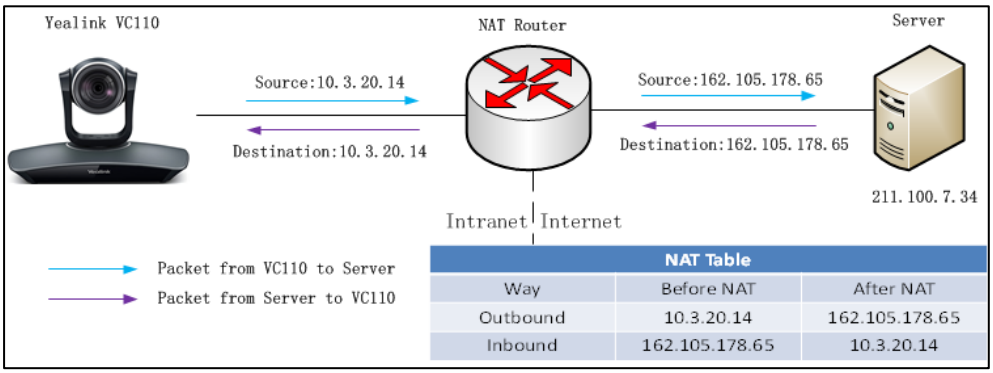
1. Select **Menu->Advanced** (default password: 0000) **->NAT/Firewall**.
2. In the **Reserved** block, configure the range of the UDP ports and TCP ports.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the endpoint immediately.

Network Address Translation

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

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



Static NAT

If NAT/Firewall devices do not support the ALG. VC110 video conferencing endpoint must be configured with the static NAT.

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

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

Note If H.460 firewall traversal is enabled on the endpoint, the endpoint will automatically ignore the static NAT settings for H.323 calls. For more information on H.460 firewall traversal, refer to on H.460 Firewall Traversal page 88.

Static NAT feature parameters on the endpoint are described below:

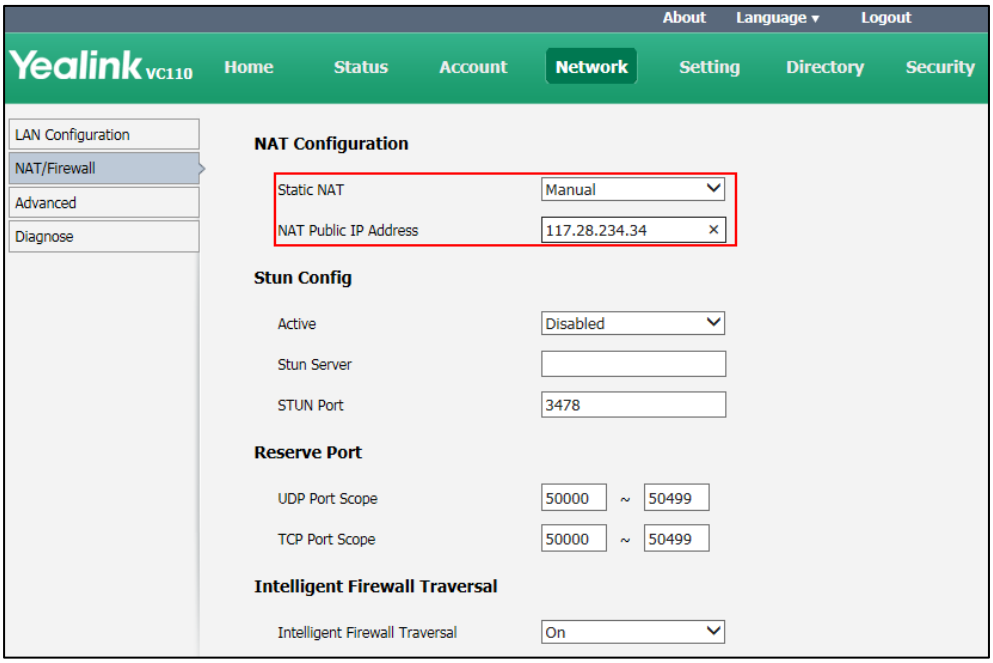
Parameter	Description	Configuration Method
Static NAT	Specifies the static NAT type. • **Disabled**—the endpoint	Remote Control Web User Interface

Parameter	Description	Configuration Method
	does not use the NAT feature. • **Manual**—the endpoint uses the manually configured NAT public address. • **Auto**—the endpoint obtains the NAT public address from the Yealink-supplied server. **Default:** Disabled	
NAT 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 endpoint if the static NAT is set to **Manual**.	Remote Control Web User Interface
NAT_Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP direct account separately. • **Disabled** • **STUN** • **StaticNat** **Default:** Disabled **Note:** Static NAT works only if this parameter is set to StaticNat.	Web User Interface

To configure static NAT via the web user interface:

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

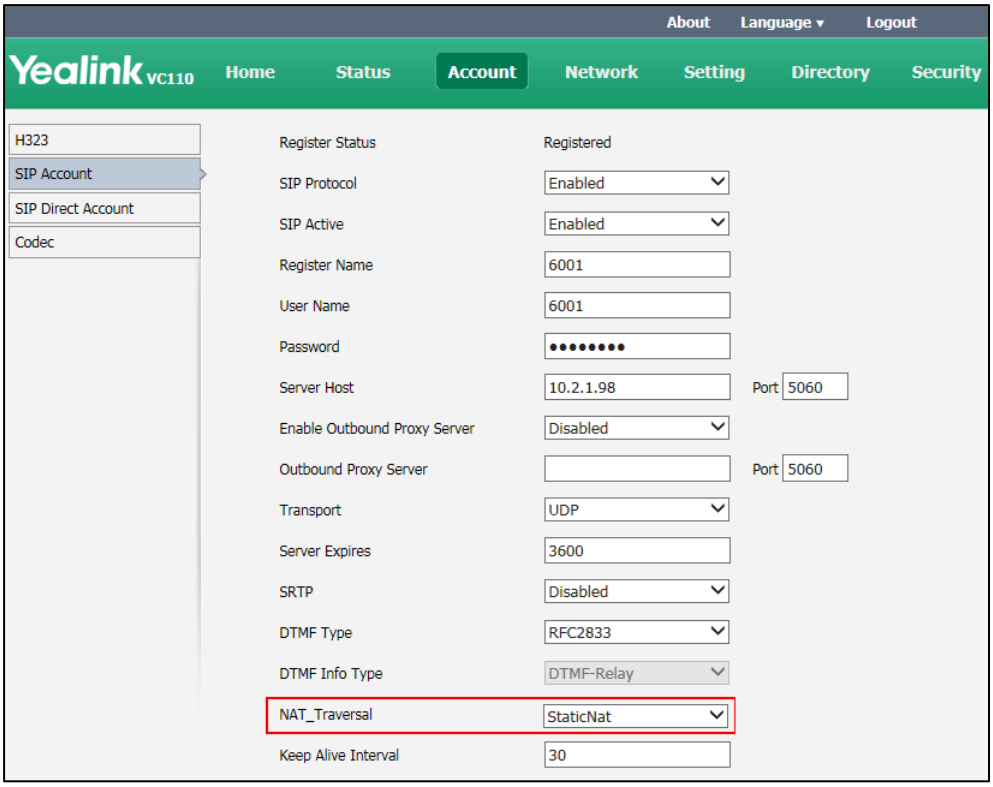
3. Configure the NAT public address in the **NAT Public IP Address** field if **Manual** is selected from the pull-down list of **Static NAT**.



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

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

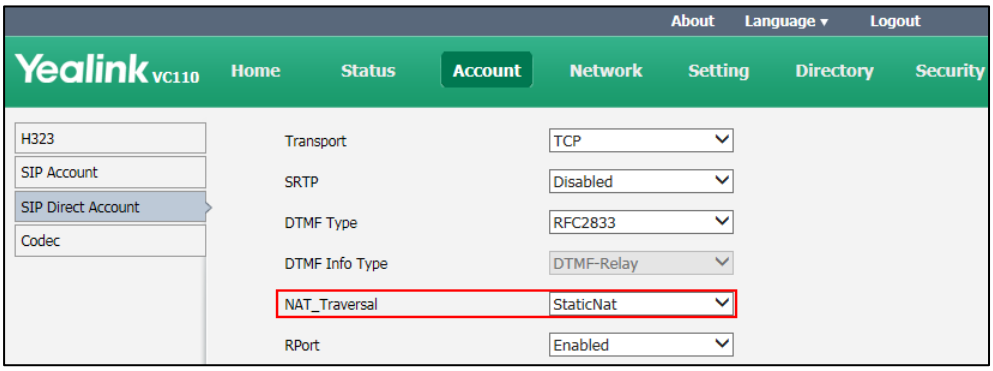
1. Click on **Account->SIP Account**.
2. Select **StaticNat** from the pull-down list of **NAT_Traversal**.



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

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

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



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

To configure static NAT via the remote control:

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

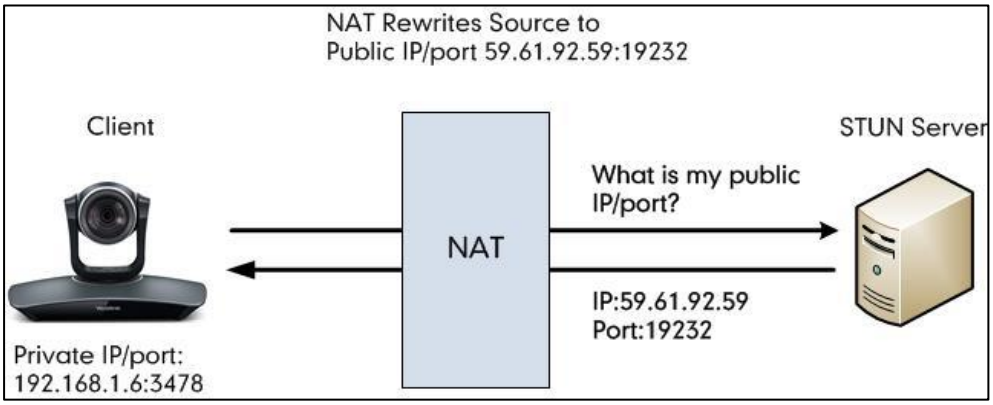
To configure static NAT for SIP direct account via the remote control:

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

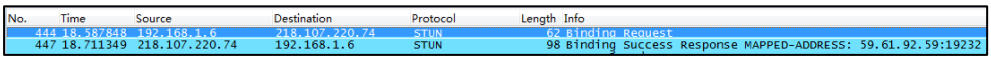
STUN

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows entities behind a NAT to first discover the presence of a NAT and the type of NAT (for more information on the NAT types, refer to NAT Types on page 85.) and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to work as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and

port used, and then informs the client. For more information, refer to RFC3489.



Capturing packets after you enable the STUN feature, you can find that the VC110 video conferencing endpoint sends Binding Request to the STUN server, and then mapped IP address and port is placed in the Binding Response: Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232.



No.	Time	Source	Destination	Protocol	Length	Info
444	13.587848	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

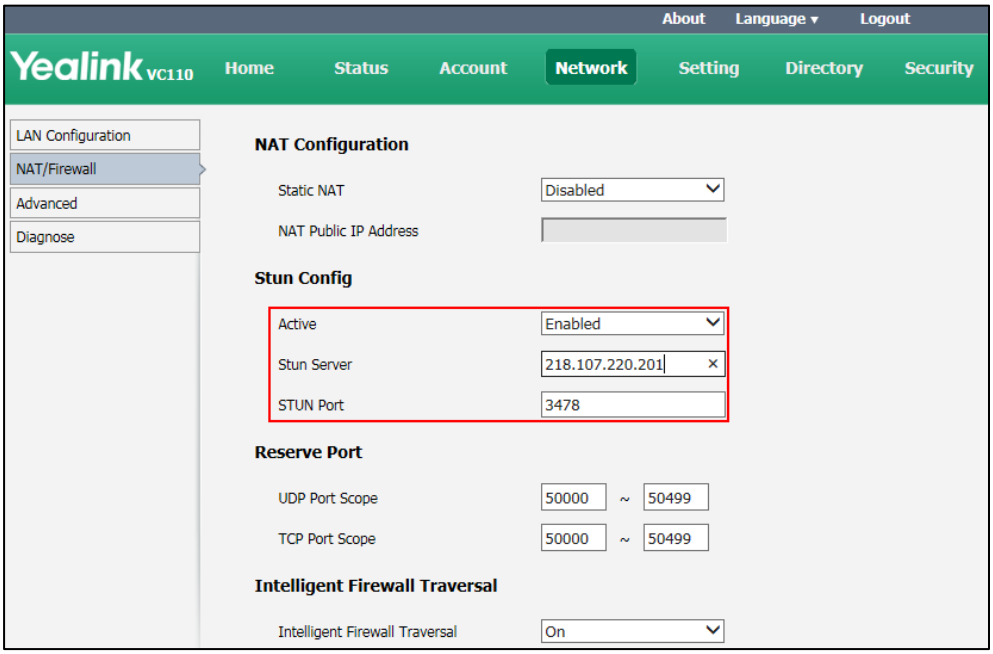
STUN feature parameters on the endpoint are described below:

Parameter	Description	Configuration Method
Active	Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the endpoint. **Default**: Disabled	Remote Control Web User Interface
STUN Server	Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. **Default**: Blank	Remote Control Web User Interface
STUN Port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Default:** 3478	Remote Control Web User Interface
NAT_Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP direct account separately. • **Disabled** • **STUN**	Web User Interface

Parameter	Description	Configuration Method
	• **StaticNat** **Default:** Disabled **Note:** STUN works only if this parameter is set to STUN.	

To configure STUN server via web user interface:

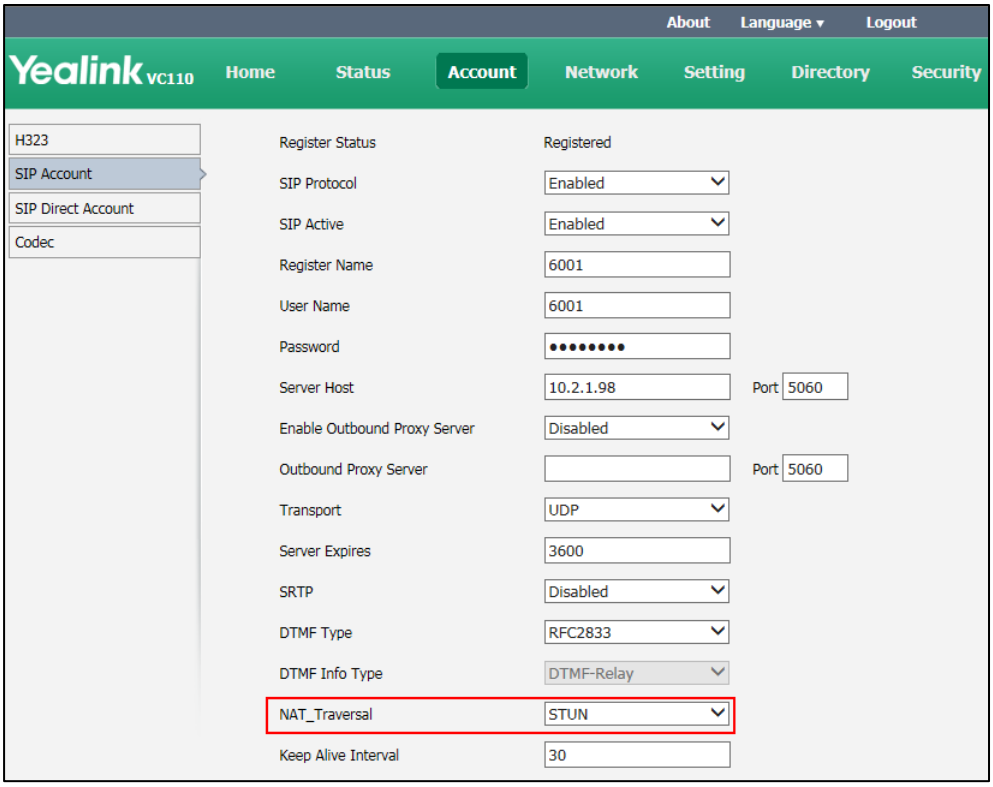
1. Click on **Network->NAT/Firewall**.
2. In the **Stun Config** block, select the desired value from the pull-down list of **Active**.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
4. Enter the port of the STUN server in the **Port** field.



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

To configure STUN for SIP account via web user interface:

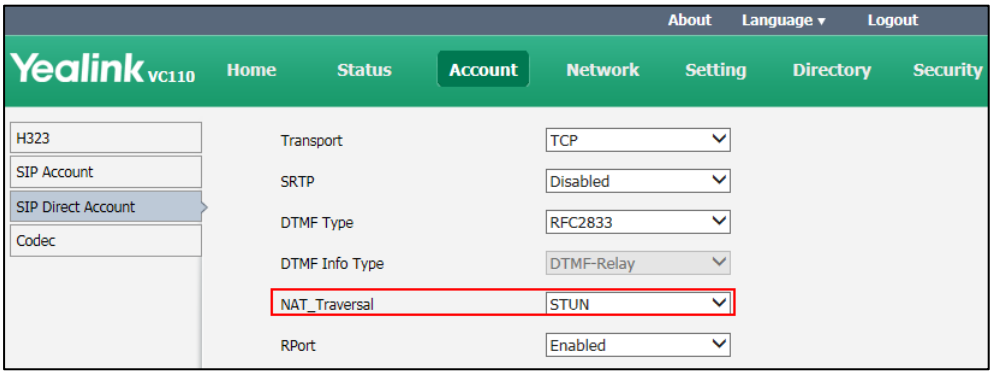
1. Click on **Account->SIP Account**.
2. Select **STUN** from the pull-down list of **NAT_Traversal**.



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

To configure STUN for SIP direct account via web user interface:

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



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

To configure STUN server via the remote control:

1. Select **Menu->Advanced** (default password: 0000) **->NAT/Firewall**.

   Mark the **ON** radio box in the **STUN Active** field.

2. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
3. Enter the port of the STUN server in the **Port** field.
4. Press the **Save** soft key to accept the change.

To configure STUN server for SIP direct account via the remote control:

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

NAT Types

Full Cone:

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

Restricted Cone:

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

Port Restricted Cone:

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

Symmetric:

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

Keep Alive

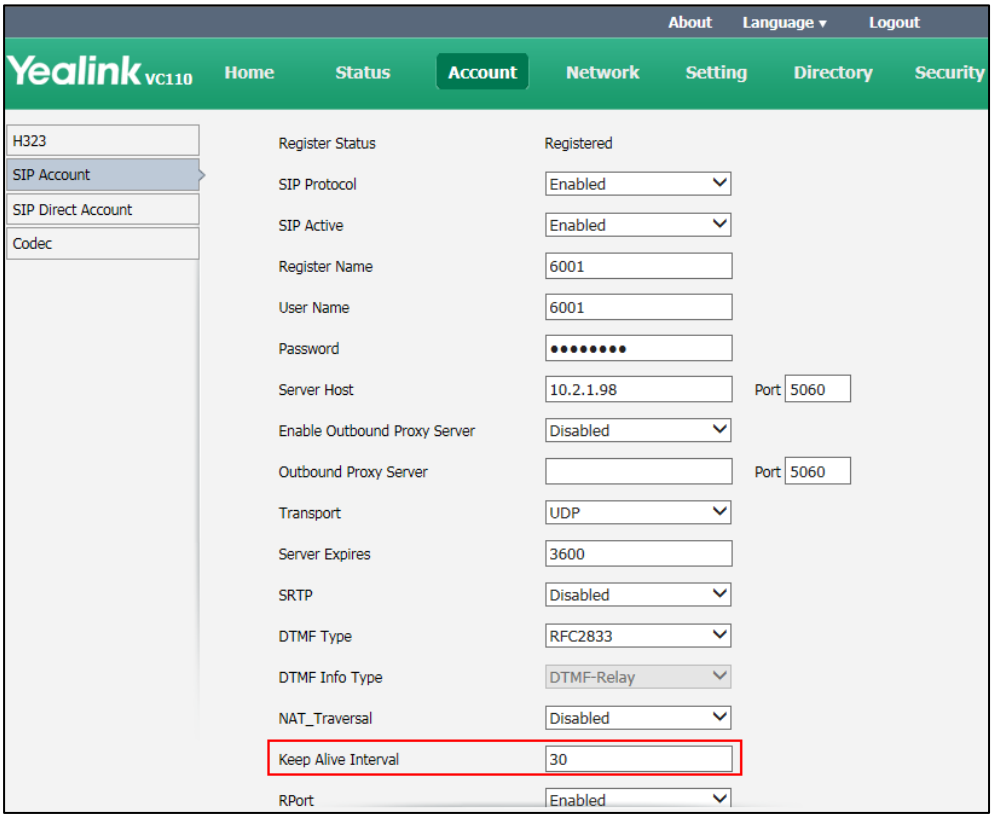
The endpoint can send keep-alive packets to NAT device for keeping the communication port open.

The Keep alive interval parameter on the endpoint is described below:

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

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

1. Click on **Account->SIP Account**.
2. Enter the keep alive interval in the **Keep Alive Interval** field.



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

Rport

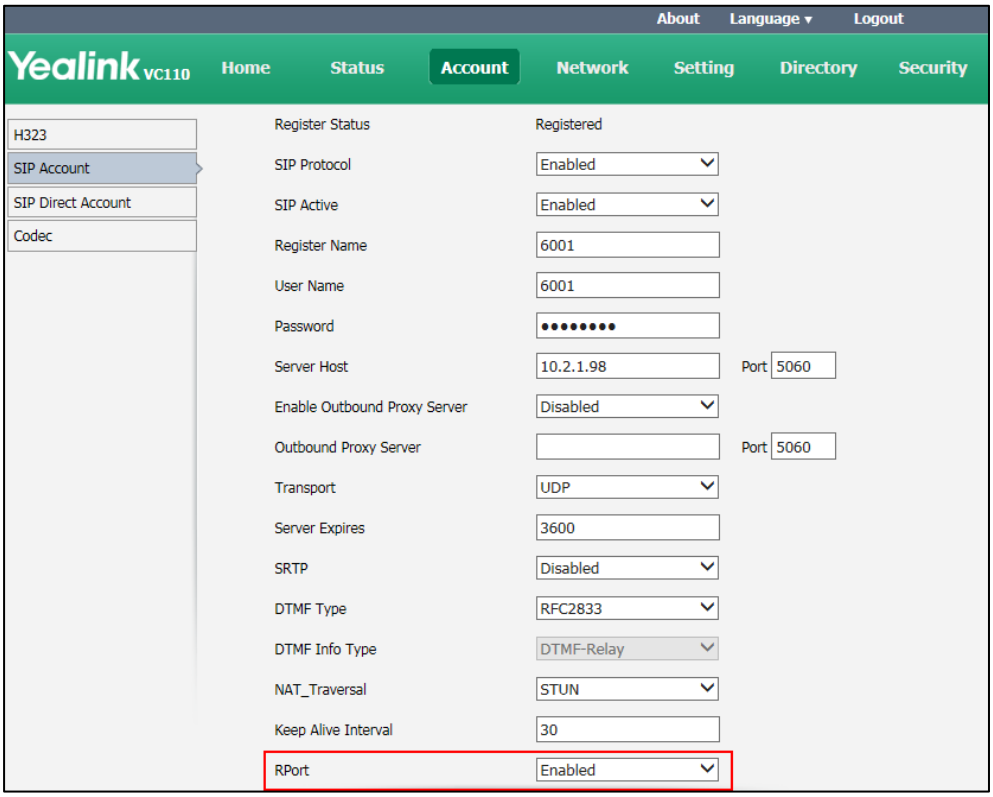
Rport in RFC 3581, allows a client to request that the server sends the response back to the source port from which the request came. Rport feature depends on support from a SIP server.

The rport parameter on the endpoint is described below:

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

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

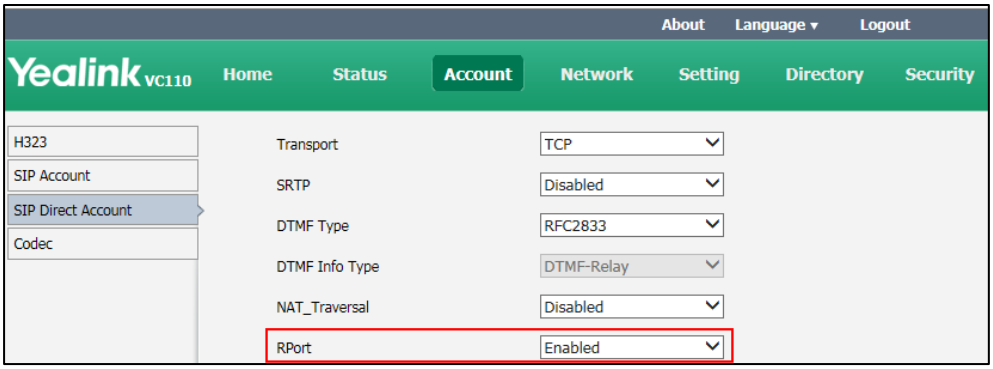
1. Click on **Account->SIP Account**.
2. Select the desired value from the pull-down list of **RPort**.



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

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

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



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

H.460 Firewall Traversal

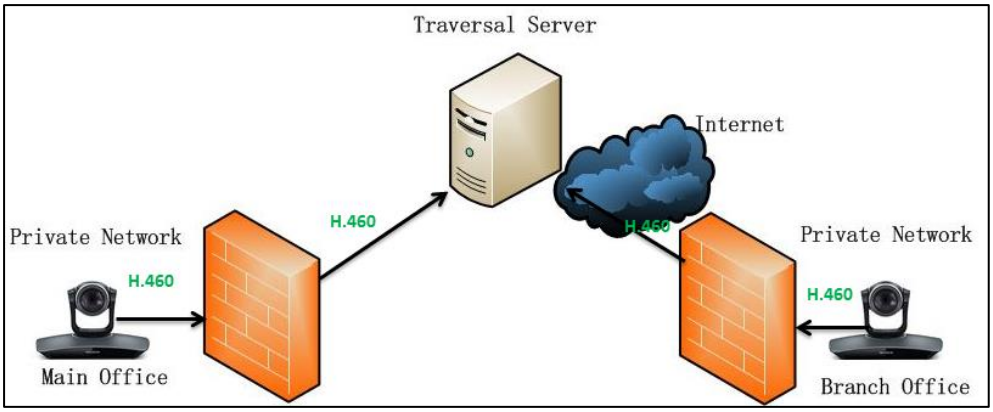
H. 323 includes signal based on TCP, while the STUN solution cannot realize the NAT traversal of TCP. Before the emergence of H.460, Enterprises have their own firewall/NAT traversal solutions, which are incompatible with each other. Therefore, IP communication between enterprises is difficult. H.460 resolves the compatibility problem.

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

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

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

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

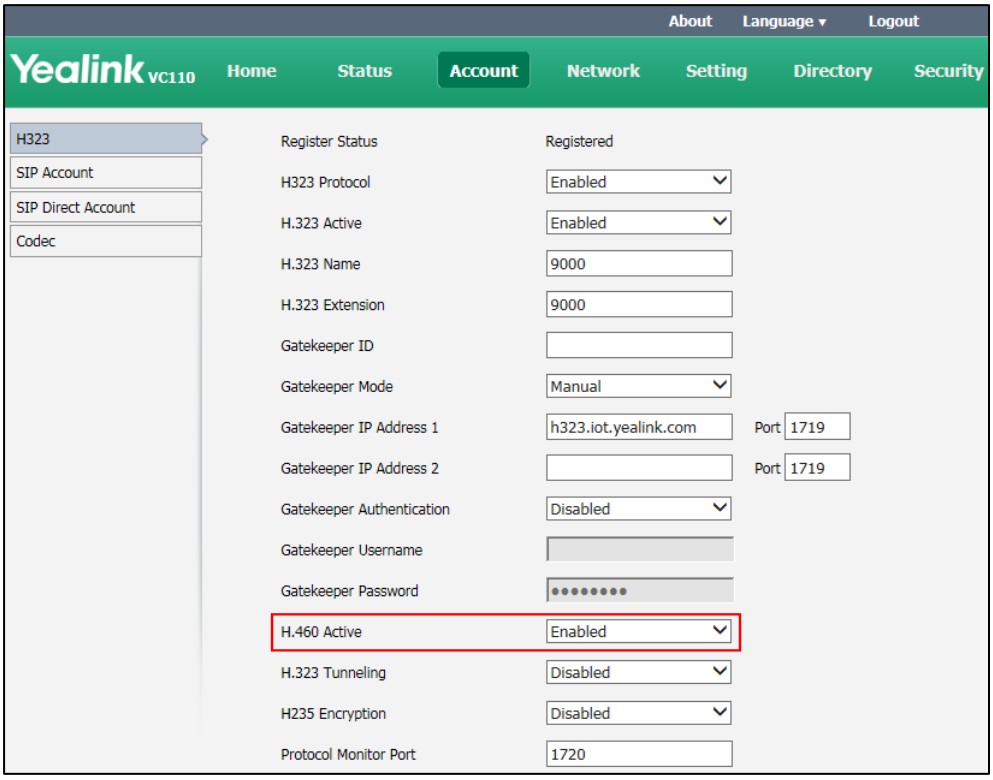


The H.460 firewall traversal parameter is described below:

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

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

1. Click on **Account->H323**.
2. Select the desired value from the pull-down list of **H.460 Active**.



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

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

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

Intelligent Firewall Traversal

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

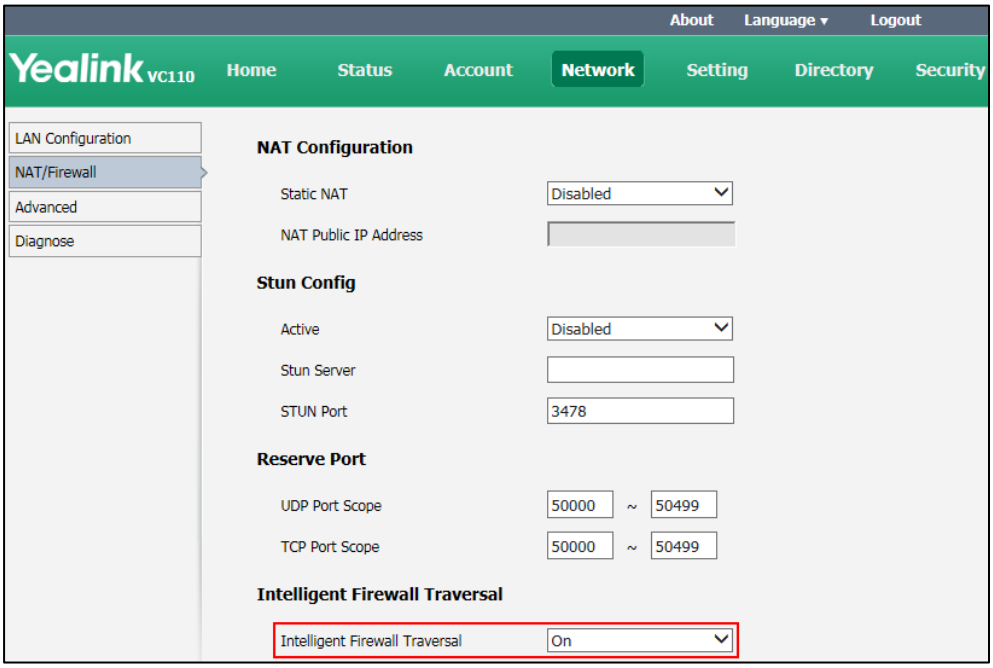
In some cases, the head office is in the WAN and lacks a VPN network, while the branch office is the LAN, and no port mapping is configured on its firewall. You can enable the intelligent firewall traversal feature, so that the head office can share content with branch office, or control the camera of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

The intelligent firewall traversal parameter is described below:

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

To configure intelligent firewall traversal via the web user interface:

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



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

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network. This allows the transport of traffic with special requirements. QoS guarantees are important for applications that require a fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides a better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in the IP networks. It provides no guarantees for data delivery, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated

Services Code Point (DSCP) is used to define DiffServ classes and is stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** – backwards compatible with IP precedence. Class Selector code points are of the form "xxx000". The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** – the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** – defines a method by which BAs (Bandwidth Allocations) can be given different forwarding assurances.
- **Default PHB** – specifies that a packet marked with a DSCP value of "000000" gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, , with regard to guaranteeing how that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice, video and data packets are given priority over other kinds of network traffic. Yealink video conferencing endpoints support the DiffServ model of QoS. DSCPs for voice, video and data packets that can be specified respectively.

Voice QoS

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

Video QoS

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

Data QoS

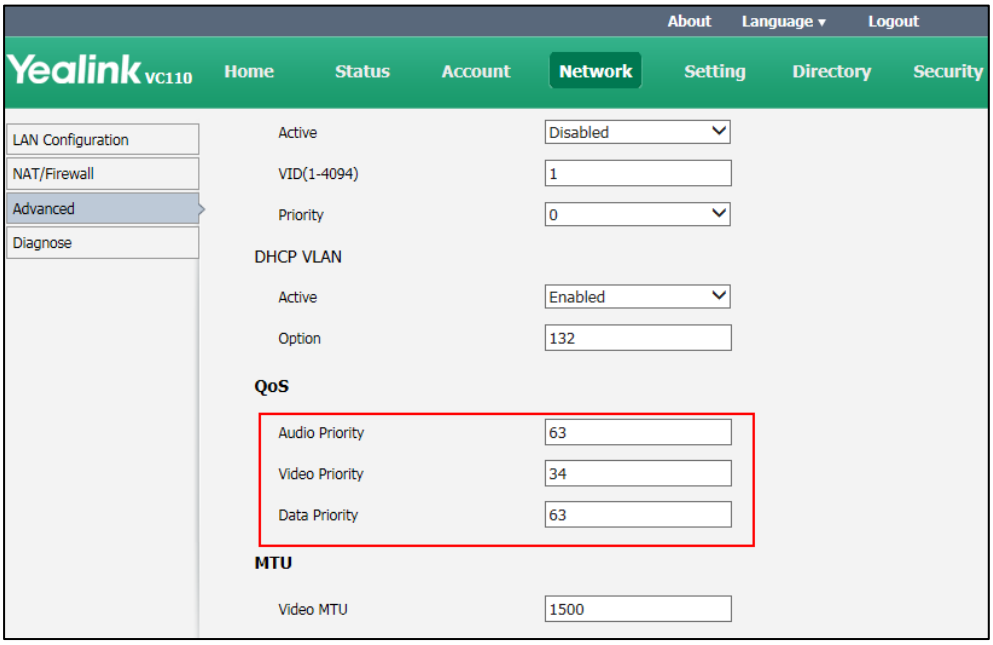
To ensure good call quality, data packets (e.g., SIP signaling and H.225 call signaling) emanated from the endpoint should be configured with a high transmission priority.

QoS feature parameters on the endpoint are described below.

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

To configure QoS via the web user interface:

1. Click on **Network->Advanced**.
2. In the **QoS** block, enter the desired values in the corresponding fields.



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

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

To configure QoS via the remote control:

1. Select **Menu->Advanced** (default password: 0000) **->Advanced Network**.
2. In the **Diffserv QoS** block, enter the desired values in the corresponding fields.
3. Press the **Save** soft key to accept the change.

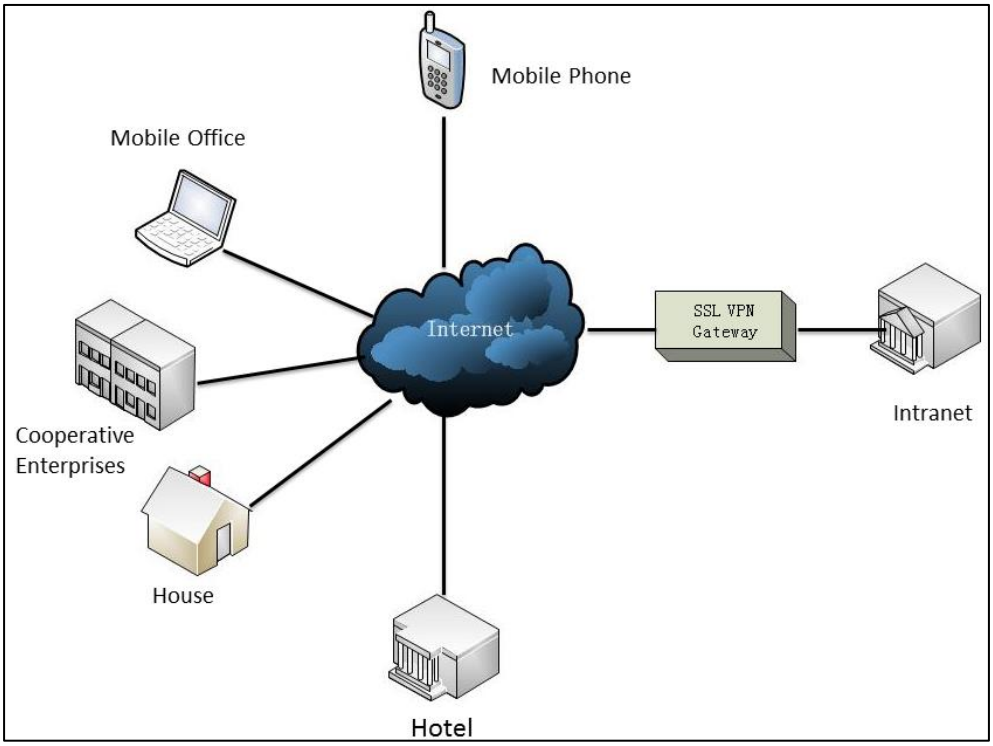
   The display device prompts "Reboot now?".
4. Select **OK** to reboot the endpoint immediately.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructures, such as the Internet. VPN has become more prevalent due to the benefits of scalability, reliability, convenience and security. VPN provides remote offices or individual users with secure access to their organization's network. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can also be classified by the

protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

The endpoint supports SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities and is designed work with the TUN/TAP virtual networking interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection, while TUN simulates a network layer device and provides a virtual network segment. The endpoint uses OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the endpoint, the endpoint works as a VPN client and uses the certificates to authenticate the VPN server.



To use VPN, the compressed package of VPN-related files should be uploaded to the endpoint in advance. The file format of the compressed package must be *.tar. The VPN-related files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information, refer to *OpenVPN Feature on Yealink IP Phones*.

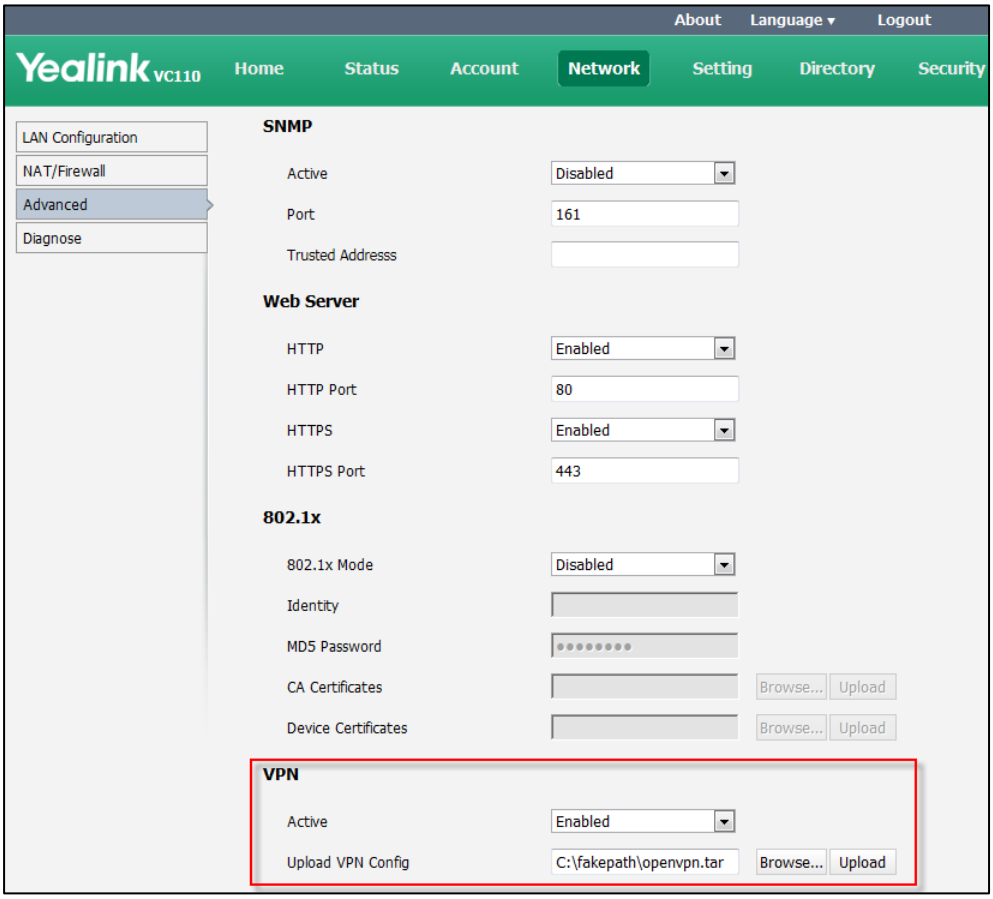
VPN feature parameters on the endpoint are described below.

Parameter	Description	Configuration Method
VPN->Active	Enables or disables VPN feature on the endpoint. **Default:** Disabled **Note**: You need to upload the	Remote Control Web User Interface

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

To configure VPN via the web user interface:

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



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

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

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

To configure VPN via the remote control:

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

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the endpoint immediately.

Configuring Call Preferences

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

This chapter provides the following sections:

- Configuring SIP Settings
- Configuring H.323 Settings
- DTMF
- Codecs
- Call Type
- Do Not Disturb
- Auto Answer
- History Record
- Call Match
- Bandwidth
- Video Size Mode
- Ringback Timeout
- Auto Refuse Timeout

Configuring SIP Settings

Yealink VC110 video conferencing endpoint supports Session Initiation Protocol (SIP). If your server supports SIP, you can use SIP to establish calls.

SIP Account

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

SIP account parameters on the endpoint are described below:

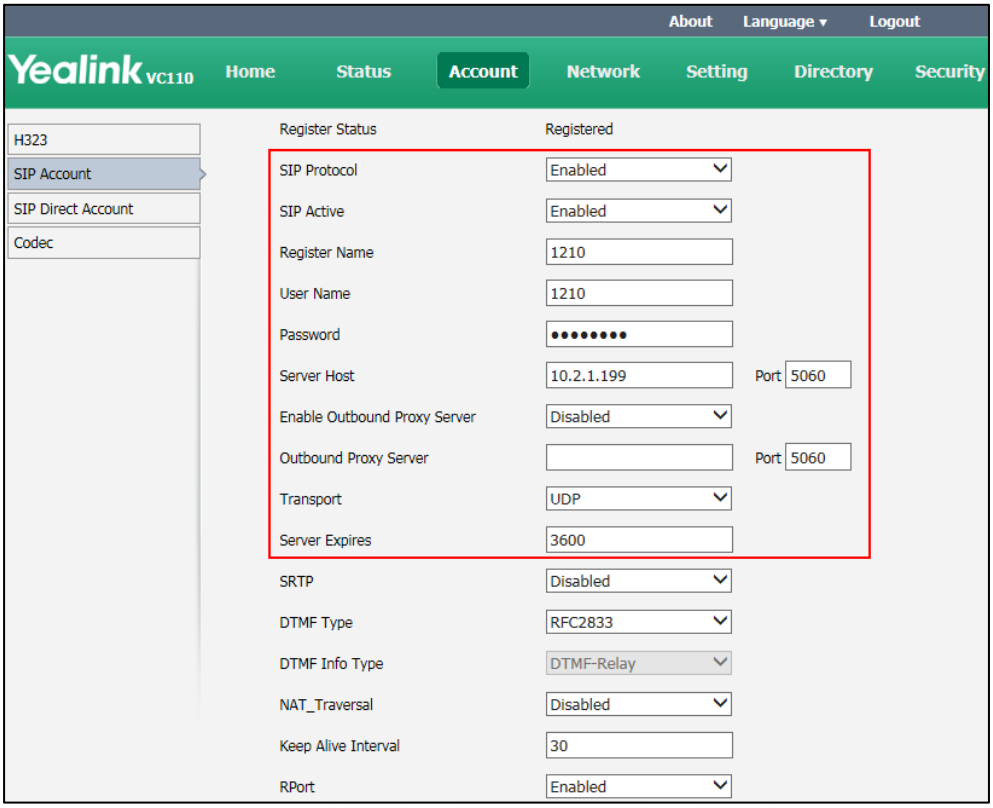
Parameter	Description	Configuration Method
SIP Protocol	Enables or disables the SIP protocol. **Default:** Enabled. **Note**: only when it is set to enabled, can SIP account be	Remote Control Web User Interface

Parameter	Description	Configuration Method
	registered.	
SIP Active	Enables or disables the SIP account. **Default:** Enabled	Remote Control Web User Interface
Register Name	Configures the user name of the SIP account for register authentication. **Default**: Blank	Remote Control Web User Interface
User Name	Specifies the user name to use for authentication when registering with a SIP server. **Default**: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the user name used to authenticate the endpoint to the SIP server. **Default**: Blank	Remote Control Web User Interface
Server Host	Configures the IP address or domain name of the SIP server for the SIP account. **Default**: Blank	Remote Control Web User Interface
Enable Outbound Proxy Server	Enables or disables the endpoint to send requests of the SIP account to the outbound proxy server. **Default:** Disabled	Remote Control Web User Interface
Outbound Proxy Server	Configures the IP address or domain name of the outbound proxy server for the SIP account. **Valid values:** Integer from 1 to 65535. **Default:** it is configurable only when the Outbound Proxy Server is enabled.	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP account. • **UDP**—provides best-effort	Remote Control Web User Interface

Parameter	Description	Configuration Method
	transport via UDP for SIP signaling. • **TCP**—provides reliable transport via TCP for SIP signaling. • **TLS**—provides secure communication of SIP signaling. • **DNS-NAPTR**—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP **Note**: TLS is available only when the endpoint is registered with a SIP server that supports TLS.	
Server Expires	Configures the registration expiration time (in seconds) of the SIP server for SIP account. **Default:**3600s	Remote Control Web User Interface

To configure SIP account via the web user interface:

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



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

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

To configure SIP account via the remote control:

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

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

SIP Direct Account

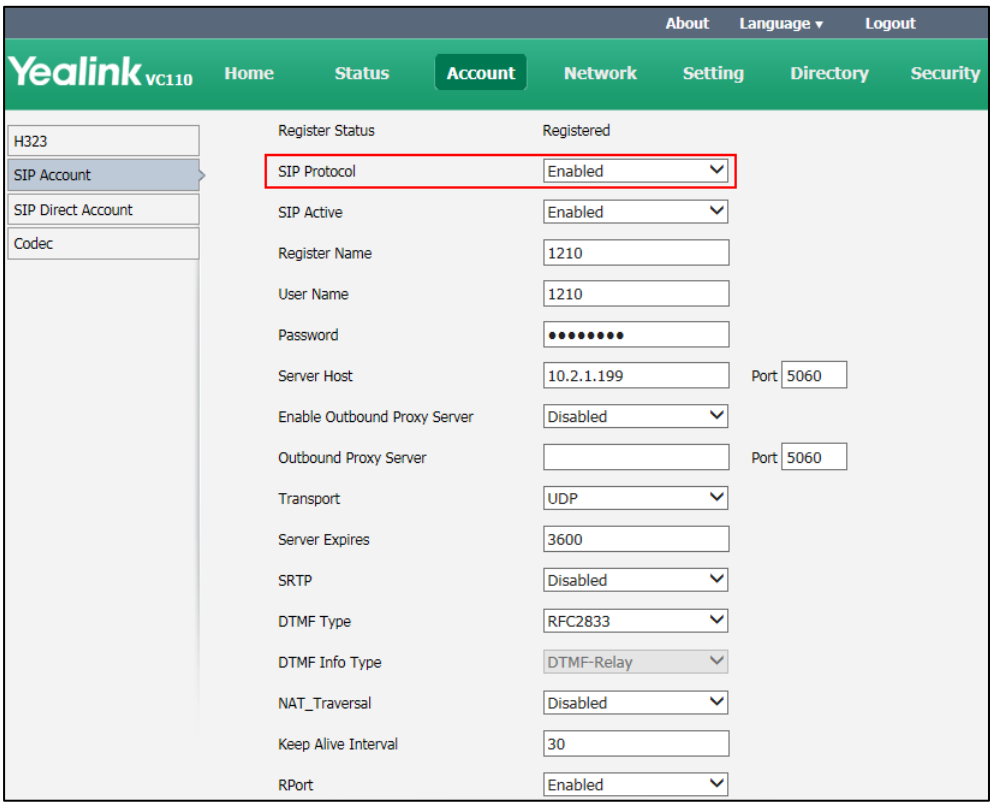
When making an IP call using the SIP protocol, the endpoint doesn't support the TLS protocol. So configuration parameters of SIP direct account are divided from the SIP account. You can configure SIP direct account separately.

SIP direct account parameters on the endpoint are described below:

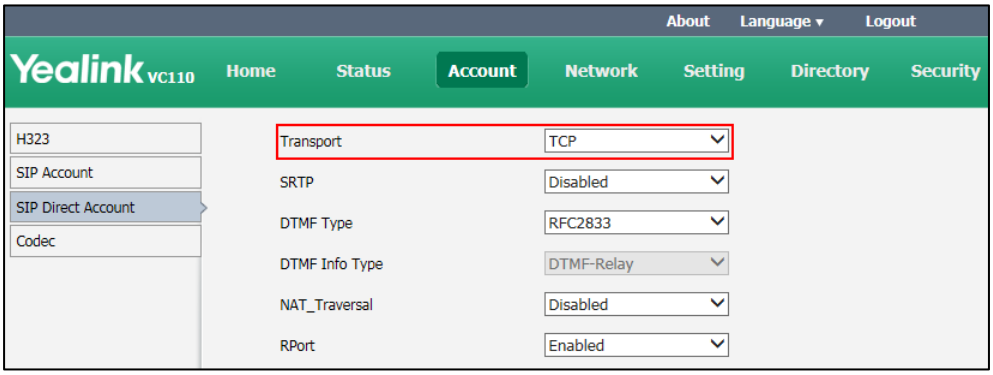
Parameter	Description	Configuration Method
SIP Protocol	Enables or disables the SIP protocol. **Default:** Enabled. **Note:** when it is set to enabled on both sites, the VC110 endpoint can call the far site by dialing IP address directly.	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP direct account. • **UDP**—provides best-effort transport via UDP for SIP signaling. • **TCP**—provides reliable transport via TCP for SIP signaling. • **DNS-NAPTR**—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given.	Remote Control Web User Interface

To configure SIP direct account via the web user interface:

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



3. Click **SIP Direct Account**.
4. Select the desired value from the pull-down list of **Transport**.



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

To configure SIP direct account via the remote control:

1. Select **Menu->Advanced** (default password: 0000) **->SIP Account**.
2. Mark the **On** radio box in the **SIP Protocol** field.
3. Press the **Save** soft key to accept the change.
4. Press the **Back** soft key to return to the Advanced menu.

5. Select **SIP Direct Call**, and then press OK.
6. Select the desired value from the pull-down list of **Transport**.
7. Press the **Save** soft key to accept the change.

Configuring H.323 Settings

Yealink VC110 video conferencing endpoints support H.323 protocol. If your network uses a gatekeeper, you can register an H.323 account for the endpoint, and specify its H.323 name and extension. This allows others to call the endpoint by entering the H.323 name or extension instead of the IP address.

H.323 settings parameters on the endpoint are described below:

Parameter	Description	Configuration Method
H.323 Protocol	Enables or disables the H.323 protocol. **Default:** Enabled. **Note:** only when it is set to enabled, can H.323 account be registered. When it is set to enabled on both sites, the VC110 endpoint can call the far site by dialing IP address directly.	Remote Control Web User Interface
H.323 Active	Enables or disables the H.323 account. **Default:** Enabled If it is set to disabled, the endpoint cannot place or receive calls with the H.323 protocol.	Remote Control Web User Interface
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this endpoint. You can make point-to-point calls using H.323 names if both endpoints are registered to a gatekeeper. **Default**: Blank	Remote Control Web User Interface
H.323 Extension	Specifies the extension that gatekeepers and gateways use	Remote Control Web User Interface

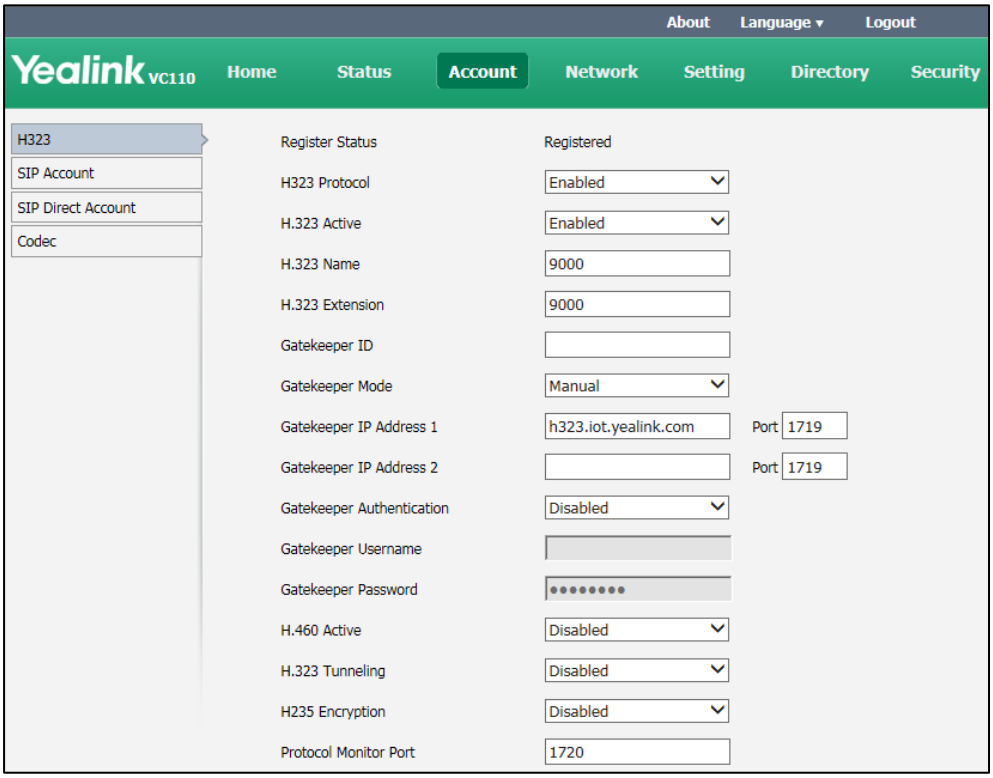
Parameter	Description	Configuration Method
	to identify this endpoint. **Default**: Blank **Note:** Users can place point-to-point calls using the extension if both endpoints are registered with a gatekeeper,	
Gatekeeper ID	Configures the gatekeeper ID. **Note:** This is set only when required by the gatekeeper. For example, for configurations with multiple gatekeepers. The gatekeeper ID must match the one configured on the gatekeeper. Do not configure this parameter if the gatekeeper does not require it, as this may result in failure to register with the gatekeeper.	Remote Control Web User Interface
Gatekeeper Mode	Configures the gatekeeper mode. • **Disabled**—the endpoint does not use a gatekeeper. • **Auto**—the endpoint automatically discovers a gatekeeper. • **Manual**—specify the IP address and port for the gatekeeper manually. **Default:** Disabled	Remote Control Web User Interface
Gatekeeper IP Address 1	Configures the IP address of the primary gatekeeper.	Remote Control Web User Interface
Gatekeeper IP Address 2	Configures the IP address of the secondary gatekeeper.	Remote Control Web User Interface
Gatekeeper Authentication	Enables or disables support for gatekeeper authentication. **Default:** Disabled **Note:** When Gatekeeper	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Authentication is enabled, the gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper.	
Gatekeeper Username	Specifies the user name for authentication with gatekeeper. **Default**: Blank	Remote Control Web User Interface
Gatekeeper Password	Specifies the password for authentication with gatekeeper. **Default**: Blank	Remote Control Web User Interface
H.460 Active	Enables or disables H.460 firewall traversal feature on the endpoint. **Default:** Disabled For more information, refer to H.460 Firewall Traversal on page 88.	Remote Control Web User Interface
H.323 Tunneling	Enables or disables the H.323 tunneling on the endpoint. **Default:** Disabled For more information, refer to H.323 Tunneling on page 71.	Remote Control Web User Interface
H235 Encryption	Specifies the H.235 type for the H.323 account. • **Disabled**—do not use H.235 in H.235 calls. • **Enabled**—negotiate with the far site whether to use H.235 for media encryption in H.323 calls. • **Compulsory**—compulsory use H.235 for media encryption in H.323 calls. **Default:** Disabled For more information, refer to	Web User Interface

Parameter	Description	Configuration Method
	H.235 on page 188.	
Protocol Monitor Port	Specifies the port for the H.323 protocol. **Default** 1720. **Note:** It is only applicable to IP direct call.	Web User Interface

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

1. Click on **Account**->**H323**.
2. Configure the H.323 account settings.



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

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

To configure H.323 account via the remote control:

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

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

DTMF

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

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

DTMF Keypad Frequencies:

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

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

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

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

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The payload type for RTP Event packets is configurable. IP phones default to 101 for the payload type, which use the definition to negotiate with the other end during call establishment.

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

INBAND

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

SIP INFO

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

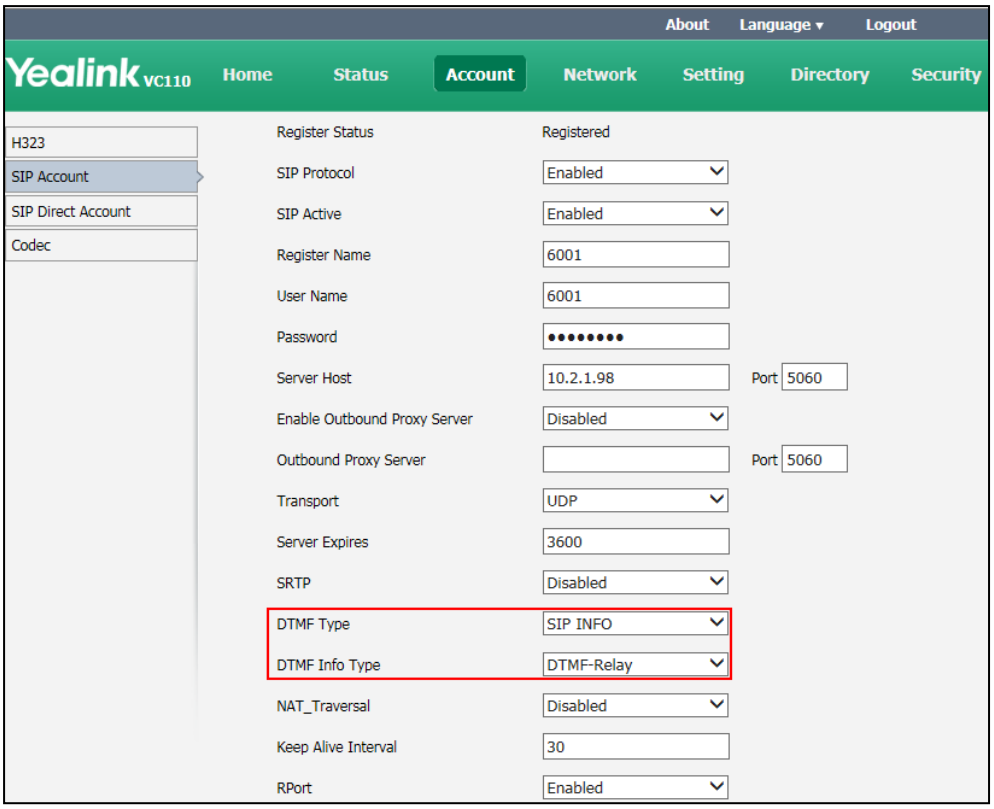
DTMF parameters on the endpoint are described below:

Parameter	Description	Configuration Method
DTMF Type	Configures the DTMF type. You can configure it for the SIP account or SIP direct account separately. • **INBAND**—DTMF digits are transmitted in the voice band. • **RFC2833**—DTMF digits are transmitted by RTP Events compliant to RFC 2833. • **SIP INFO**—DTMF digits are transmitted by the SIP INFO messages. **Default:** INBAND	Remote Control Web User Interface
DTMF Info Type	Configures the DTMF info type when DTMF type is set to SIP INFO. You can configure it for the SIP account or SIP direct account separately. • **DTMF-Relay** • **DTMF** • **Telephone-Event** **Default:** DTMT-Relay	Remote Control Web User Interface

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

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

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

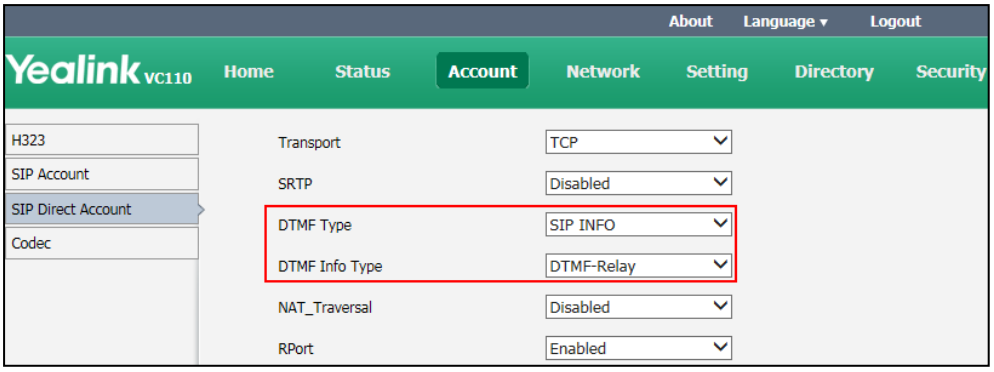


3. Click **Confirm** to accept the change.

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

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

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



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

Codecs

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

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

The following table summarizes the supported codecs on the endpoint:

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

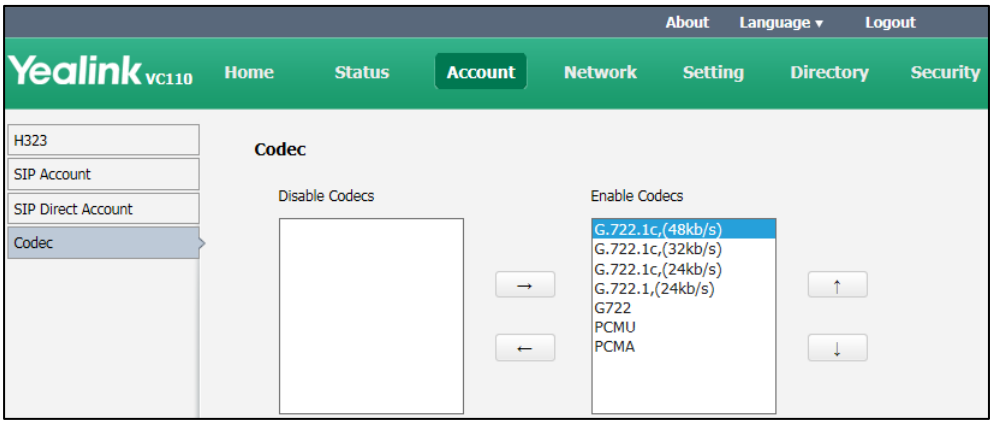
Codecs parameters on the endpoint are described below:

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

To configure codecs via the web user interface:

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

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



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

Call Type

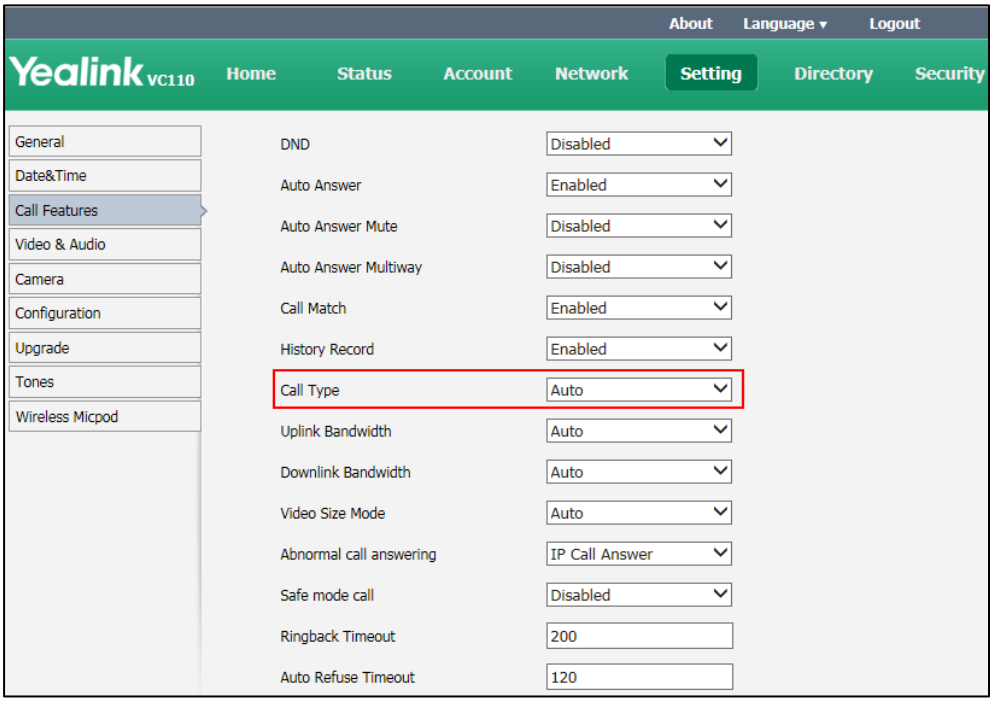
The endpoint supports SIP and H.323 protocols for incoming and outgoing calls. H.323 is commonly used to communicate to other video conferencing endpoints. SIP is commonly used to communicate with other VoIP devices. The default call type on the endpoint is Auto, and the endpoint preferentially uses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

The call type parameter on the endpoint is described below:

Parameter	Description	Configuration Method
Call Type	Specifies the desired call type for placing calls. • **Auto**—the endpoint automatically uses the available call type. • **SIP**—the endpoint uses the SIP protocol for placing calls. • **H.323**—the endpoint uses H.323 protocol for placing calls. **Default:** Auto	Remote Control Web User Interface

To configure call type via the web user interface:

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



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

To configure call type via the remote control:

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

Do Not Disturb

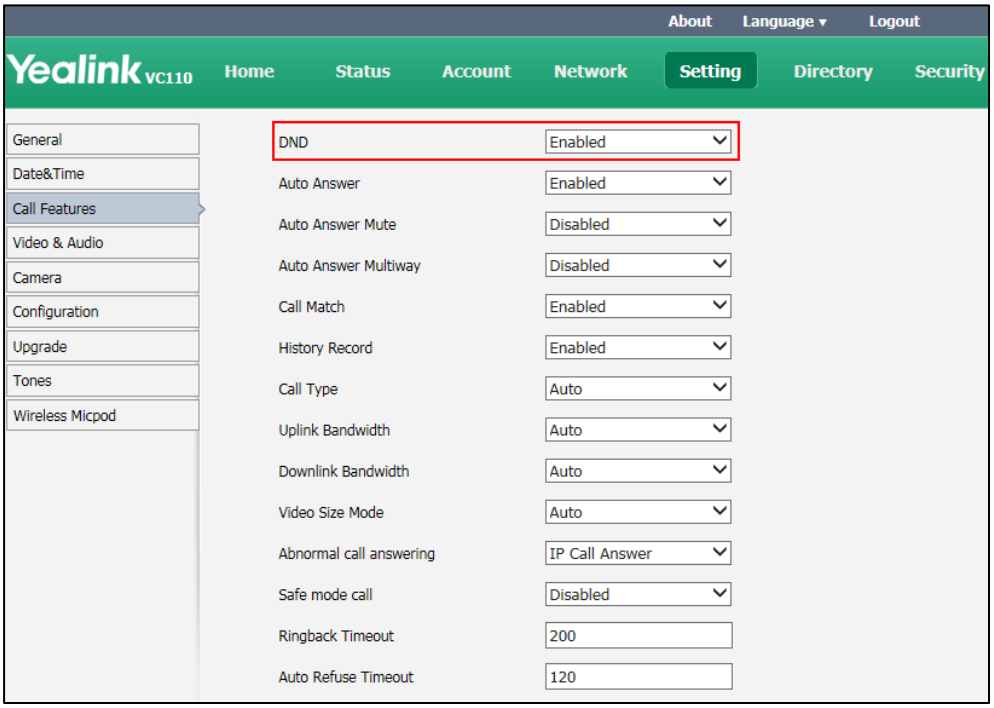
Do not Disturb allows the endpoint to reject all incoming calls automatically. You can activate the DND mode for the endpoint when it is idle, and the DND mode will be deactivated after the endpoint places a call. You can also activate the DND mode for the endpoint during a call, and the DND mode will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

The DND parameter on the endpoint is described below:

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

To configure DND via the web user interface:

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



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

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

To configure DND via the remote control:

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

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

To configure DND during a call via the web user interface:

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

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

To configure DND during a call via the remote control:

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

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

Auto Answer

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

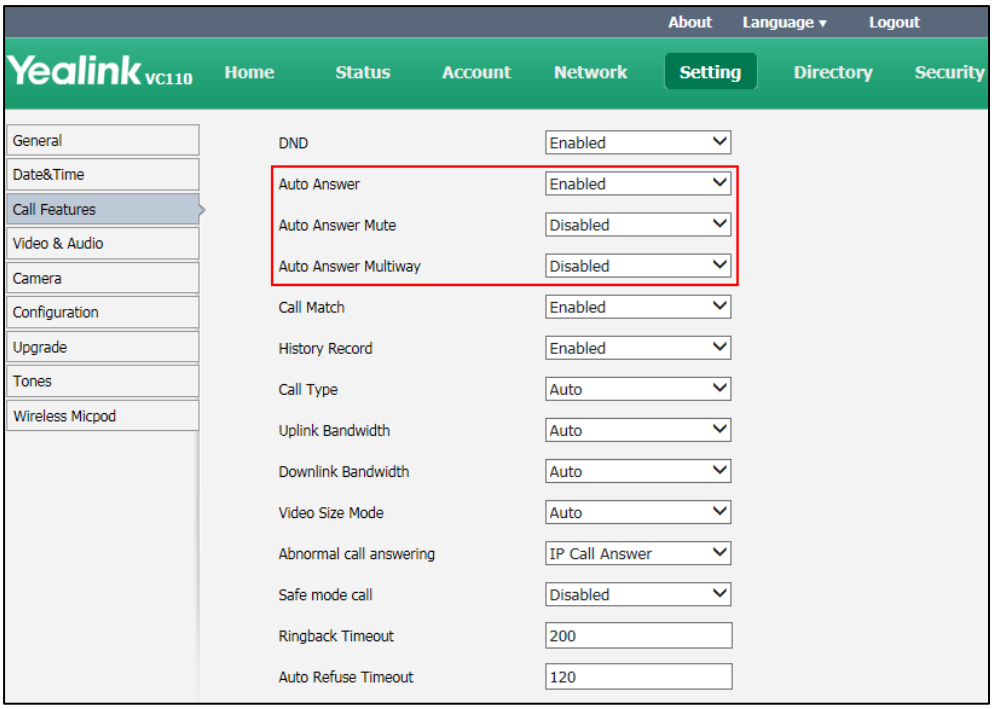
Auto answer parameters on the endpoint are described below:

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

To configure auto answer via the web user interface:

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

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



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

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

To configure auto answer via the remote control:

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

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

Call Match

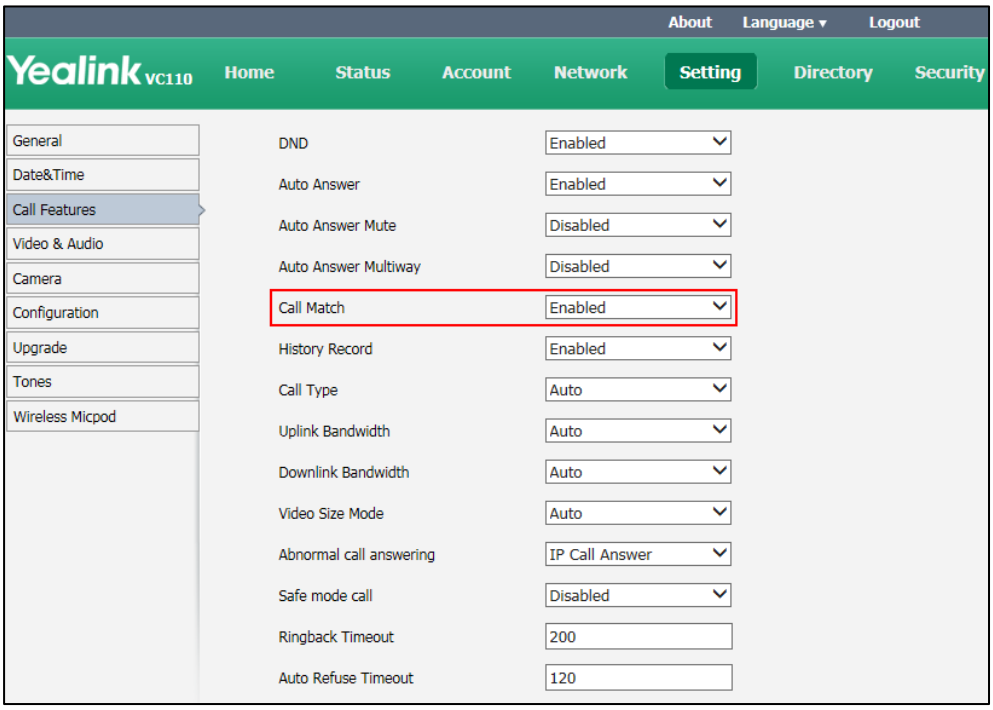
The call match feature allows the endpoint to search entries automatically from the search source list based on the entered string. Once matched, the results will be displayed on the screen. If no list is added to the search source list, the endpoint will not perform a search even if call match is enabled. For more information on how to search source list in dialing, refer to Search Source List in Dialing on page 168 .

Parameter of call match on the endpoint is described below:

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

To configure call match via the web user interface:

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



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

To configure call match via the remote control:

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

History Record

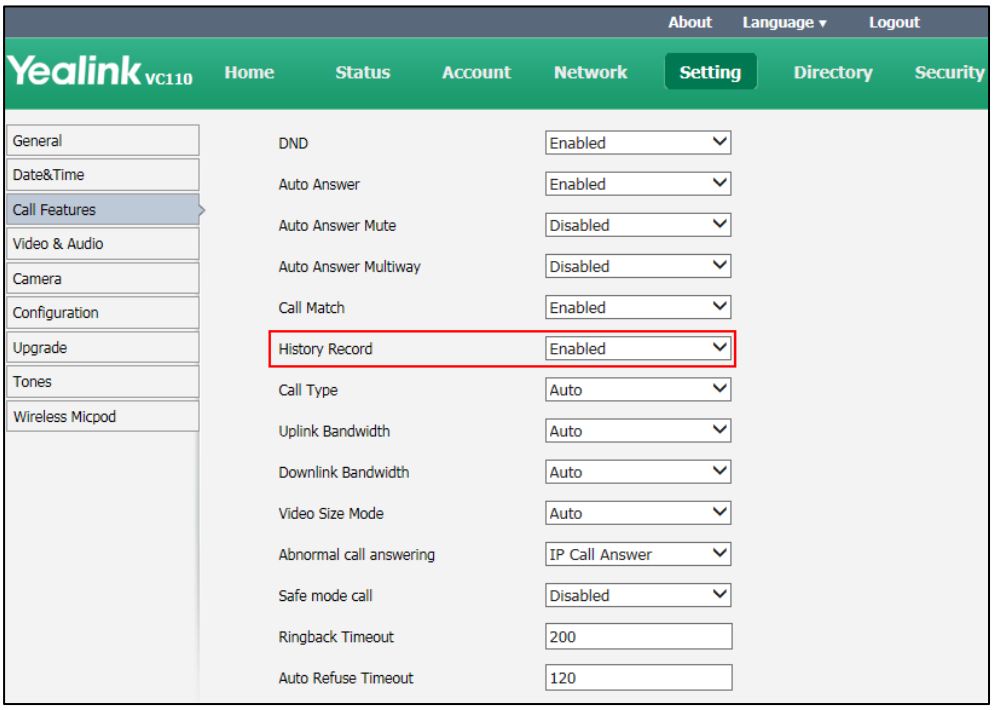
The endpoint maintains a local call history, which contains call information such as remote party identification, time and date, and call duration (call duration is only listed on the web user interface). Users can manage call history list via the remote control, web user interface and VCP40 phone. To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

The history record parameter on the endpoint is described below:

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

To configure history record via the web user interface:

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



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

To configure history record via the remote control:

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

Bandwidth

The endpoint automatically detects the available bandwidth for call connection by default. The VC110 supports connecting to other devices with different bandwidth. If a device with lower bandwidth joins a call, the video quality will stay the same or will not reduce a lot. You can specify the uplink and downlink bandwidths for the endpoint to achieve the best result. Uplink bandwidth is the max bandwidth of outgoing calls. And downlink bandwidth is the max bandwidth of incoming calls. The configurable

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

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

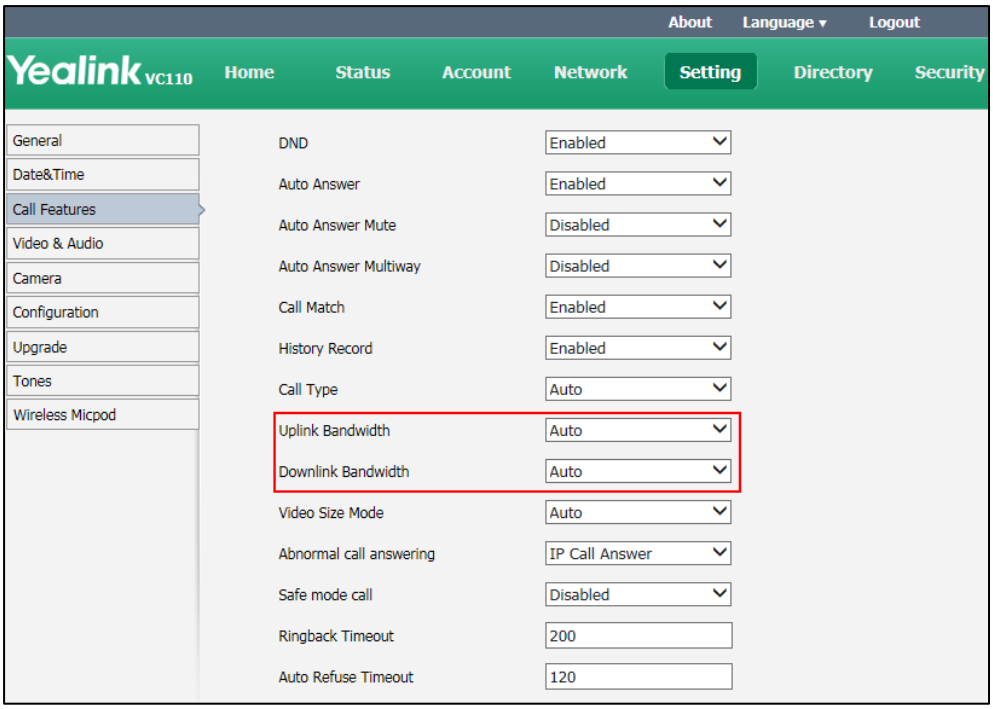
Bandwidth settings parameters on the endpoint are described below:

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

To configure bandwidth via the web user interface:

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

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



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

To configure bandwidth via the remote control:

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

Video Size Mode

You can configure video size mode for the VC110 video conferencing endpoint according to current network environment.

The video size mode parameters on the endpoint are described below:

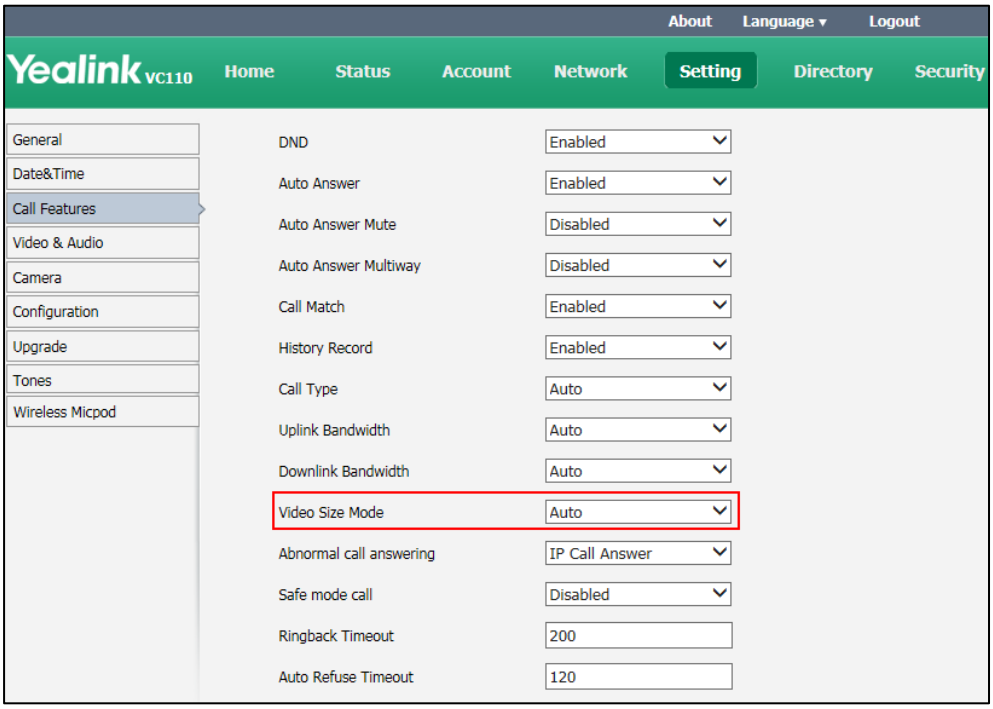
Parameter	Description	Configuration Method
Auto	Selects the video size mode automatically. If the other party is Yealink endpoint, then the endpoint will send and receive 1080p30 video. If the other party is not Yealink endpoint, then the endpoint will send and receive 720p30 video.	Remote Control Web User Interface

Parameter	Description	Configuration Method
1080P	No matter what device the other party is, the endpoint will send and receive 1080p30 video forcibly. **Note**: If it is selected, the endpoint cannot share content during a call with non-Yealink device.	Remote Control Web User Interface
720P	No matter what device the other party is, the endpoint will send and receive 720p30 video forcibly.	Remote Control Web User Interface

Yealink VC110 can adjust the video resolution automatically. When the video stream (For example: sharing content or recording) increases, the video resolution will decrease automatically. When the video stream decreases, the video resolution will increase automatically.

To configure video size mode via the web user interface:

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



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

Ringback Timeout

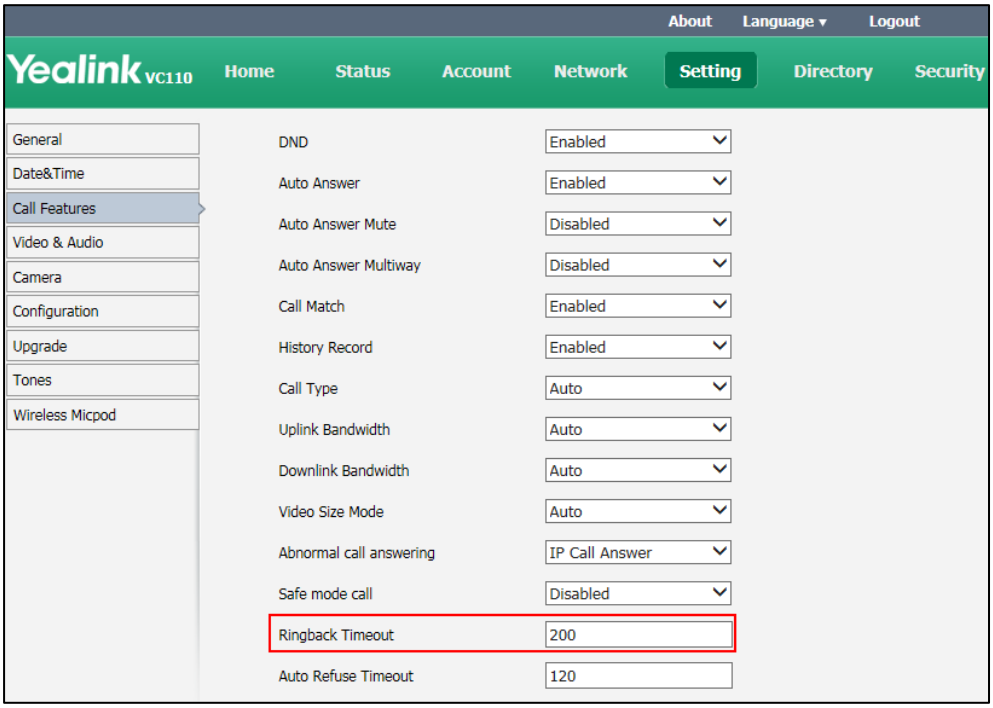
Ringback timeout defines a specific period of time within which the VC110 video conferencing endpoint will cancel the dialing if the call is not answered.

The ringback timeout parameter on the endpoint is described below:

Parameter	Description	Configuration Method
Ringback Timeout	Configures the duration time (in seconds) in the ringback state. **Default:** 200 If it is set to 200, the endpoint will cancel the dialing if the call is not answered within 200s.	Web User Interface

To configure ringback timeout via the web user interface:

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



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

Auto Refuse Timeout

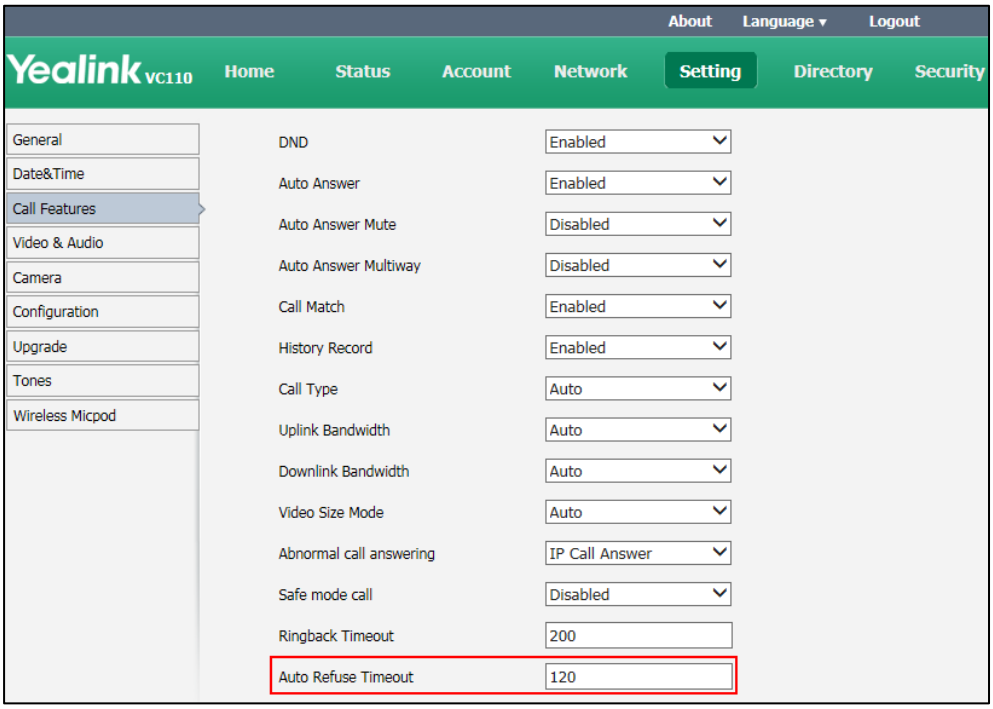
Auto refuse timeout defines a specific period of time within which the video conferencing endpoint will stop ringing if the call is not answered.

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

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

To configure auto refuse timeout via the web user interface:

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



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

Configuring Endpoint Settings

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

Topics include:

- General Settings
- Audio Settings
- Adjusting MTU of Video Packets
- Dual-Stream Protocol
- Mix Sending
- Configuring Camera Settings
- Far-end Camera Control
- Camera Control Protocol
- Tones

General Settings

Site Name

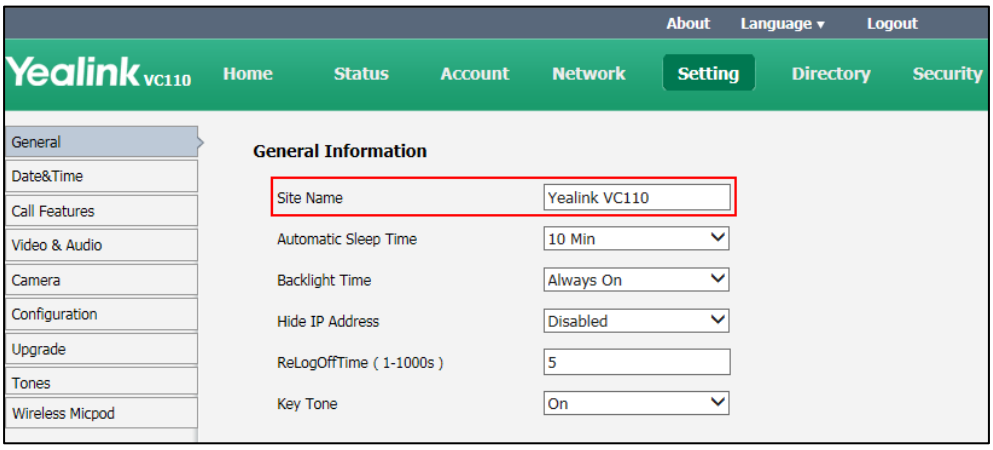
When the endpoint is idle, the site name is displayed on the status bar of display device and VCP40 phone. When H.323 or SIP protocol is enabled, you can make an IP address call to the far site, the site name will be displayed on the display device of the far site. Site name can consist of letters, numbers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

The site name parameter is described below:

Parameter	Description	Configuration Method
Site Name	Configures the site name of the endpoint. **Valid values:** String within 64 characters **Default:** Yealink VC110	Remote Control Web User Interface

To configure the site name via the web user interface:

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



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

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

To configure the site name via the remote control:

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

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

Backlight of the VCP40 Video Conferencing Phone

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

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

- **Always On:** Backlight is turned on permanently.
- **15 s, 30 s, 10 min, 20 min, 30 min, 1 Hour, 2 Hour, 3 Hour, 4 Hour:** Backlight is turned off when the phone is inactive after a preset period of time. It is automatically turned on if the status of the phone changes or any key is pressed.

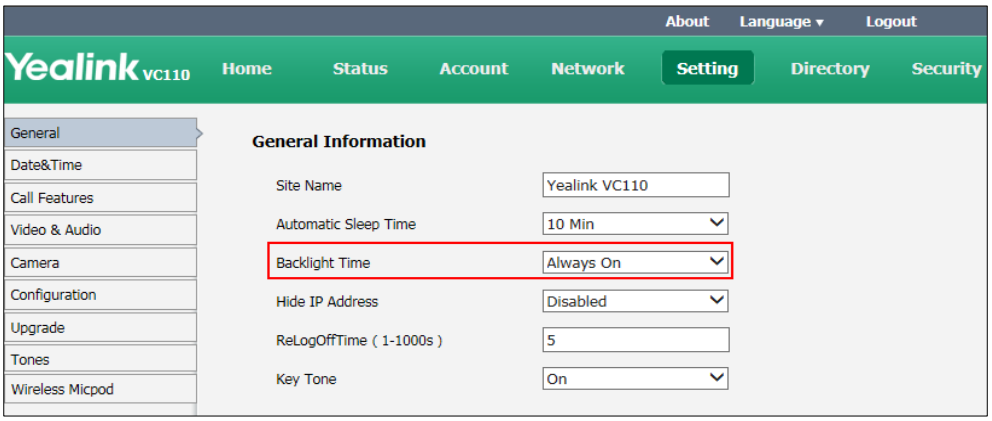
The backlight parameter on VCP40 phone is described below:

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

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

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

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



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

Language

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

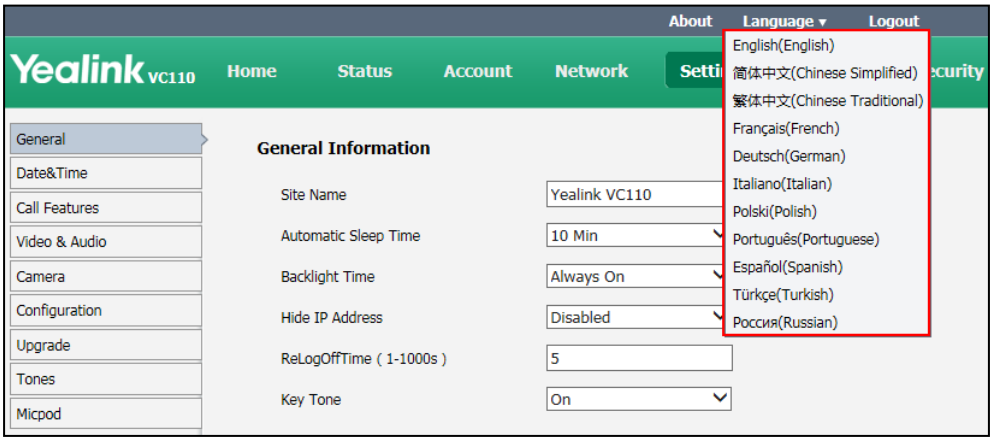
The default language of the web user interface is English. You can change the language of the web user interface via the web user interface. The available languages for endpoint are English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish and Russian.

The language parameters on the endpoint are described below:

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

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

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



To specify the language for the display device and the VCP40 phone via the remote control:

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

Date & Time

Time and date are displayed on the idle screen of the display device and the VCP40 phone. Time and date are synced automatically from the NTP server by default. The default NTP server is cn.pool.ntp.org. The NTP server is configurable manually or obtained by DHCP via DHCP Option 42. The phone will use the NTP server obtained by DHCP preferentially. If the endpoint cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date can use one of several different formats.

Time Zone

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

Daylight Saving Time

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summertime so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn.

Many countries have used DST at various times, details vary by location. DST can be adjusted automatically from the time zone configuration. Typically, there is no need to change this setting.

DST parameters are described below:

Parameter	Description	Configuration Method
DHCP Time	Enables or disables the endpoint to update time with the offset time obtained from the DHCP server. **Default:** Disabled **Note:** it is only available to GMT 0.	Web User Interface
Time Zone	Configures the time zone. **Default:** +8 China (Beijing)	Remote Control Web User Interface
Primary Server/NTP Primary Server	Configures the primary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Secondary Server/NTP Secondary Server	Configures the secondary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Synchronism (15~86400s)	Configures the interval (in minutes) for the endpoint to synchronize time and date with NTP server. **Default**: 1000.	Web User Interface
Daylight Saving Time	Configures the Daylight Saving Time (DST) type. The available types for the endpoint are: • **Disabled**-not use DST. • **Enabled**-use DST. You can manually configure the start time, end time and offset according to your needs. • **Automatic**-use DST. DST will be configured	Remote Control Web User Interface

Parameter	Description	Configuration Method
	automatically. You do not need to manually configure the start time, end time and offset. **Default:** Automatic	
Fixed Type	Configures the DST calculation methods. • **By Date**- specifies the month, day and hour to be the DST start /end date. • **By Week**- specifies the month, week, day and hour the DST start /end date. **Note:** It only works if the value of Daylight Saving Time is set to Enabled.	Web User Interface
Start Date	When the DST calculation method is set to **By Date**. Configures the time to start DST. **Note:** It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
End Date	When the DST calculation method is set to **By Date**. Configures the time to end DST. **Note:** It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Start Month **DST Start Day of Week** **DST Start Day of Week Last in Month**	When the DST calculation method is set to **By Week**. Configures the time to start DST. **Note**: It only works if the value	Web User Interface

Parameter	Description	Configuration Method
Start Hour of Day	of the Daylight Saving Time is set to Enabled.	
DST Stop Month **DST Stop Day of Week** **DST Stop Day of Week Last in Month** **End Hour of Day**	When the DST calculation method is set to **By Week**, Configures the time to end DST. **Note**: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
Offset(minutes)	Configures the DST offset time (in minutes). **Valid values**: -300 to +300. **Note**: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
Time Type	Configures the DST time type. • **SNTP:** obtain the time and date from the NTP server automatically. • **Manual Time:** configure the time and date manually. **Default:** SNTP	Remote Control Web User Interface
Time Format/ Time	Configures the time format. • Hour12 • Hour24 **Default:** Hour 24	Remote Control Web User Interface
Date Format/Date	Configures the date format. • 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	Remote Control Web User Interface

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

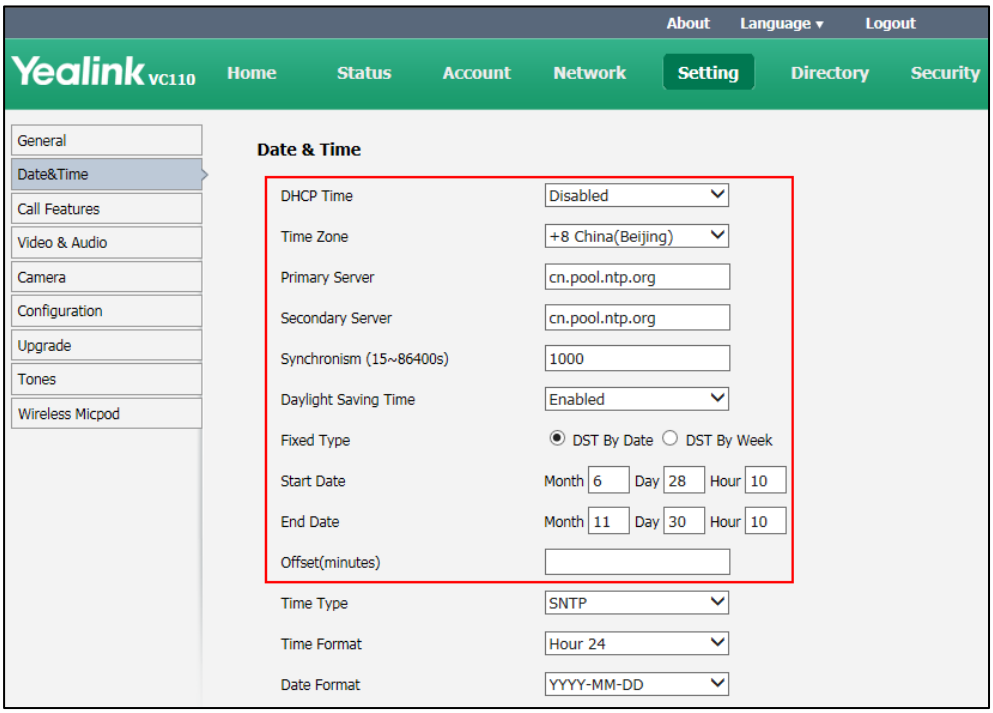
1. Click on **Setting->Time & Date**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter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

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

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

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

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

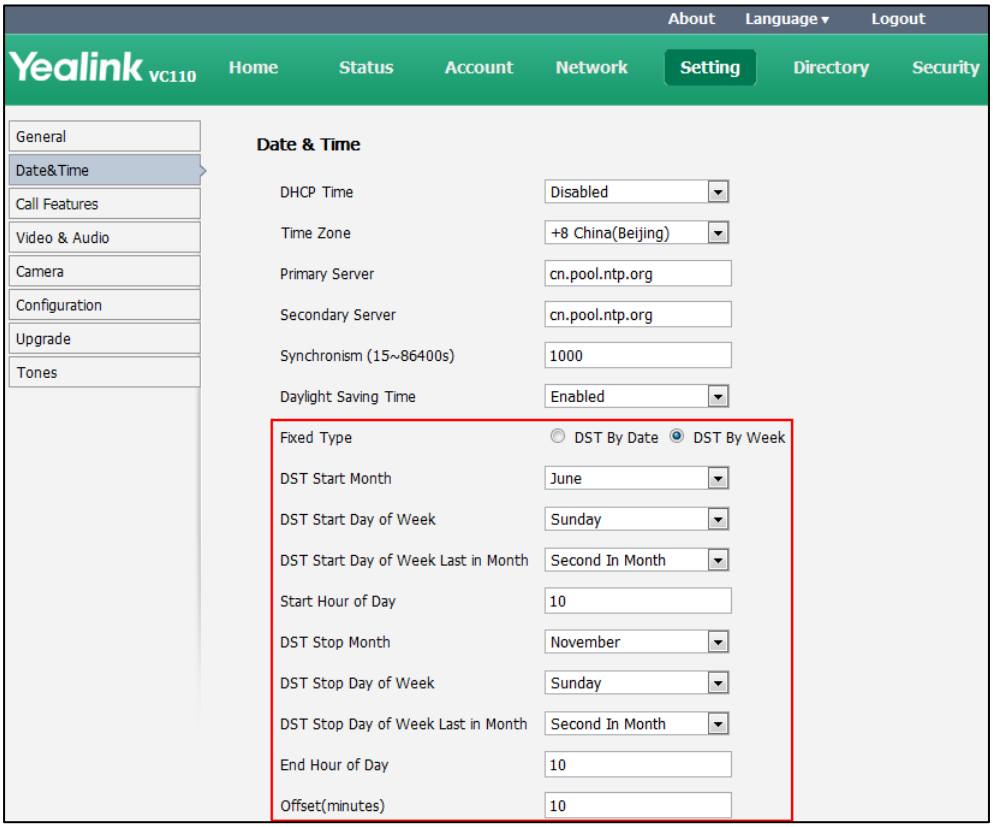


   - Mark the **DST By Week** radio box in the **Fixed Type** field.

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

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

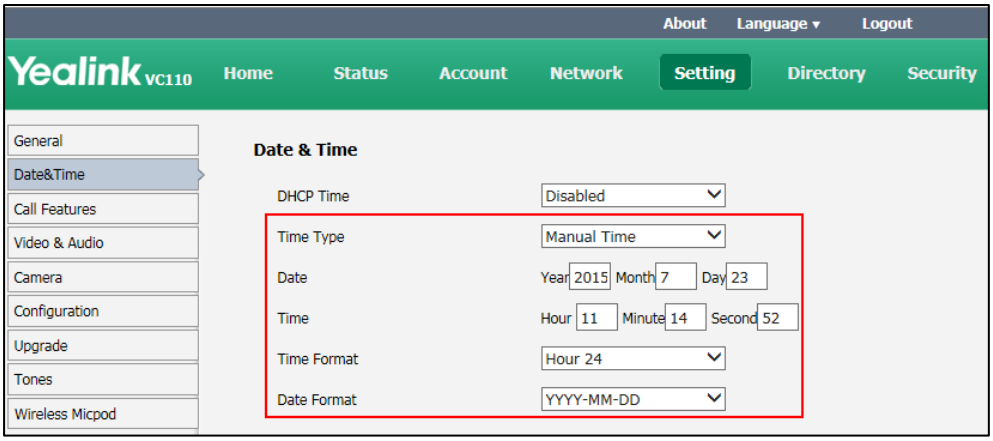
Enter the desired time in the **End Hour of Day** field.



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

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

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



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

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

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

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

Automatic Sleep Time

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

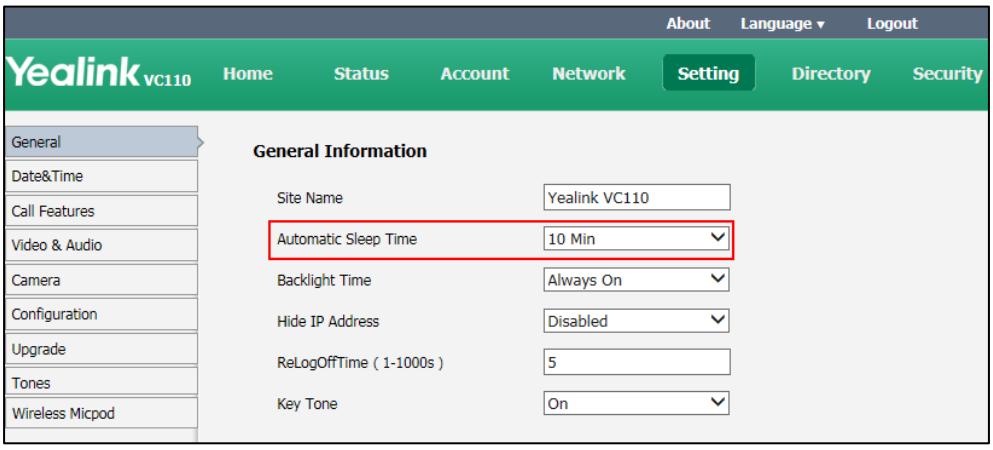
You can change the automatic sleep time via the remote control or web user interface. You can also press the sleep key on the remote control to make the endpoint sleep immediately.

The automatic sleep time is described below:

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

To configure the automatic sleep time via the web user interface:

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



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

To configure the automatic sleep time via the remote control:

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

Hide IP Address

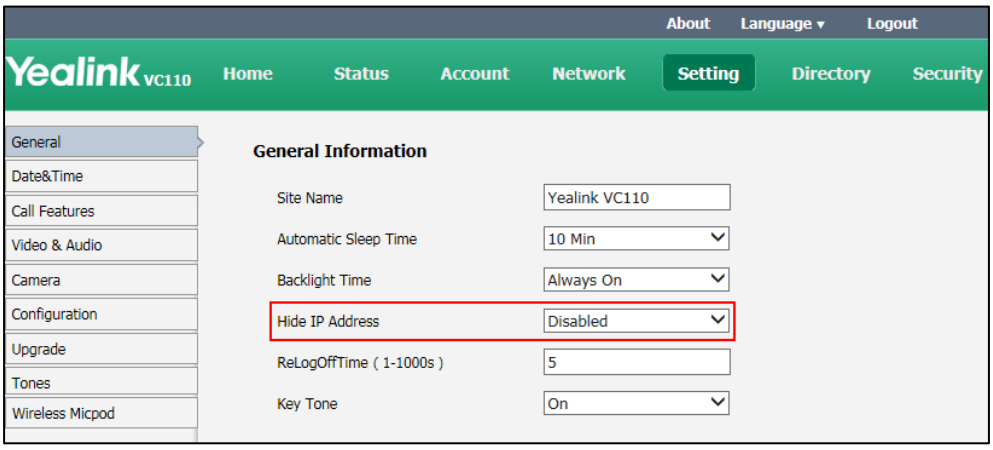
When the endpoint is idle, the display device displays shortcut keys and the status bar. The status bar displays time and date, site name, IP address, SIP and H.323 account (when SIP and H.323 account are registered). You can hide the endpoint IP address.

The hide IP address parameter is described below:

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

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

1. Click on **Setting->General**.
2. Select **Enabled** from the pull-down list of **Hide IP Address**.



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

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

Relog Offtime

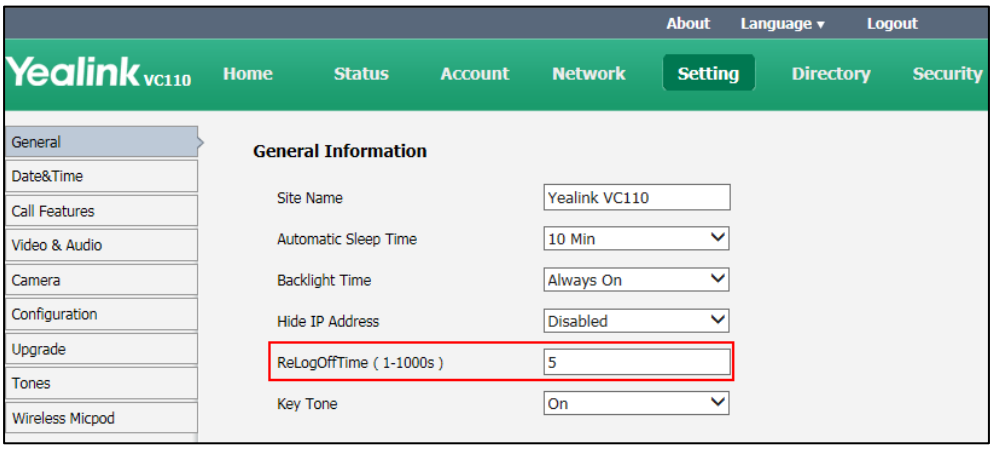
The endpoint will log out of the web user interface automatically after being inactive for a period of time (default: 5 minutes). You need to re-enter the user name and password to login. You can only configure the relog offtime via the web user interface.

The relog offtime parameter is described below:

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

To configure the relog offtime via the web user interface:

1. Click on **Setting->General**.
2. Enter the desired time in the **ReLogOffTime** field.



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

Key Tone

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

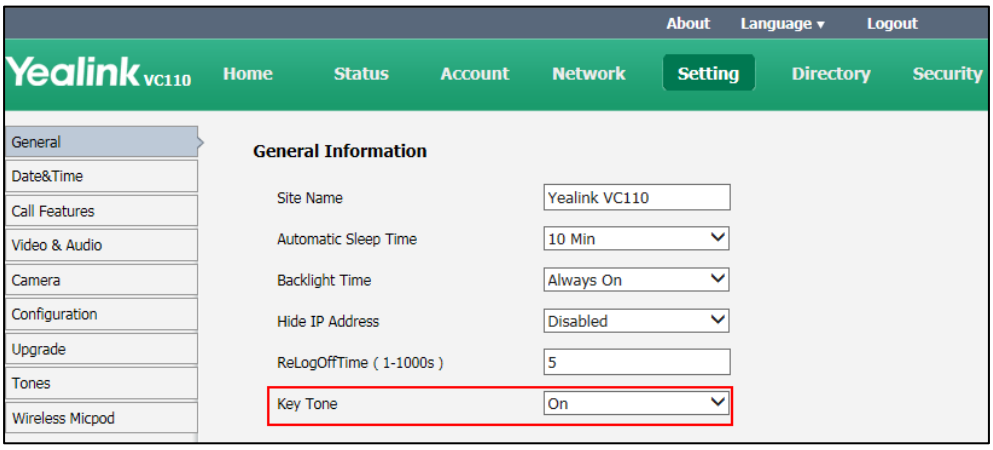
Key tone is configurable via the remote control or web user interface.

The key tone parameter is described below:

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

To configure the key tone via the web user interface:

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



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

To configure the key tone via the remote control:

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

Audio Settings

Audio Output Device

The endpoint supports the following audio output devices:

- **Auto**
- **VCS Phone**
- **HDMI**
- **Line Output**

By default, the endpoint automatically selects the audio output devices with highest priority. The priority is: VCS Phone> HDMI>Line Output. If the audio output device with highest priority is removed from the VC110, the VC110 will select the next highest priority device.

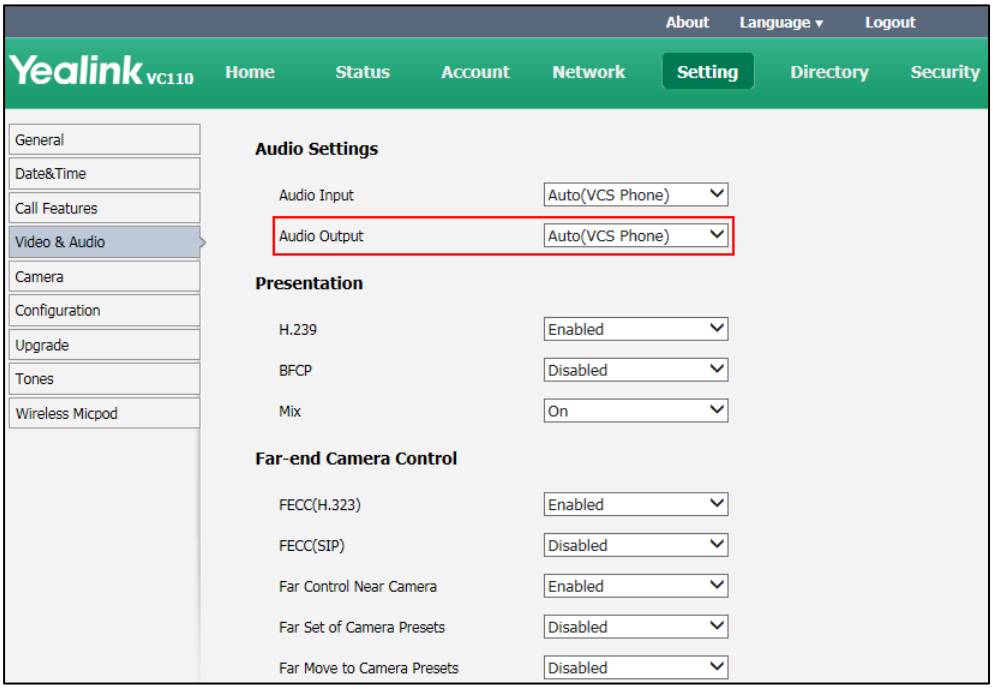
You can also specify the desired audio output device via the remote control or the web user interface.

The audio output device parameter is described below:

Parameter	Description	Configuration Method
Audio Output	Specifies the audio output device for the endpoint. **Valid values:** • **Auto** - selects the audio output device with higher priority. • **HDMI** - selects the built-in speakerphone of the display device. • **Line Output** - selects the speakerphone connected to the Line Out port on the VC110 all-in-one unit. • **VCS Phone** - selects the VCP40 phone. **Default:** Auto. If **VCS Phone** is selected as the audio output device manually or automatically, the audio input device must be **VCS Phone** or **Line In+VCS Phone**.	Remote Control Web User Interface

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

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



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

To configure the audio output device via the remote control:

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

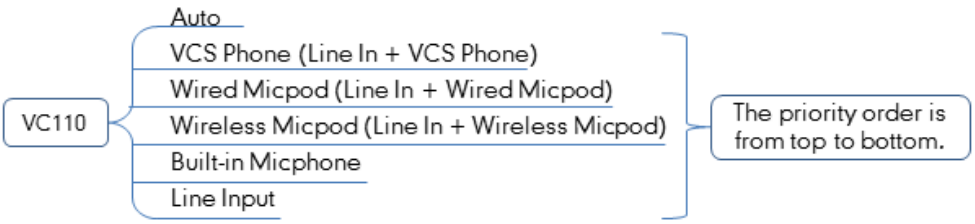
Audio Input Device

The endpoint supports the following audio input devices:

- **Auto** (select the audio input device with highest priority)
- **VCS Phone** (VCP40 phone)
- **Wired Micpod** (VCM30)
- **Wireless Micpod** (VCM60)
- **Built-in Micphone** (built-in micphone of VC110)
- **Line Input** (microphone connected to the Line In port on the VC110 all-in-one unit)
- **Line In + VCS Phone**
- **Line In + Wired Micpod**
- **Line In + Wireless Micpod**

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

The priority of audio input device is:



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

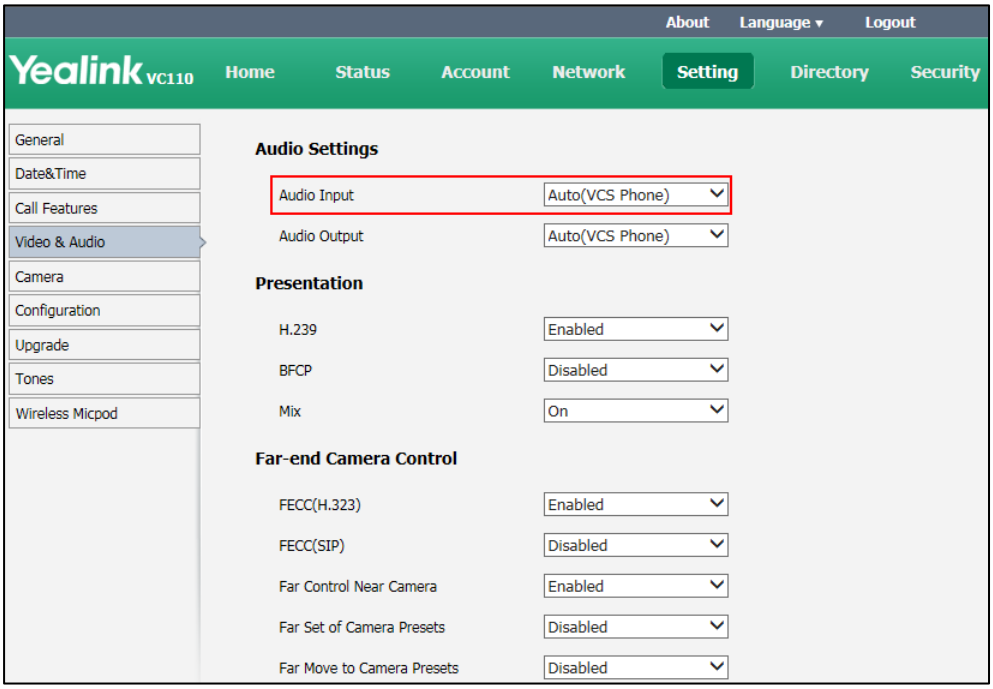
The audio input device parameter is described below:

Parameter	Description	Configuration Method
Audio Input	Specifies the audio input device for the endpoint. **Valid values:** • **Auto**- selects the audio input device with highest priority. • **VCS Phone**- selects the VCP40 phone. • **Wired Micpod**- selects the VCM30 video conferencing microphone array • **Wireless Micpod** -selects the VCM60 video conferencing wireless microphone. • **Built-in Microhone**-selects the vc110 built-in microphone. • **Line Input**- selects the microphone connected to the Line In port on the VC110 all-in-one unit. • **Line In +VCS Phone**- selects microphone connected to the Line In port on the VC110 all-in-one unit and VCP40 phone. • **Line In + Wired Micpod** -	Remote Control Web User Interface

Parameter	Description	Configuration Method
	selects microphone connected to the Line In port on the VC110 all-in-one unit and VCM30 video conferencing microphone array. • **Line In + Wireless Micpod**- selects the microphone connected to the Line In port on the VC110 all-in-one unit and VCM60 video conferencing wireless microphone. **Default:** Auto. If "Line Input" is selected as the audio input device, the near end will not play sound from the Line Input device. If "Line Input" is selected as an auxiliary audio input, which means that "Line In + Other device" is selected as the audio input device, the near end will play sound from the Line Input device. (For example: during a video training for main office and branch office, both offices need to hear the video sound).	

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

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



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

To configure the audio input device via the remote control:

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

Adjusting MTU of Video Packets

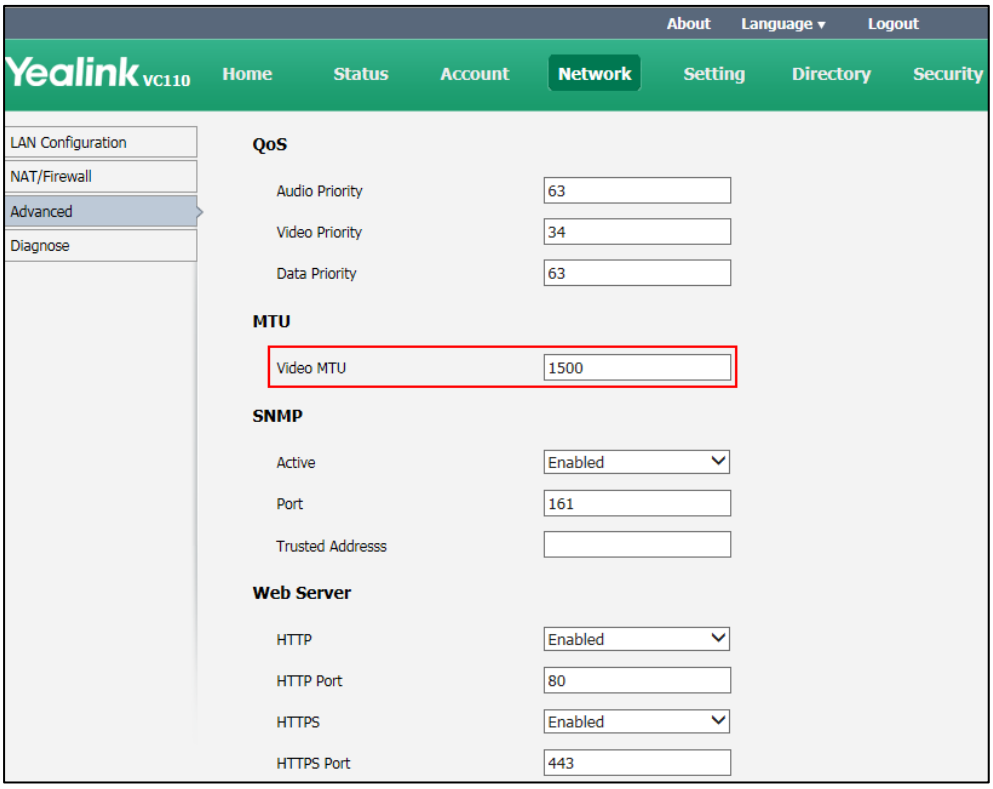
Video packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped. This results in poor quality video at the receiving device. You can set the maximum MTU size of the video packets sent by the endpoint. The default value is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

The MTU parameter on the endpoint is described below.

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

To configure MTU via the web user interface:

1. Click on **Network->Advanced**.
2. In the **MTU** block, enter the desired value in the **Video MTU** field.



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

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

To configure MTU via the remote control:

1. Select **Menu->Advanced** (default password: 0000) **->Advanced Network**.

2. Enter the desired value in the **Video MTU(1000-1500)** field.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the endpoint immediately.

Dual-Stream Protocol

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

The Yealink video conferencing endpoint supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol). H.239 protocol is used when sharing content with the far site in H.323 calls. BFCP protocol is used when sharing content with the far site in SIP calls. Before enabling the desired protocol, ensure that the protocol is supported and enabled by the far site you wish to call. If the far site does not support the protocol for sharing content, MCU will automatically mix the content and camera video, and send them in one channel. For more information on mix sending, refer to Mix Sending on page 146.

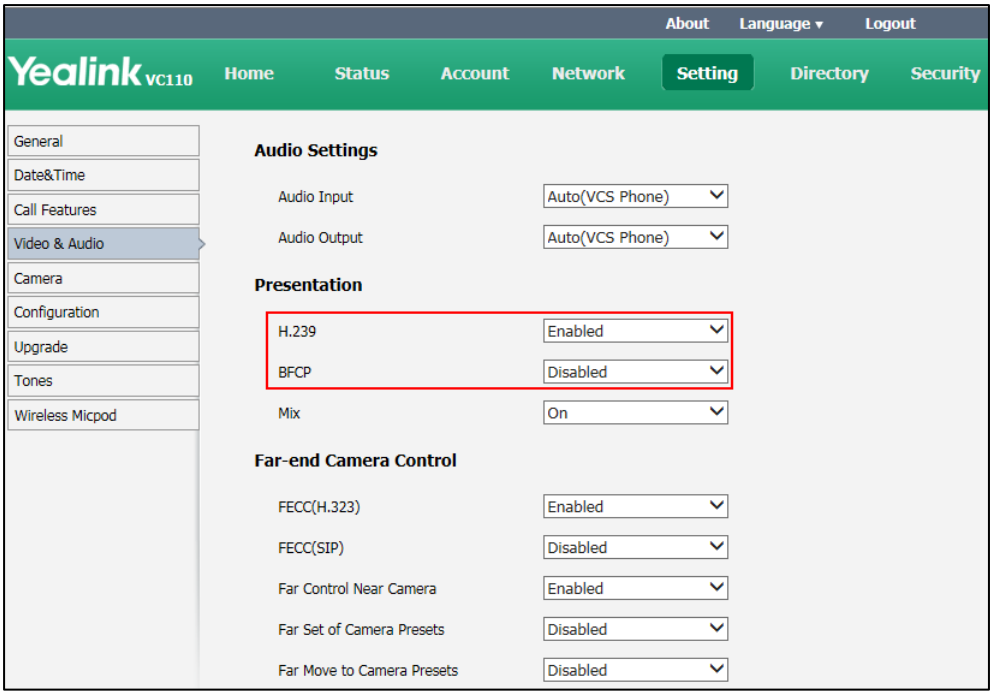
Dual-stream protocol parameters on the endpoint are described below.

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

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

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

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



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

Mix Sending

Content sharing allows users to share content with other conference participants during a call. When a PC is connected to the PC port on the VC110 all-in-one unit, the display device can display both the camera video and the shared content. The content sharing feature is very useful in the conference scenario in which content sharing is needed (e.g., a slide or a flash).

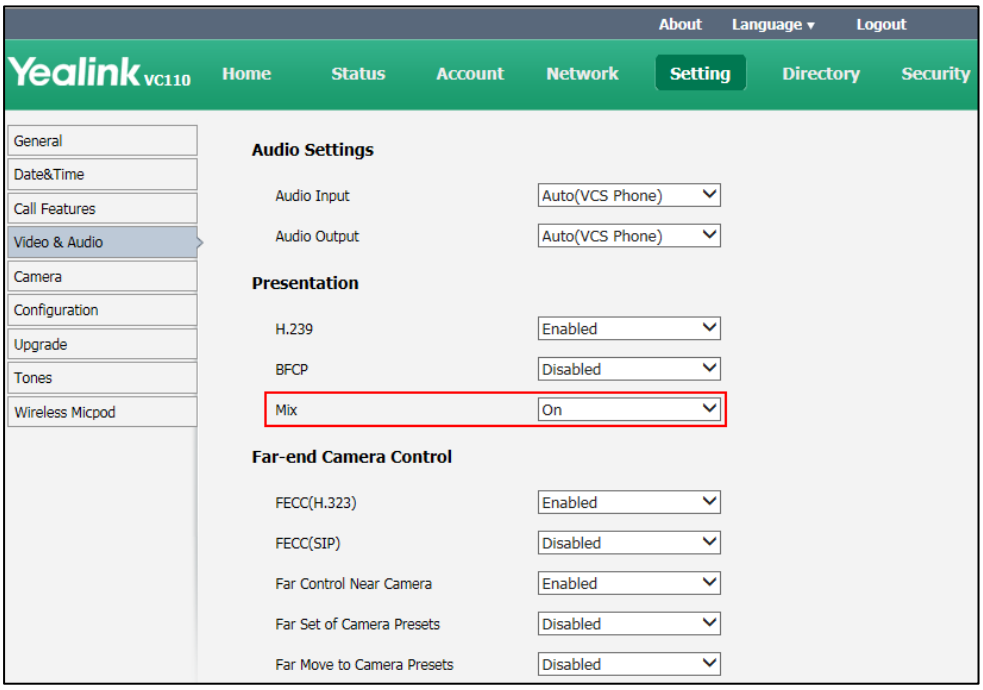
During a conference call, the far site may not support receiving shared content. In this case, you can enable mix sending feature on the endpoint. Mix sending feature allows the sender to compound multiple video streams (local image+shared content) to one video stream, and then send it to the far site.

The mix sending parameter on the endpoint is described below.

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

To configure mix sending via the web user interface:

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



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

Configuring Camera Settings

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

Camera settings parameters are described below.

Parameter	Description	Configuration Method
Exposure Compensation	Configures the value of camera exposure compensation. • Off • 1 • 2 • 3 **Default:** 1 Exposure compensation is used to compensate the camera effectively when shooting in a	Remote Control Web User Interface

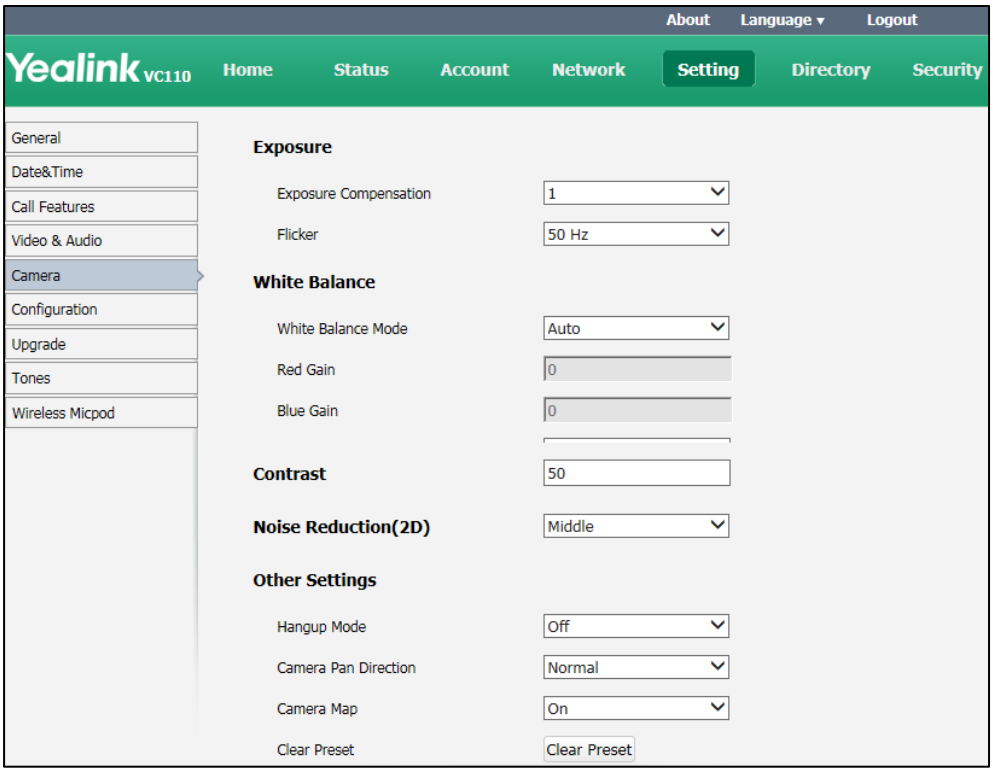
Parameter	Description	Configuration Method
	backlight environment. If the environment light is dark, increase the compensation value.	
Flicker	Configures the value of camera flicker frequency. • 50Hz • 60Hz **Default:** 50Hz **Note**: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by.	Remote Control Web User Interface
White Balance Mode	Configures the white balance mode of the camera. • Auto—Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. • One push—Use the predefined color temperature settings to provide acceptable color reproduction. • ATW—Automatically adjust the white balance based on the video image shoot by the camera. • Manual—Manually set red and blue gain. **Default:** Auto	Remote Control Web User Interface
Red Gain	Configures the red gain of the camera. **Valid Values:** 0-100	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: 0 **Note**: You can set this parameter only when the white balance mode is configured to Manual.	
Blue Gain	Configures the blue gain of the camera. **Valid Values:** 0-100 **Default:** 0 **Note**: You can set this parameter only when the white balance mode is configured to Manual.	Remote Control Web User Interface
Saturation	Configures the saturation of the camera. **Valid Values:** 0-14 **Default:** 7	Remote Control Web User Interface
Sharpness	Configures the sharpness of the camera. **Valid Values:** 0-14 **Default:** 1 **Note**: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.	Remote Control Web User Interface
Brightness	Configures the brightness of the camera. **Valid Values:** 0-100 **Default:** 50	Remote Control Web User Interface
Contrast	Configures the contrast of the camera. **Valid Values:** 0-100 **Default:** 50	Remote Control Web User Interface
Noise Reduction (2D)	Specifies the noise reduction (2D) mode. • Off • Low	Remote Control Web User Interface

Parameter	Description	Configuration Method
	• Middle • High **Default:** Middle	
Hangup Mode	Enables or disables the camera to flip the image view when camera is handed at up-side-down position **Default:** Off	Remote Control Web User Interface
Camera Pan Direction	Configures the pan direction of the camera. • Normal • Reversed **Default:** Normal If the camera reversed mode is enabled, the camera pan direction will be reversed when pressing the left and right navigation keys on the remote control. In this case, you can set the camera pan direction to Reversed.	Remote Control Web User Interface
Camera Map	Enables or disables the preview of camera presets. **Default:** On **Note**: If it is set to on, you can view the pre-saved camera presets.	Remote Control Web User Interface
Clear Preset	Clears all camera presets.	Remote Control Web User Interface
Reset Camera	Reset the camera settings to factory defaults. **Note:** The camera presets will also be cleared.	Remote Control Web User Interface

To configure camera settings via the web user interface:

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



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

To configure camera settings via the remote control:

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

Far-end Camera Control

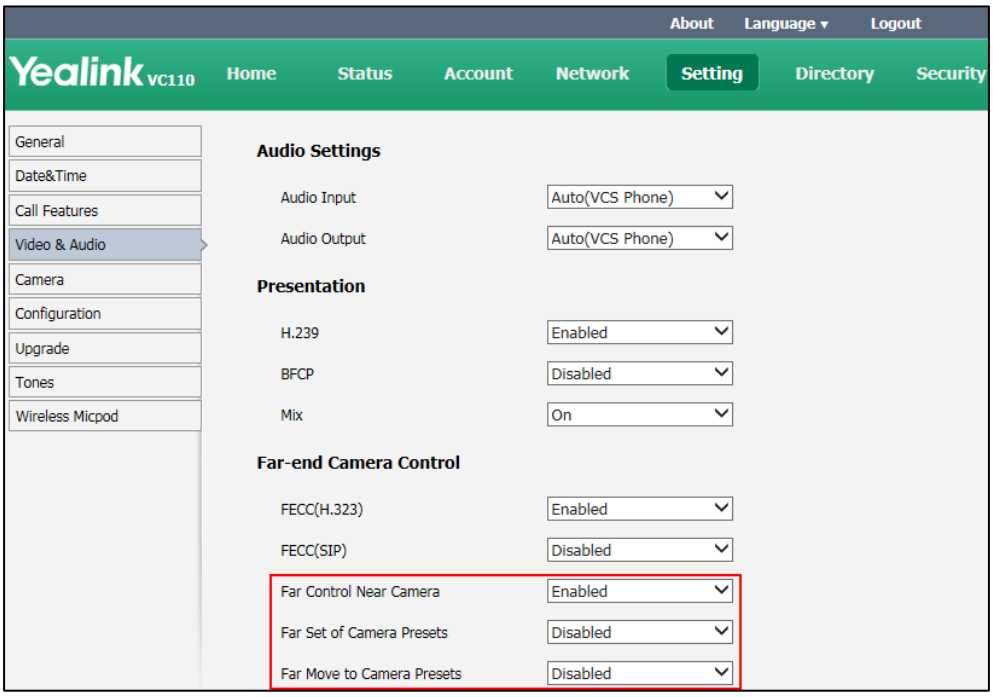
Local video is displayed on the display device of the far site during a call. For the best view, you can enable the Far Control of Near Camera feature to allow the far site to control the focus and angle of the local camera. You can also specify whether the far site is allowed to store and use the local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

Far control of the near camera parameters are described below.

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

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

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



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

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

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

Camera Control Protocol

VC110 video conferencing endpoints support camera control protocols: FECC (Far End Camera Control). You can enable the FECC protocol for SIP call or H.323 call.

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

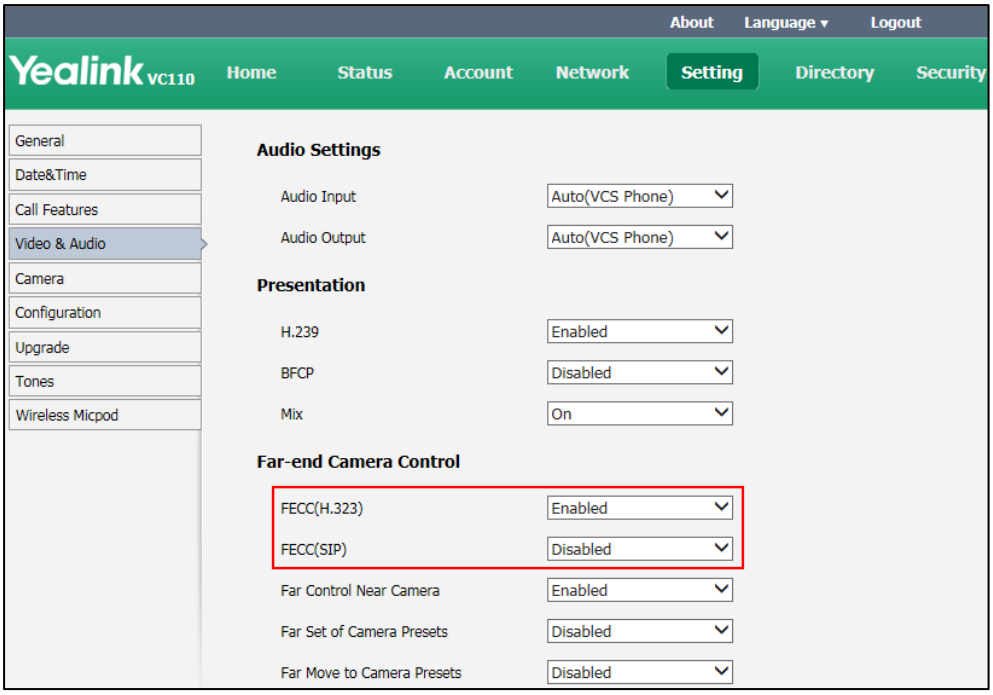
Camera control protocol parameters are described below:

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

To configure camera control protocol via the web user interface:

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

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



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

Tones

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

- Australia
- Austria
- Brazil
- Belgium
- China
- Chile
- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain

- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States

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

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

Tones parameters on the endpoint are described below:

Parameter	Description	Configuration Method
Select Country	Customizes tones or selects the desired country tone set. **Default:** Custom	Web User Interface
Ring Back	Customizes the ring-back tone for the endpoint. tone = element1[,element2][,element3]…[,element8] Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4	Web User Interface

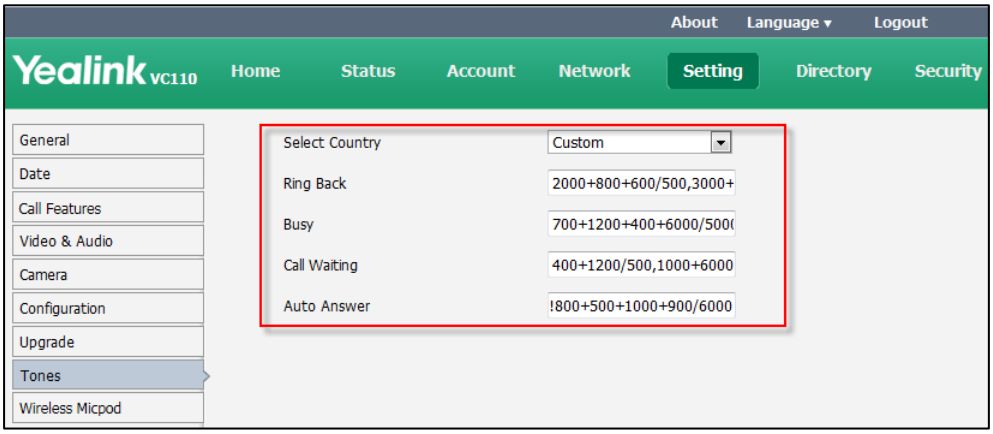
Parameter	Description	Configuration Method
	] /Duration **Freq**: the frequency of the tone (ranges from 200Hz to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone consists of at most four different frequencies. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). If you want the endpoint to play tones once, add an exclamation mark "!" before tones (e.g., !250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	
Busy	Customizes the busy tone for the endpoint. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Call Waiting	Customizes the call waiting tone for the endpoint. For more information on how to customize the tone, refer to the parameter "Ring Back".	Web User Interface

Parameter	Description	Configuration Method
	Default: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	
Auto Answer	Customizes the auto answer tone for the endpoint. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface

To configure tones via the web user interface:

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

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



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

Endpoint Management

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

- Local Directory
- LDAP
- Call History
- Search Source List in Dialing
- Dual Screen

Local Directory

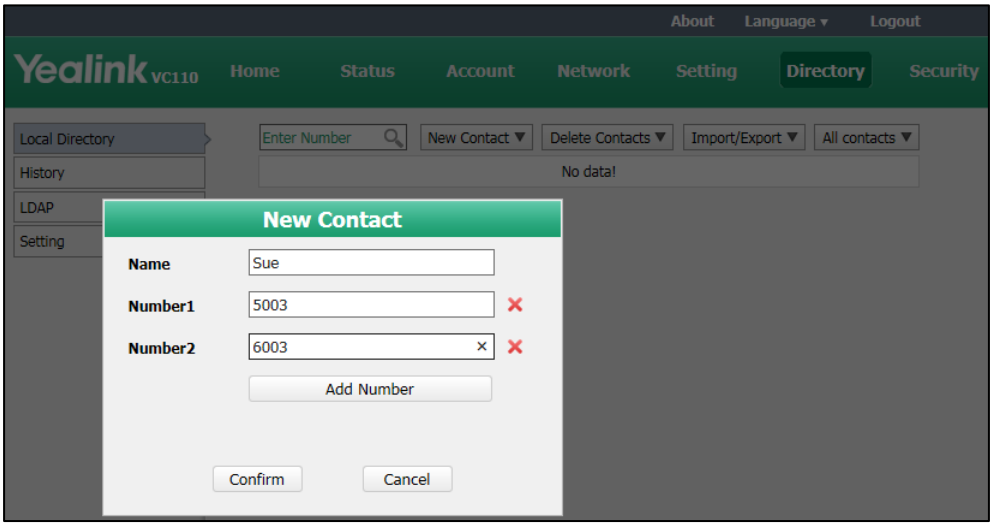
The VC110 endpoint can store up to 500 local contacts. You can add multiple numbers for a contact (at most 3).

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

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

To add local contacts via the web user interface:

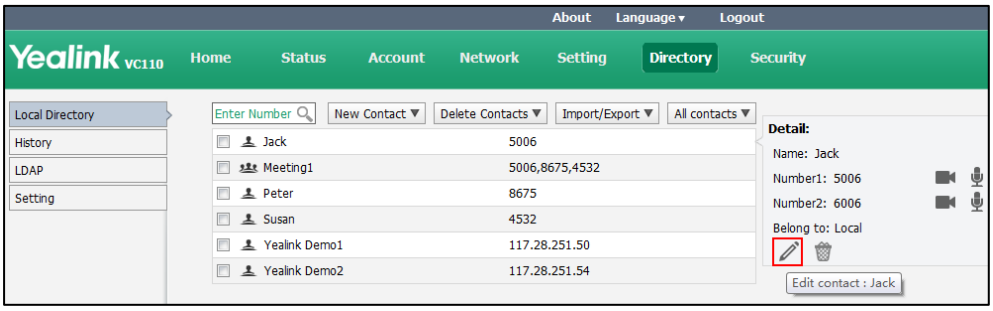
1. Click on **Directory->Local Directory**.
2. Click **New Contact**, and select **Local**.
3. Enter the desired name in the **Name** field.
4. Enter the desired number in the **Number** field.
5. Click **Add Number,** enter other number of the contact.



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

To edit contacts via the web user interface:

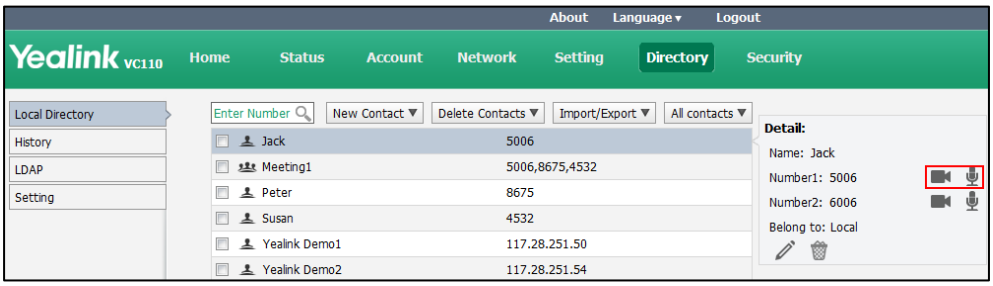
1. Click on **Directory->Local Directory**.
2. Hover your cursor over the contact you want to edit.
3. Click in the pop-up detail box.



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

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

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

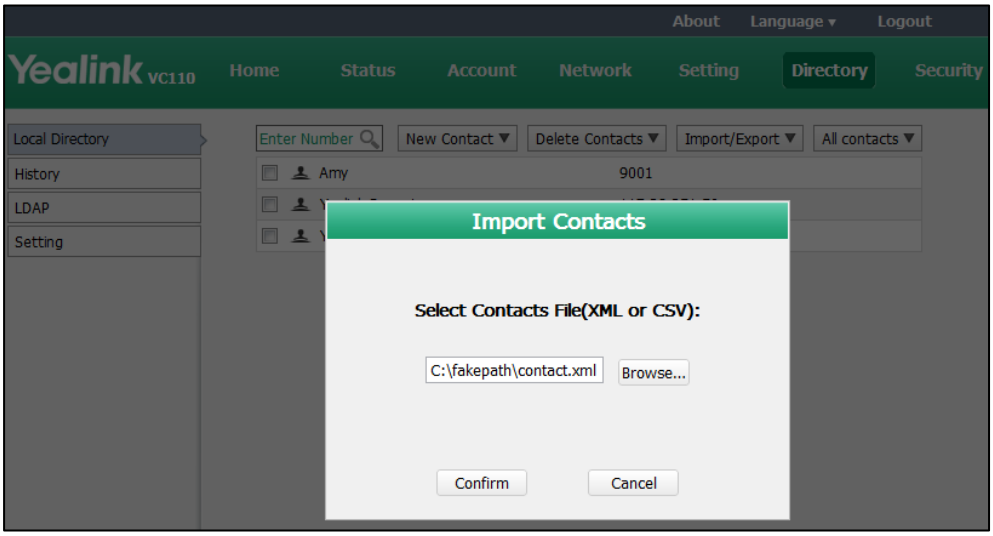


The web user interface prompts" Connecting, please wait!" and jumps automatically to the **Home** screen.

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

1. Click on **Directory->Local Directory**.
2. Click **Import/Export**, and select **Import**.

3. Click **Browse** to locate a contact list file (file format must be *.xml) from your local endpoint.



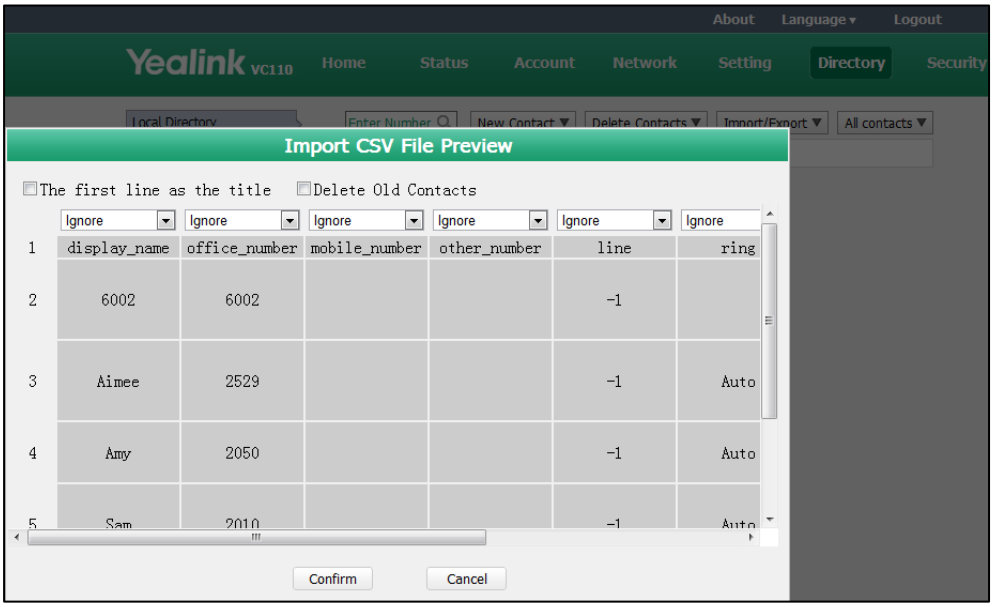
4. Click **Confirm** to import the contact list.

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

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

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

   The web user interface is shown below:



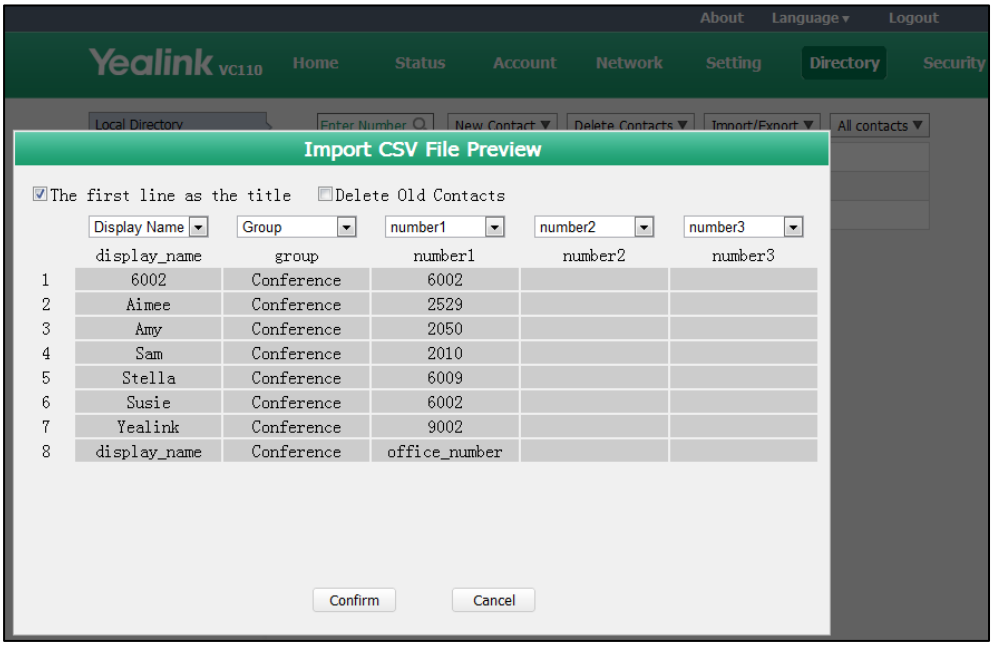
5. (Optional.) Check the **The first line as the title** checkbox.

It will prevent importing the title of the contact information which is located in the first line of the CSV file.

6. (Optional.) Check the **Delete Old Contacts** checkbox.

   It will delete all existing contacts while importing the contact list.

7. Select the desired value from the pull-down list.
   - If **Ignore** is selected, this column will not be imported to the endpoint.
   - If **Display Name** is selected, this column will be imported to the endpoint as the contacts' name.
   - If **number1/2/3** is selected, this column will be imported to the endpoint as the contacts' number.



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

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

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

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

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. Yealink VC110 endpoint is configurable to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

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

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using the endpoint. Therefore they do not have to maintain the local directory. Users can search and dial out from the LDAP directory and save LDAP entries to the local directory. LDAP entries displayed on the display device screen are read only. They cannot be added to, edited or deleted by users. When an LDAP server is configured properly, the endpoint can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select the desired entry or group, and retrieve the desired information.

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

Performing a LDAP search on the endpoint:

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

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

LDAP Attributes

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

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

LADP parameters are described below:

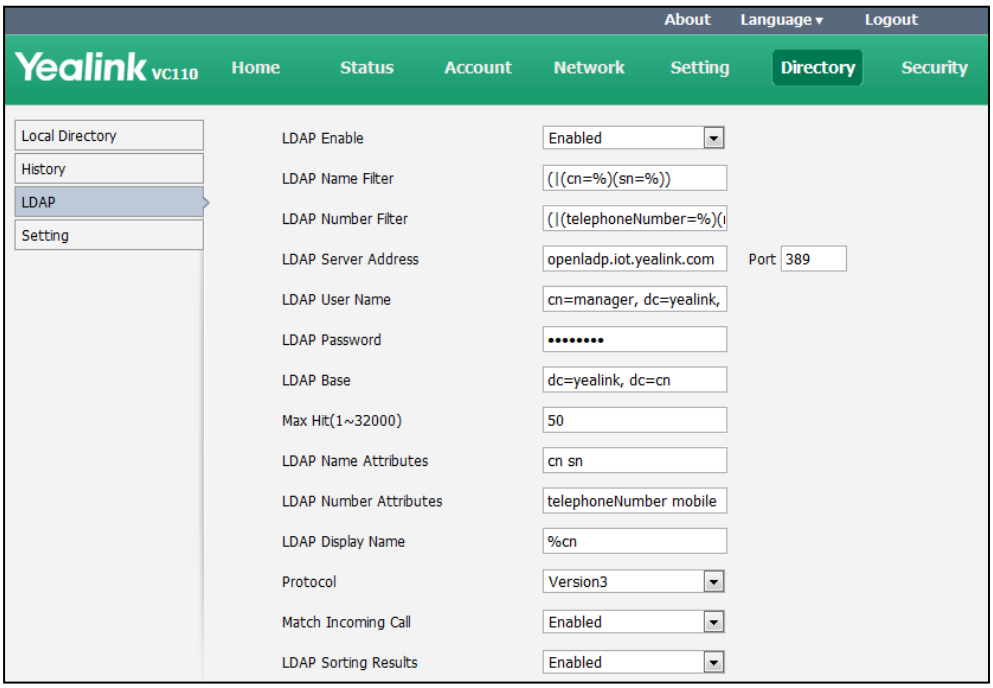
Parameter	Description	Configuration Method
LDAP Enable	Enables or disables the LDAP feature on the endpoint. **Default:** Disabled	Web User Interface
LDAP Name Filter	Configures the name attribute for LDAP searching. **Example:** (|(cn=%)(sn=%))	Web User Interface
LDAP Number Filter	Configures the number attribute for LDAP searching. **Example:** (|(telephoneNumber=%)(mobile=%))	Web User Interface
LDAP Server Address	Configures the domain name or IP address of the LDAP server.	Web User Interface
Port	Configures the LDAP server port. **Default:** 389	Web User Interface
LDAP User Name	Configures the user name used to log into the LDAP server. **Note:** The user name is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user name to access the LDAP server.	Web User Interface
LDAP Password	Configures the password to log into the LDAP server. **Note:** The password is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user password to access the LDAP server.	Web User Interface
LDAP Base	Configures the root path of the LDAP search base. **Example:**	Web User Interface

Parameter	Description	Configuration Method
	cn=manager,dc=yealink,dc=cn	
Max Hit(1~32000)	Configures the maximum number of search results to be returned by the LDAP server.	Web User Interface
LDAP Name Attributes	Configures the name attributes of each record to be returned by the LDAP server. **Note:** multiple name attributes should be separated by spaces. **Example**: cn sn	Web User Interface
LDAP Number Attributes	Configures the number attributes of each record to be returned by the LDAP server. **Note:** multiple numbers attributes should be separated by spaces. **Example**: telephoneNumber mobile	Web User Interface
LDAP Display Name	Configures the display name of the contact record displayed on the LCD screen. **Note:** multiple numbers attributes should be separated by spaces. **Example**: %cn	Web User Interface
Protocol	Configures the protocol for the LDAP server. **Note:** Make sure the protocol value corresponds with the version assigned on the LDAP server.	Web User Interface
Match Incoming Call	Enables or disables the endpoint to match caller numbers with LDAP contacts. **Default**: Disabled	Web User Interface
LDAP Sorting Results	Enables or disables the endpoint to sort the search results in alphabetical order or numerical order. **Default**: Disabled	Web User Interface

For more information on string representations of LDAP query filters, refer to RFC 2254.

To configure LDAP via the web user interface:

1. Click on **Directory->LDAP**.
2. Enter the values in the corresponding fields.
3. Select the desired values from the corresponding pull-down lists.



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

Call History

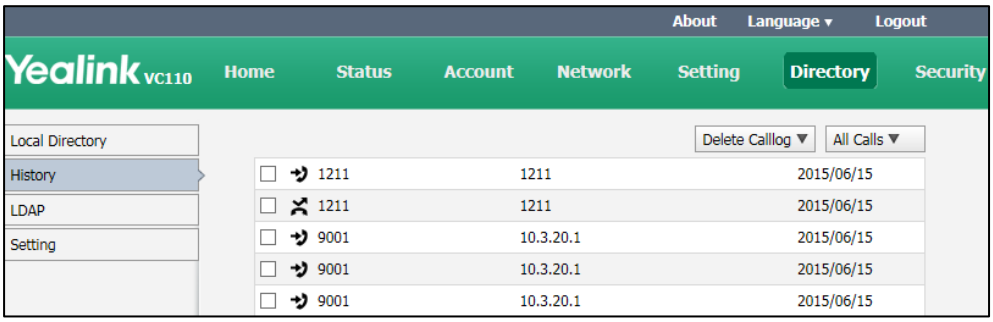
The VC110 video conferencing endpoint maintains call history lists of All Calls, Missed Calls, Placed Calls and Received Calls. Call history lists supports up to 400 entries. You can view the call history, place a call or delete an entry from the call history list. You can view the call history and place a call from the call history list via the web user interface or the remote control, but you can delete call history only via the web user interface.

History record feature is enabled by default. If it is disabled, the call history won't be saved. For more information, refer to History Record on page 118.

To view call history via the web user interface:

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

   The web user interface displays all call history.



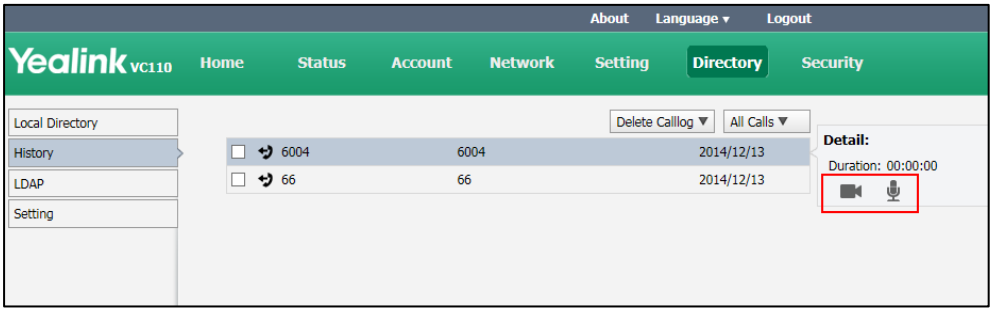
2. Click **All Calls**, select the desired call history list.

To place a call from the call history list via the web user interface:

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

   The web user interface displays all call history.

2. Hover your cursor over the entry you want to call.
3. Click or in the pop-up detail box to place a video or audio call.



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

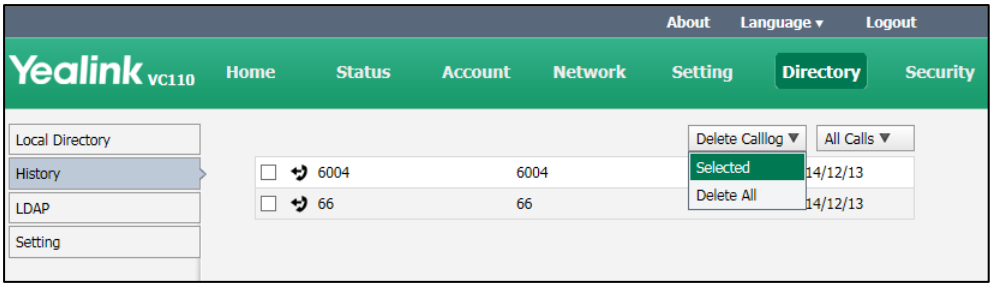
To delete an entry from the call history list via the web user interface:

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

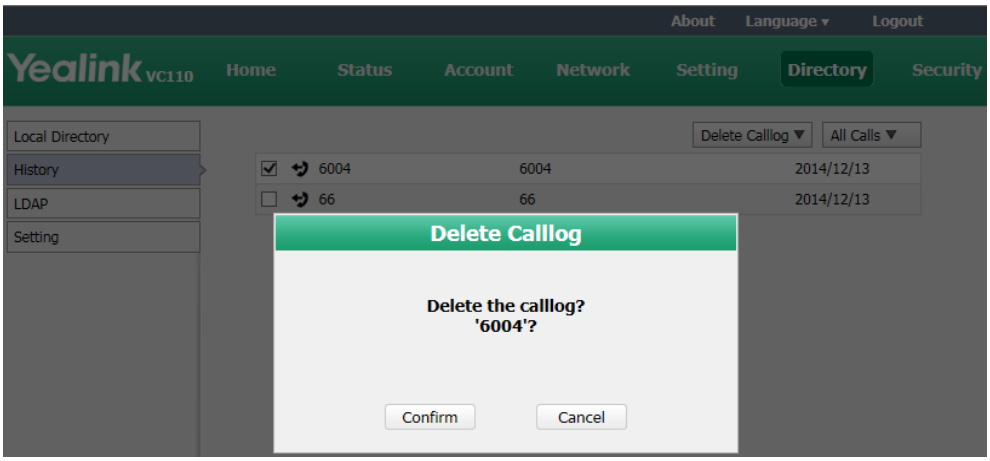
   The web user interface displays all call history.

2. Check the checkbox for the entry you want to delete.

3. Click **Delete Calllog**, and select **Selected**.



The web user interface prompts "Delete the calllog 'xxx'？"



5. Click **Confirm** to delete the call log.

You can also select **Delete All** from the from the pull-down list of **Delete Calllog** to delete all call log.

Search Source List in Dialing

When you enter a few characters in the dialing screen, the endpoint will search for contacts from the enabled search source lists, and display the result in the dialing screen. The lists can be Local Directory, History and LDAP.

To match the desired list, you need to enable the search source list first. If you want to match the LADP list, make sure LDAP is already configured. For more information on how to configure LDAP, refer to LDAP on page 162.

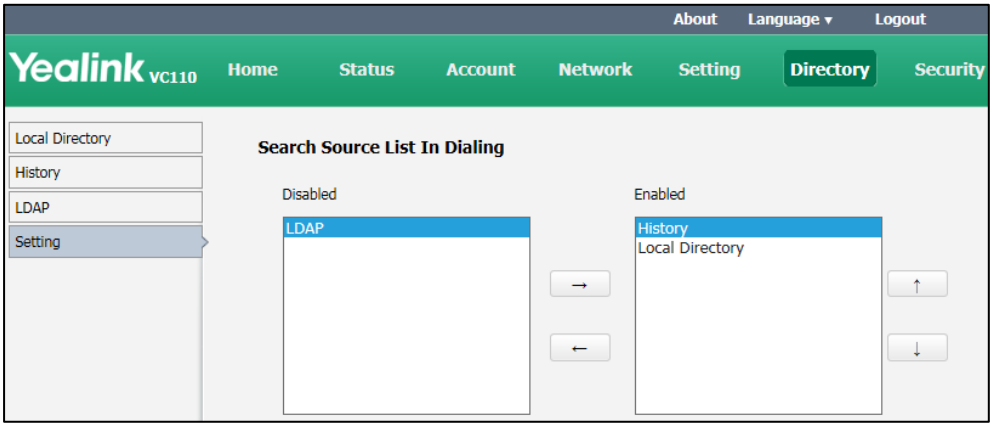
To configure search source list in dialing via the web user interface:

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

   The selected list appears in the **Enabled** column.
3. Repeat step 2 to add more lists to the **Enabled** column.
4. (Optional.) To remove a list from the **Enabled** column, select the desired list and

then click ← .

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



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

Dual Screen

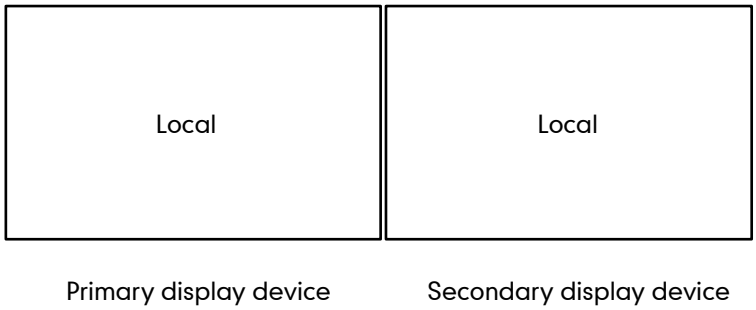
The VC110 has two display ports. When connecting only one display device to the VC110 all-in-one unit, Display1 port is the only available port. To make it easier for users to view video images, users can connect two display devices to Display1 and Display2 ports respectively. When two display devices are connected to the VC110 all-in-one unit, the status bar of the primary display device will display icon.

Two display devices (dual screen) are connected to the VC110 all-in-one unit:

- When the endpoint is idle and does not start a presentation.

  In the primary display device, the local video image is shown in full size.

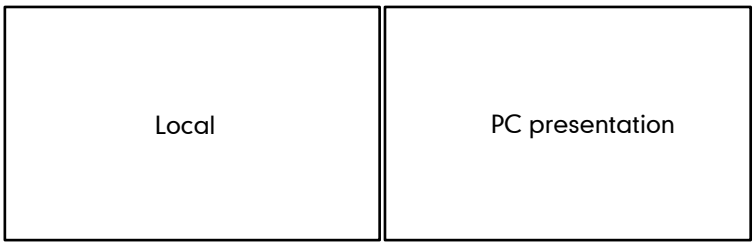
  In the secondary display device, the local video image is shown in full size (no menu and status bar).



- When the endpoint is idle and starts a presentation.

  In the primary display device, the local video image is shown in full size.

  In the secondary display device, the presentation is shown in full size (no menu and status bar).

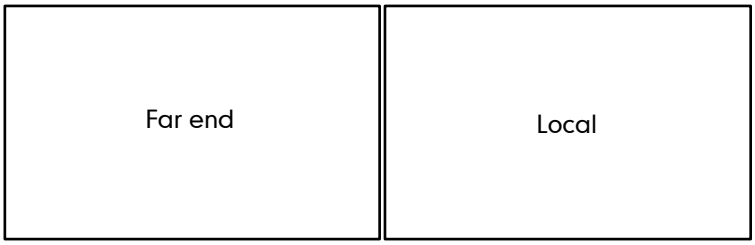


Primary display device Secondary display device

- When the endpoint is during a call and does not start a presentation.

  In the primary display device, the remote video image is shown in full size.

  In the secondary display device, the local video image is shown in full size.

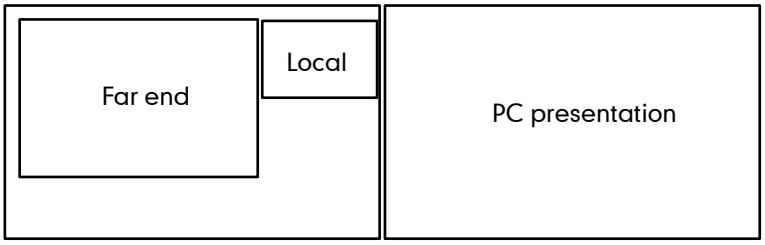


Primary display device Secondary display device

- When the endpoint is during a call and starts a presentation.

  In the primary display device, the remote video image is shown in big size, local video image along the right side of the screen is shown in small size.

  In the secondary display device, the presentation is shown in full size.



Primary display device Secondary display device

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

To specify the display content on the secondary display device via the remote control:

1. Press the **More** soft key during an active call.
2. Select **Focus (Display2)**, and then press OK.
3. Press ◀ or ▶ to select the desired content, and then press OK.

The secondary display device displays the selected content. The icon is displayed on the focus content.

After reassigning the display content on the secondary display device, the presentation will automatically be displayed on the primary display device.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- User Mode
- Administrator Password
- Web Server Type
- Transport Layer Security
- Secure Real-Time Transport Protocol
- H.235
- Attack Defense in Public Network

User Mode

Users can access the endpoint menus directly (except the "Advanced" menu) on the display device. The "Advanced" menu requires administrator credentials. You can enable the user mode to provide two levels of access for the menus. You need to configure a password for the user when the user mode is enabled. Users are prompted to enter the password when accessing the menus (except the "Status" menu). After the user mode is enabled, the user can l log into the web user interface of the endpoint with user credentials. The default user name is "user".

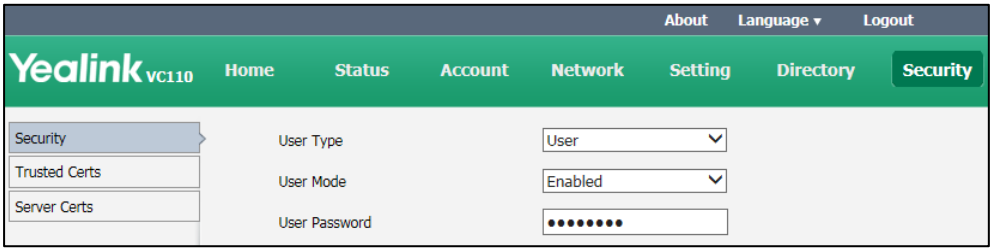
User mode parameters on the endpoint are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To enable the user type, you need to select User for this parameter.	Web User Interface
User Mode	Enables or disables the user mode. **Default:** Disabled **Note:** It is only applicable to the user mode. The administrator mode is enabled by default.	Web User Interface
User Password	Configures a password for the	Web User Interface

Parameter	Description	Configuration Method
	user to access the menus or log into the web user interface. **Note:** It can only be configured when the user mode is enabled. The endpoint supports ASCII characters 32-126(0x20-0x7E) in passwords. You can leave the password blank.	

To configure user mode via the web user interface:

1. Click on **Security**->**Security**.
2. Select **User** from the pull-down list of **User Type**.
3. Select **Enabled** from the pull-down list of **User Mode**.
4. Configure a password or leave it blank in the **User Password** field.



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

Administrator Password

The default enabled user type is administrator. Users can log into the web user interface and access the "Advanced" menu with administrator privilege by default. The default administrator password is "0000" and can be only changed by an administrator. For security reasons, the administrator should change the default administrator password as soon as possible. The endpoint supports ASCII characters 32-126(0x20-0x7E) in passwords.

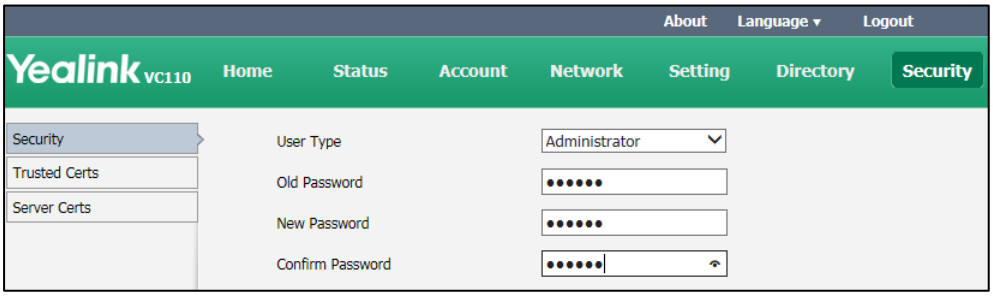
Administrator password parameters on the endpoint are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To configure a new administrator password, you need to select Administrator for this parameter.	Web User Interface

Parameter	Description	Configuration Method
Old Password	Enters the old administrator password. **Note:** The default administrator password is "0000".	Remote Control Web User Interface
New Password	Configures a new administrator password. **Note:** You can leave the password blank.	Remote Control Web User Interface
Confirm Password	Enters the new configured administrator password. **Note:** The entered password must be the same as the one configured by the parameter "New Password".	Remote Control Web User Interface

To configure administrator password via the web user interface:

1. Click on **Security**->**Security**.
2. Select **Administrator** from the pull-down list of **User Type**.
3. Enter the old administrator password in the **Old Password** field.
4. Enter a new password in the **New Password** field.
5. Enter the new password or leave it blank in the **User Password** field.



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

To configure administrator password via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Password Reset**.
2. Enter the old password in the **Current Password** field.
3. Configure a new password in the **New Password** and **Confirm Password** fields.
4. Press the **Save** soft key to accept the change.

Web Server Type

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

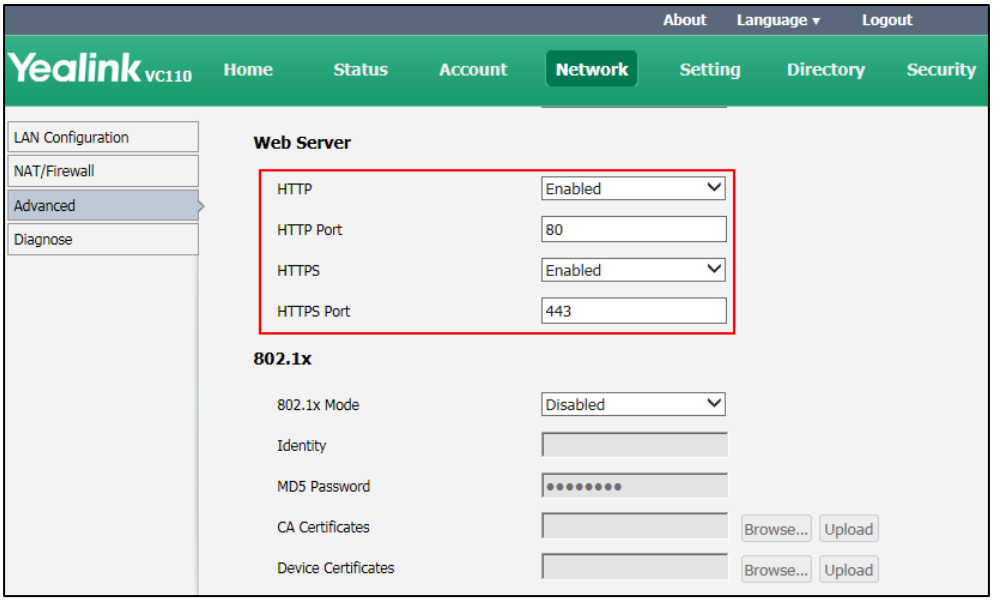
Web server type parameters on the endpoint are described below:

Parameter	Description	Configuration Method
HTTP	Enables or disables the user to access the web user interface of the endpoint using the HTTP protocol. **Default:** Enabled **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	Remote Control Web User Interface
HTTP Port	Specifies the HTTP port for the user to access the web user interface of the endpoint. **Valid Values:** 1-65535 **Default:** 80 **Note:** Ensure that the configured port is not used. If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
HTTPS	Enables or disables the user to access the web user interface of the endpoint using the HTTPS protocol. **Default:** Enabled **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	Remote Control Web User Interface
HTTPS Port	Specifies the HTTPS port for the	Web User Interface

Parameter	Description	Configuration Method
	user to access the web user interface of the endpoint. **Valid Values:** 1-65535 **Default:** 443 **Note:** Ensure that the configured port is not used. If you change this parameter, the endpoint will reboot to make the change take effect.	

To configure web server type via the web user interface:

1. Click on **Network->Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port in the **HTTP Port** field.
4. Select the desired value from the pull-down list of **HTTPS**.
5. Enter the desired HTTPS port in the **HTTPS Port** field.



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

   A dialog box pops up to prompt that the settings will take effect after a reboot.
7. Click **Confirm** to reboot the endpoint immediately.

To configure web server type via the remote control:

1. Select **Menu->Advanced** (default password: 0000) **->Advanced Network**.
2. Select the desired value from the pull-down list of **Web Server Type**.
3. Press the **Save** soft key to accept the change.

The display device prompts "Reboot now?".

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

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing the endpoint to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

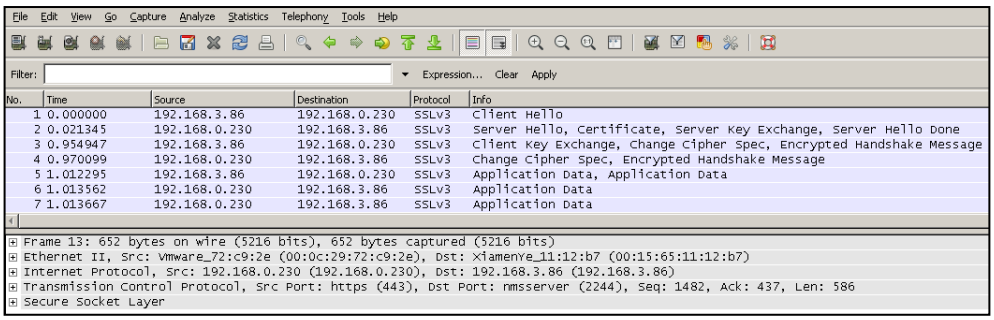
TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The endpoint supports TLS 1.0. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. The endpoint supports the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA

- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the endpoint and TLS server to establish an encrypted communication channel:



Step1: The endpoint sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

Step3: The endpoint sends key session information (encrypted by server's public key) in the "Client Key Exchange" message.

Step4: Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

The endpoint can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for the SIP account, the message of the SIP account will be encrypted after the successful TLS negotiation.

Certificates

The endpoint can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the endpoint requests a TLS connection with a server, the endpoint should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The endpoint has 30 built-in trusted certificates. You can upload up to 10 custom certificates to the endpoint. The format of the certificates must be *.pem, *.cer, *.crt and *.der. For more information on 30 trusted certificates, refer to Appendix B: Trusted Certificates on page 220.
- **Server Certificate**: When clients request a TLS connection with the endpoint, the endpoint sends the server certificate to the clients for authentication. The endpoint has two types of built-in server certificates: a unique server certificate and a

generic server certificate. You can only upload one server certificate to the endpoint. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer.

- **A unique server certificate**: It is installed by default and is unique to a endpoint (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
- **A generic server certificate**: It is installed by default and is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the endpoint may send a generic certificate for authentication.

The endpoint can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the endpoint accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the endpoint to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

TLS parameters on the endpoint are described below:

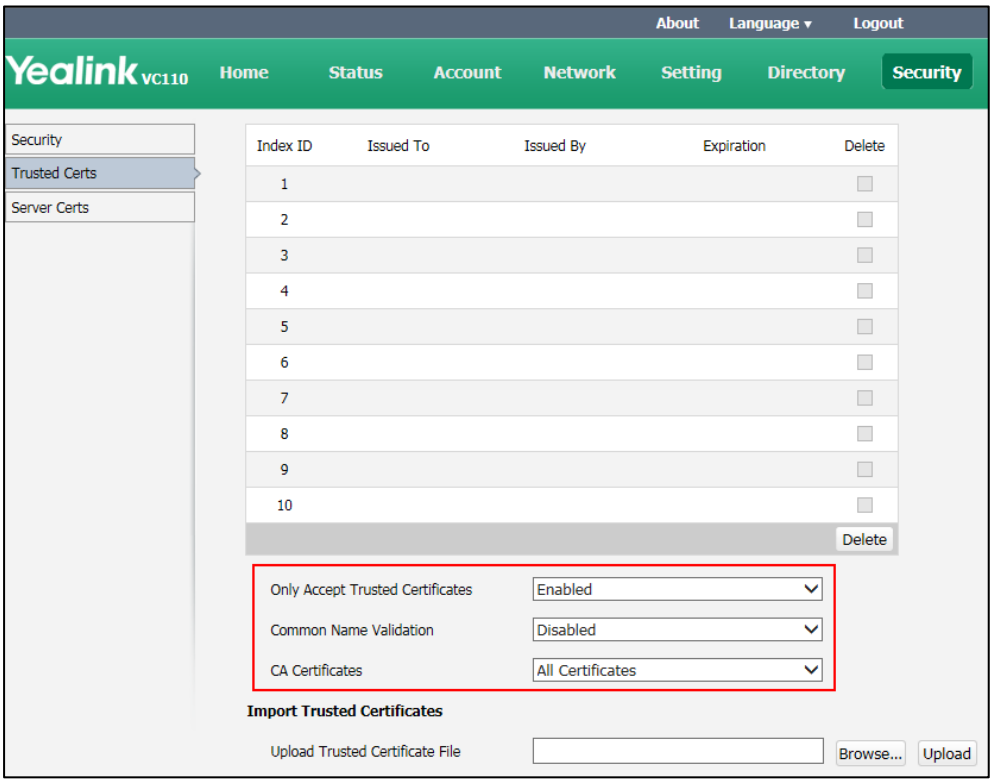
Parameter	Description	Configuration Method
Transport	Configures the type of transport protocol for the SIP account. • **UDP**—provides best-effort transport via UDP for the SIP signaling. • **TCP**—provides reliable transport via TCP for SIP signaling. • **TLS**—provides secure communication for SIP signaling. TLS is available only when the endpoint is registered with a SIP server that supports TLS.	Remote Control Web User Interface
Only Accept Trusted Certificates	Enables or disables the endpoint to only trust the server certificates in the Trusted Certificates list. **Default:** Enabled **Note:** If it is enabled, the endpoint will authenticate the server certificate based on the trusted	Web User Interface

Parameter	Description	Configuration Method
	certificates list. Only when the authentication succeeds, will the endpoint trust the server. If you change this parameter, the endpoint will reboot to make the change take effect.	
Common Name Validation	Enables or disables the endpoint to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **Default:** Disabled **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the type of certificates in the Trusted Certificates list for the endpoint to authenticate for the TLS connection. • **Default Certificates** • **Custom Certificates** • **All Certificates** **Default:** Default Certificates **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
Upload Trusted Certificate File	Upload the custom CA certificate to the endpoint. **Note:** A maximum of 10 CA certificates can be uploaded to the endpoint. The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	Web User Interface
Device Certificates	Upload the customized CA certificate to the endpoint. • **Default Certificates**	Web User Interface

Parameter	Description	Configuration Method
	• **Custom Certificates** **Default:** Default Certificates **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	
Upload Server Certificate File	Upload the custom device certificate to the endpoint. **Note:** Only one device certificate can be uploaded to the endpoint. The device certificate you want to upload must be in *.pem or *.cer format.	Web User Interface

To configure the trusted certificate feature via the web user interface:

1. Click on **Security->Trusted Certs**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
3. Select the desired value from the pull-down list of **Common Name Validation**.
4. Select the desired value from the pull-down list of **CA Certificates**.



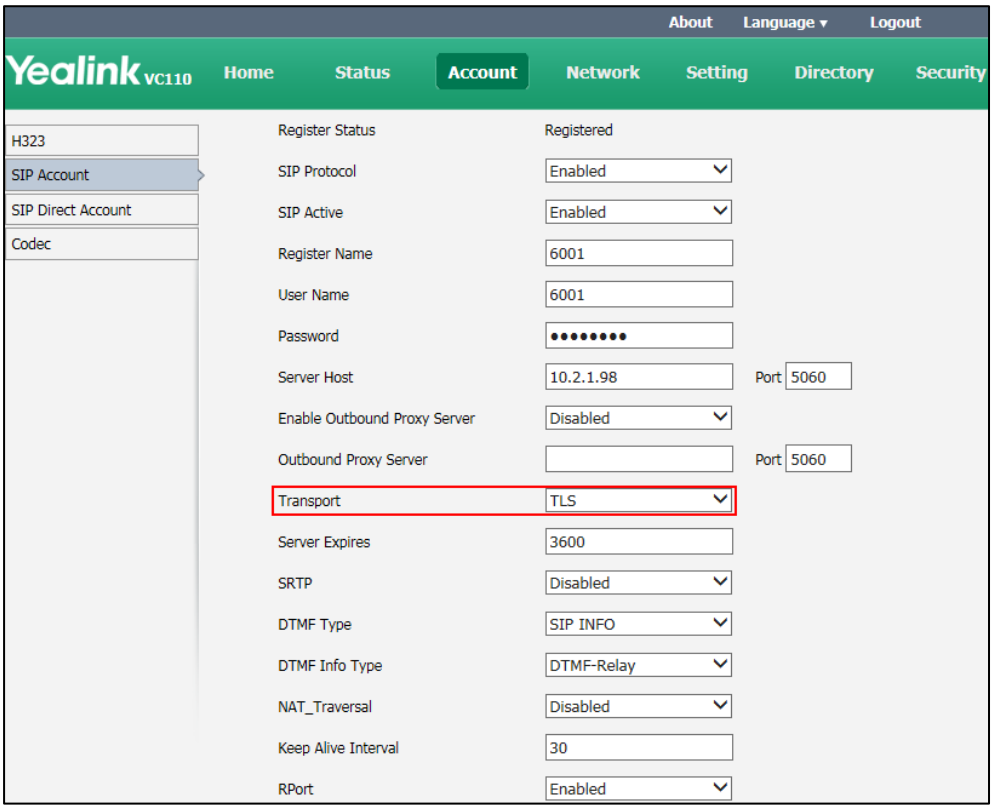
5. Click **Confirm** to accept the change.

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

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

To configure TLS for the SIP account via the web user interface:

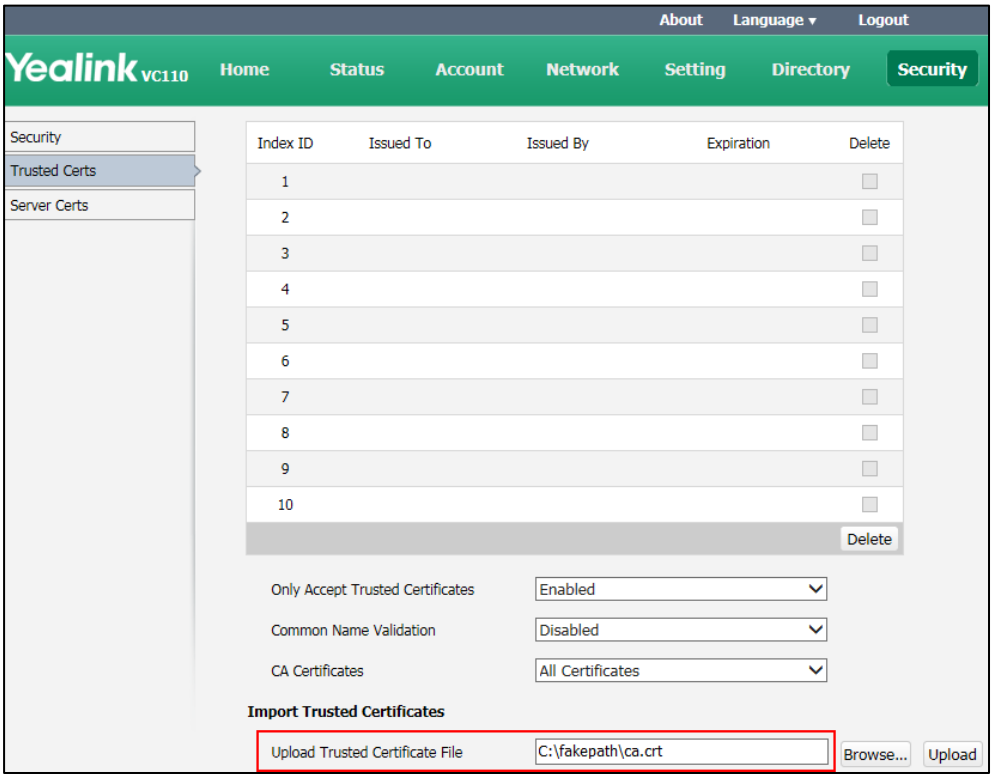
1. Click on **Account->SIP Account**.
2. Select **TLS** from the pull-down list of the **Transport**.



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

To upload a CA certificate via the web user interface:

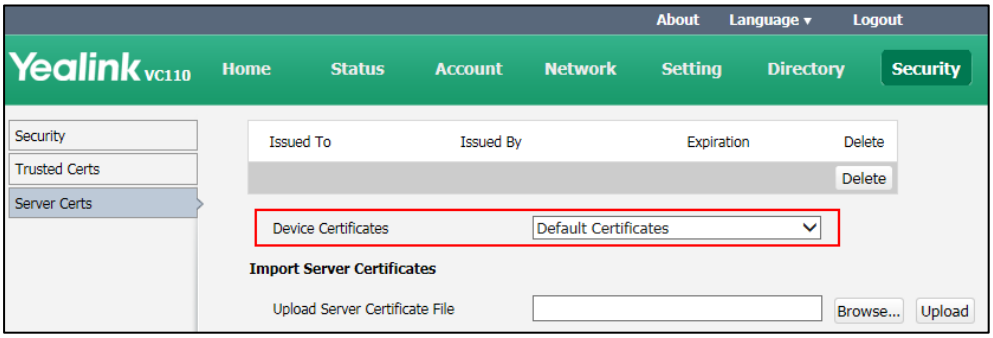
1. Click on **Security->Trusted Certs**.
2. Click **Browse** to locate the certificate (*.pem,*.crt, *.cer or *.der) from your local endpoint.



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

To configure the device certificate via the web user interface:

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

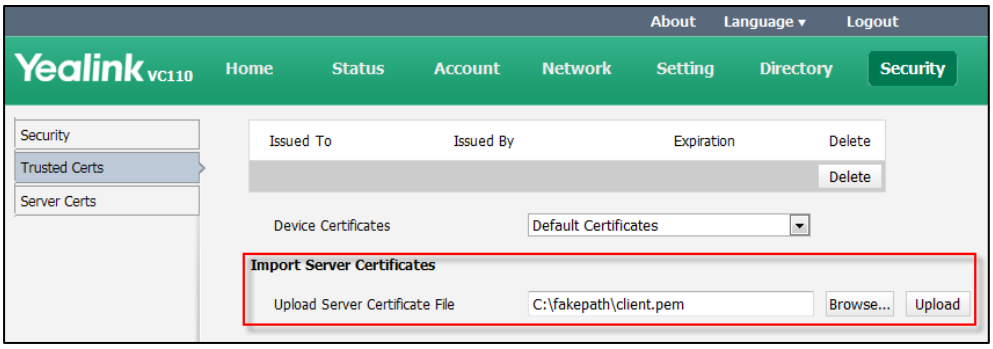


3. Click **Confirm** to accept the change.

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

To upload a device certificate via the web user interface:

1. Click on **Security->Server Certs**.
2. Click **Browse** to locate the certificate (*.pem or *.cer) from your local endpoint.



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

Secure Real-Time Transport Protocol

During a confidential call, you can configure Secure Real-Time Transport Protocol (SRTP) to encrypt RTP streams to avoid interception and eavesdropping. Both RTP and RTCP signaling may be encrypted using an AES algorithm as described in RFC3711. Encryption modifies the data in the RTP streams so that, if the data is captured or intercepted, it cannot be understood—it sounds like noise. Only the receiver knows the key to restore the data. To use SRTP encryption for SIP calls, the participants in the call must enable SRTP simultaneously. When this feature is enabled on both endpoints, the encryption algorithm utilized for the session is negotiated between the endpoints. This negotiation process is compliant with RFC 4568.

When a site places a call on the SRTP enabled endpoint, the endpoint sends an INVITE message with the RTP encryption algorithm to the destination endpoint.

The following is an example of the RTP encryption algorithm carried in the SDP of the INVITE message:

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

The following is an example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

The SRTP parameter on the endpoint is described below:

Parameter	Description	Configuration Method
SRTP	Specifies the SRTP type. You can specify it to the SIP account or SIP direct account separately. • **Disabled**—do not use SRTP in SIP calls. • **Enabled**—negotiate with the far site whether to use SRTP for media encryption in SIP calls. • **Compulsory**—compulsory use SRTP for media encryption in SIP calls. **Default:** Disabled	Web User Interface

Rules of SRTP for media encryption in SIP calls:

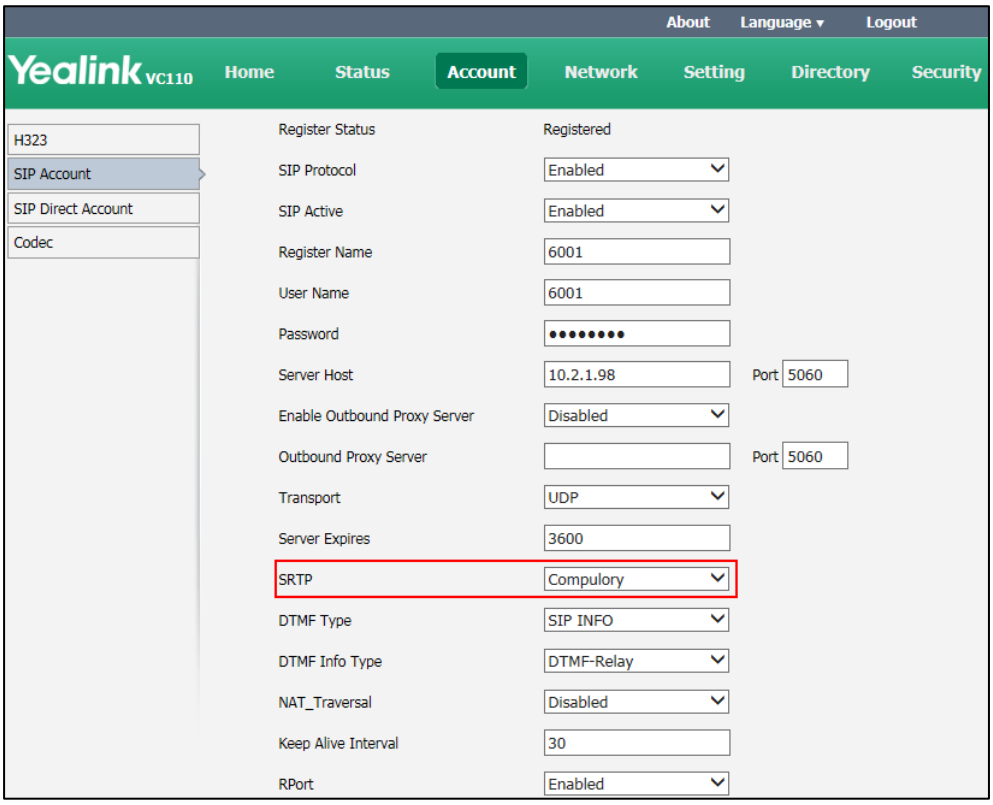
Far \ Near	Compulsory	Enabled	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Enabled	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

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

Note If SRTP is enabled for the SIP account, you should also configure the transport type to TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security on page 178.

To configure SRTP for SIP account via the web user interface:

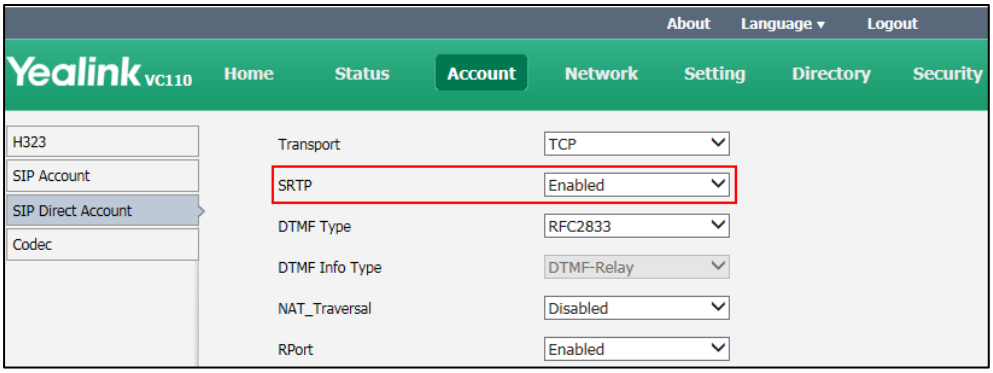
1. Click on **Account->SIP Account**.
2. Select the desired value from the pull-down list of **SRTP**.



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

To configure SRTP for SIP direct account via the web user interface:

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



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

H.235

Yealink VC110 video conferencing endpoints support H.235 128-bit AES algorithm using the Diffie-Hellman key exchange protocol in H.323 calls. To use H.235 feature for H.323 calls, the participants in the call must enable the H.235 feature simultaneously. When a site places a call on the H.235 feature enabled endpoint, the endpoint negotiates the encryption algorithm with the destination endpoint.

The H.235 parameter on the endpoint is described below:

Parameter	Description	Configuration Method
H.235	Specifies the H.235 type for the H.323 calls. • **Disabled**—do not use H.235 in H.323 calls. • **Enabled**—negotiate with the far site whether to use H.235 in H.323 calls. • **Compulsory**—compulsively use H.235 in H.323 calls. **Default:** Disabled	Web User Interface

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

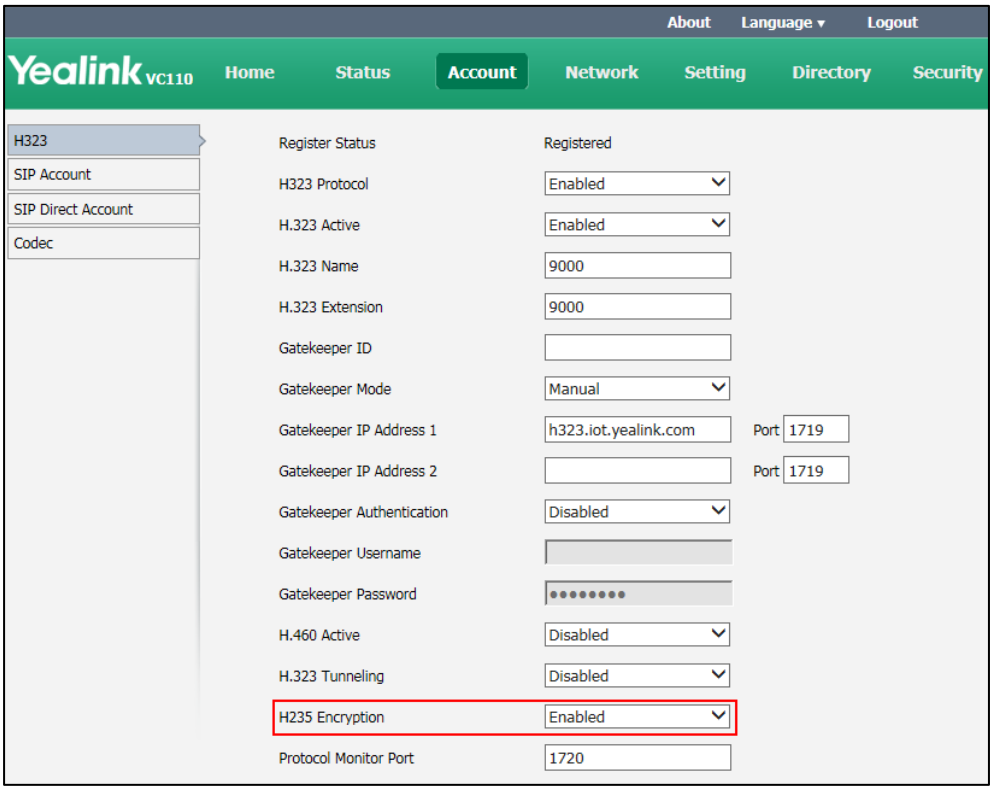
Far \ Near	Compulsory	Enabled	Disabled
Compulsory	Encrypted Call	H.235 Call	Fail to establish call
Enabled	H.235 Call	H.235 Call	Unencrypted Call

Disabled	Fail to establish a call	RTP Call	RTP Call

When H.235 is enabled on both endpoints, calls will be encrypted, and the lock icon appears on the display device of each endpoint during a call..

To configure H.235 via the web user interface:

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



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

Attack Defense in Public Network

VoIP phones often suffer from network attacks in public network, which results in communication failure. To ensure the safety of the enterprise VoIP phone, you can configure abnormal call answering feature for handling abnormal calls using the SIP protocol. For abnormal calls using the H.323 protocol, you can configure safe mode call feature to handle them.

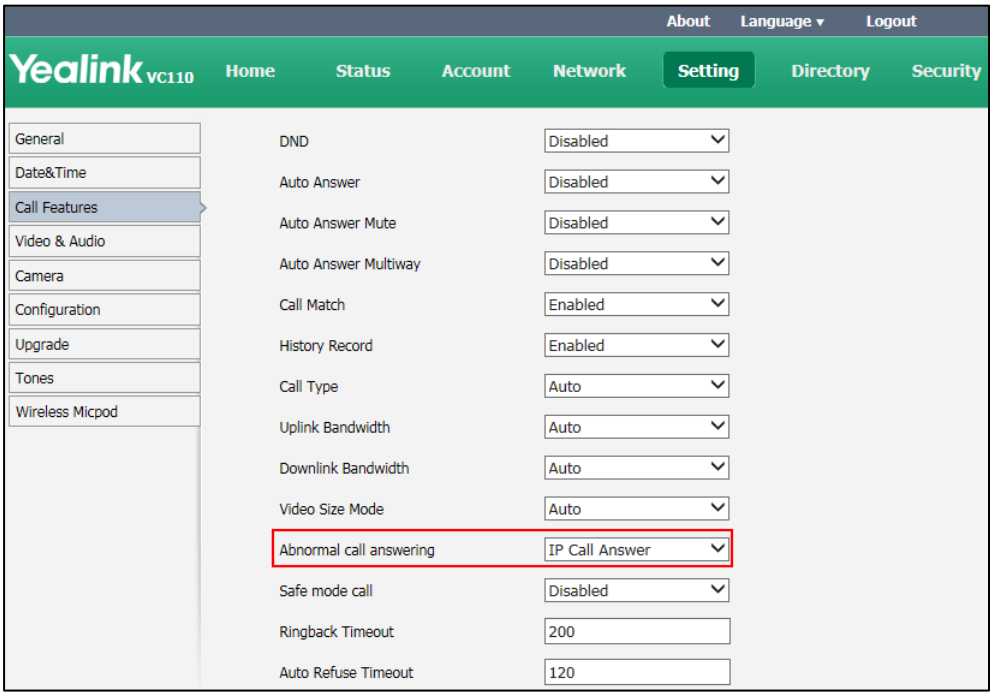
Abnormal Call Answering

The abnormal call answering parameters on the endpoint are described below:

Parameter	Description	Configuration Method
Abnormal call answering	Specifies the account type for answering SIP incoming call from public network. • **Disabled**—reject the SIP incoming call from public network. • **Account Answer**—use first SIP account to answer the SIP incoming call from public network. • **IP Call Answer**—use endpoint IP to answer the SIP incoming call from public network. **Default:** IP Call Answer	Web User Interface

To configure abnormal call answering via the web user interface:

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



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

Configuring Safe Mode Call

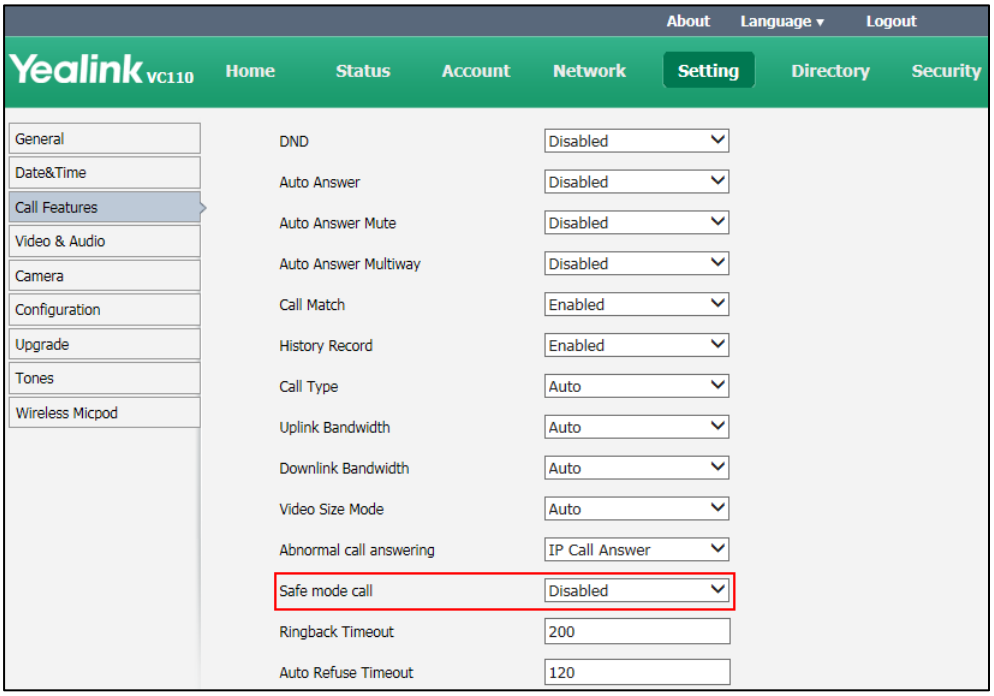
You can configure safe mode call feature to handle abnormal H.323 calls.

The safe mode call parameters on the endpoint are described below:

Parameter	Description	Configuration Method
Safe mode call	Enables or disables the safe mode call feature for H.323 incoming call from public network. • **Disabled**—do not use safe mode call. • **Enabled**—use safe mode call. **Default:** Disabled **Note:** If it is enabled, the endpoint will reject H.323 incoming call from public network. If it is disabled, any H.323 incoming call from public network can be accepted.	Web User Interface

To configure safe mode call via the web user interface:

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



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

Endpoint Maintenance

This chapter provides basic endpoint maintenance, including upgrading firmware, managing configurations, resetting endpoints and how to monitor network via SNMP. Topics include:

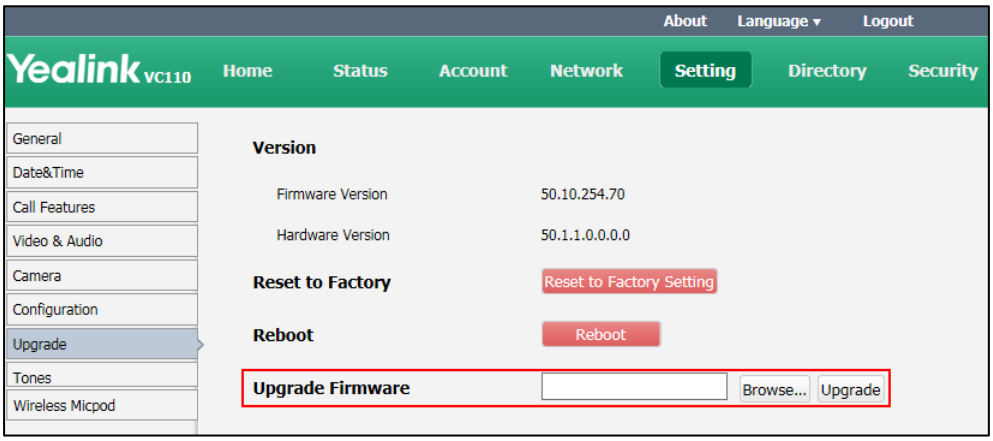
- Upgrading Firmware
- Importing/Exporting Configuration
- Resetting to Factory
- SNMP

Upgrading Firmware

The newly released firmware version may add new features. Because of this, Yealink recommends you to update the latest firmware. You can upgrade the endpoint firmware via the web user interface. The firmware name of the VC110 video conferencing endpoint is: 50.x.x.x.rom (x is the actual firmware version). You can download the latest firmware version from the Yealink website.

To upgrade firmware via the web user interface:

1. Click on **Setting**->**Upgrade**.
2. Click **Browse** to locate the firmware from your local endpoint.



3. Click **Upgrade** to upgrade the firmware.

   The browser pops up the dialog box "Firmware of the video conference endpoint will be updated. It will take 5 minutes to complete. Please don't power off!".

4. Click **Confirm** to confirm upgrading.

Note

Caution! Don't remove the Ethernet cable and power cord during the upgrade process. Don't close or refresh the web page when upgrading the firmware via the web user interface.

Importing/Exporting Configuration

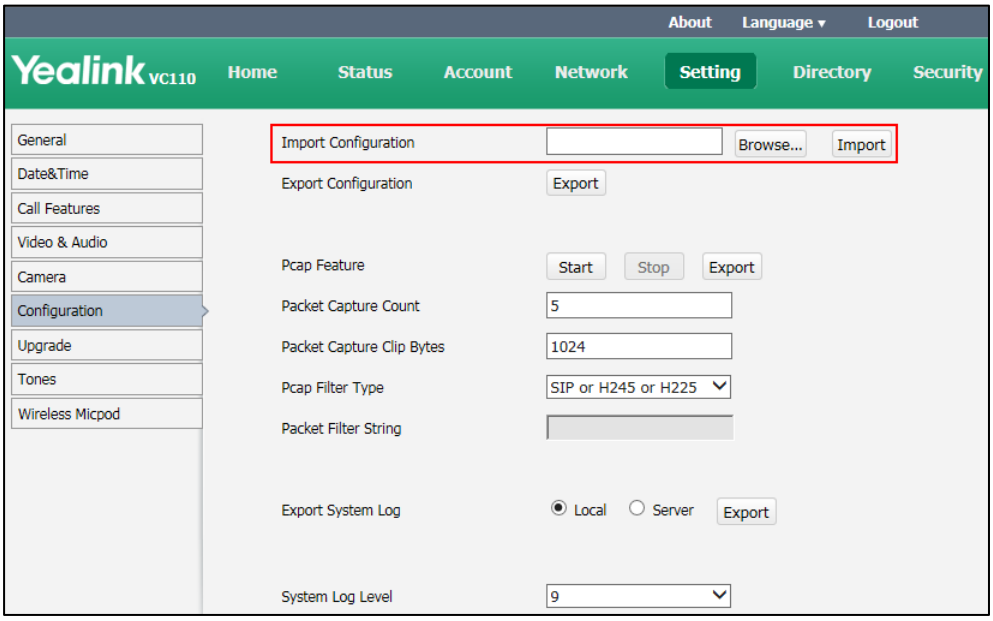
We may need you to provide the endpoint configurations for the Yealink field application engineers to help analyze problems. You can import configurations to your endpoint to configure your endpoint quickly. The file format of configuration file must be *.bin.

To export the endpoint configurations via the web user interface:

1. Click on **Setting->Configuration**.
2. Click **Export.**
3. Click **Confirm** to export the configurations.

To import the endpoint configurations via the web user interface:

1. Click on **Setting->Configuration**.
2. Click **Browse** to locate a configuration file from your local endpoint.



3. Click **Import** to import the configuration file.

Resetting to Factory

Reset the endpoint to factory configurations after you have tried all appropriate troubleshooting suggestions but still have not solved your problems.

When factory resetting the video endpoint, the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.
- All system parameters will be reset to default values.
- All custom files will be deleted. Such as, certificates, local contacts and registered accounts.

It is not possible to undo a factory reset. But you can export the configuration first, and then you can re-import the configuration to recovery the endpoint after the reset.

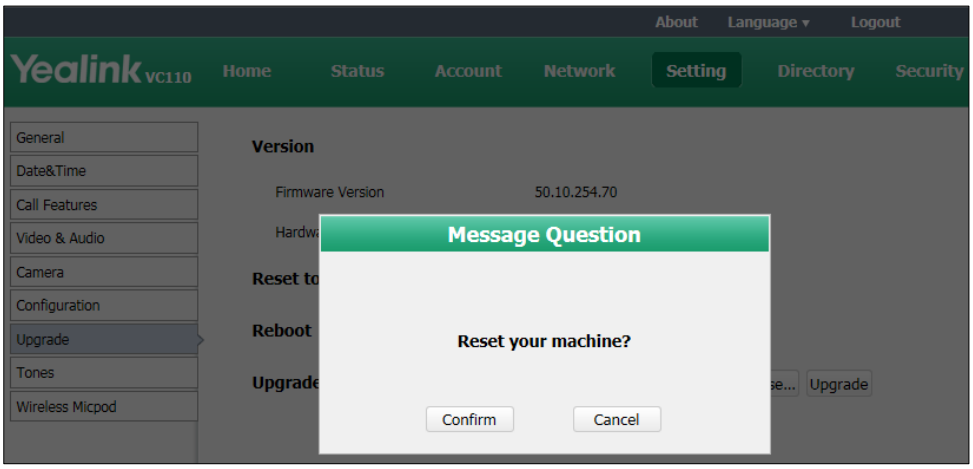
You can reset the endpoint via the reset key on the VC110 all-in-one unit, remote control or web user interface.

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

To reset the endpoint via the web user interface:

1. Click on **Setting**->**Upgrade**.
2. Click **Reset to Factory Setting** in the **Reset to Factory** field.

   The web user interface prompts the message "Reset your machine?".



3. Click **Confirm** to confirm the resetting.

To reset the endpoint via the remote control:

1. Select **Menu** ->**Advanced** (default password: 0000)->**Reboot & Reset**
2. Select **Reset**, and then press OK .

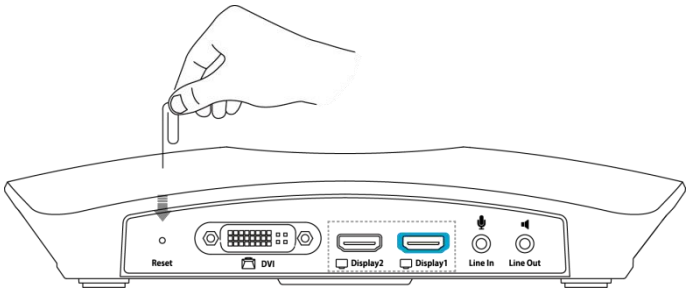
   The display device prompts" Reset to Factory? "
3. Select **OK**, and then press OK.

   The endpoint reboots automatically. The endpoint will reset to factory sucessfully after startup.

To reset the endpoint via the rest key on the VC110 all-in-one unit:

Using tiny objects (for example, the paper clip) to press and hold the reset button for 15 seconds until the screen turns black.

Do not power off the endpoint during the factory restore process. The endpoint reverts to the default factory settings and restarts automatically. This will take a few minutes.



SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management endpoints to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed endpoints, which describe the endpoint configuration. These variables can then be queried (and sometimes set) by managing applications. The variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs).

Yealink endpoints support SNMPv1 and SNMPv2. They work as SNMP clients, receiving requests from the SNMP server. The SNMP server may send requests from any available source port to the configured port on the client, while the client responds to the source port on the SNMP server. Yealink endpoints only support the GET request from the SNMP server.

You can download SNMP application to monitor and manage information on a network entity.

The following table lists the basic object identifiers (OIDs) supported by the endpoint.

MIB	OID	Description
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.1.0	The textual identification of the contact person for the endpoint, together with the contact information. For example, Sysadmin (root@localhost)
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.2.0	An administratively-assigned name for the endpoint. If the name is unknown, the value is a zero-length string.

MIB	OID	Description
		For example, Yealink VCS.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.3.0	The physical location of the endpoint. For example, Server Room
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.4.0	The time (in milliseconds) since the network management portion of the endpoint was last re-initialized.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.5.0	The firmware version of the endpoint.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.6.0	The hardware version of the endpoint.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.7.0	The endpoint's model.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.8.0	The MAC address of the endpoint.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.9.0	The IP address of the endpoint.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.10.0	The target version to which the current version is updated automatically. Format: MacVersion[*]ComVersion[*] For example, MacVersion[0.0.0.1]ComVersion[0.0.0.1]
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.11.0	The command of the endpoint reboot. Format: snmpset -v 2c XXXX public 37459.2.1.11.0 s reboot XXXX refers to the IP address of the endpoint.

SNMP parameters on the endpoint are described below:

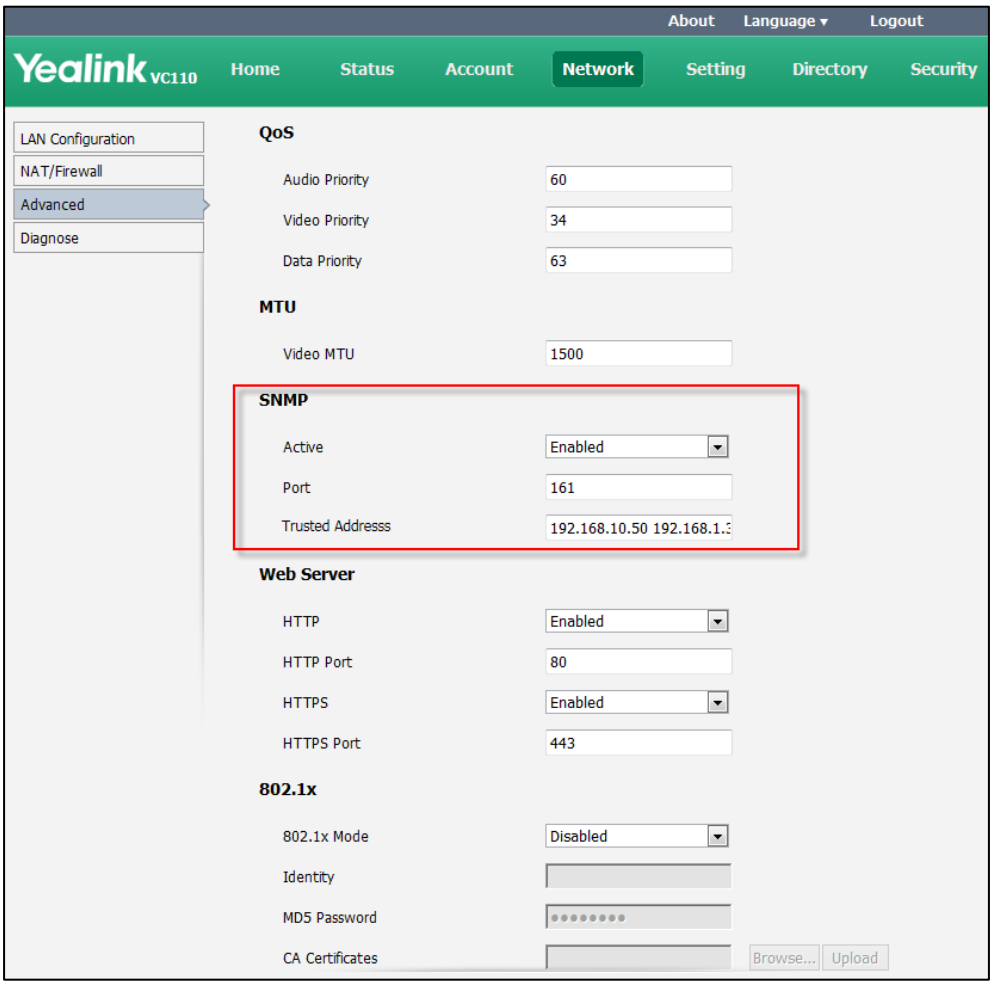
Parameter	Description	Configuration Method
SNMP->Active	Enables or disables SNMP feature on the endpoint. **Default:** Disabled **Note:** If you change this parameter, the endpoint will	Web User Interface

Parameter	Description	Configuration Method
	reboot to make the change take effect.	
Port	Specifies the SNMP port. **Valid Values:** 1-65535 **Default:** 161 **Note:** If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface
Trusted Address	Configures IP address(es) or domain name of the trusted SNMP server. Multiple IP addresses or domain names should be separated by spaces. **Note:** If it is left blank, the endpoint accepts and handles GET requests from any SNMP server. If you change this parameter, the endpoint will reboot to make the change take effect.	Web User Interface

To configure SNMP via the web user interface:

1. Click on **Network**->**Advanced**.
2. In the **SNMP** block, select **Enabled** from the pull-down list of **Active**.
3. Enter the SNMP port in the **Port** field.
4. Enter the IP address or domain name of the SNMP server in the **Trusted Address** field.

Multiple IP addresses or domain names should be separated by spaces.



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

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

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

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using the VC110 video conferencing endpoint.

Troubleshooting Methods

The endpoint can provide feedback in a variety of forms, such as log files, packets, status indicators and so on, which can help an administrator to find the endpoint problem more easily and resolve it.

The following sections will help you to better understand and resolve the working status of the endpoint.

- Viewing Log Files
- Capturing Packets
- Getting Information from Status Indicators
- Analyzing Configuration Files
- Viewing Call Statistics
- Using Diagnostic Methods

Viewing Log Files

The log files are Yealink specific debug files which may be requested by the Yealink support organization if you need technical support. The current log files are time stamped event log files. You can export the log files to a syslog server or the local endpoint. The administrator can specify the location where the log will be exported to and the severity level of the log.

Endpoint Log Level specifies the log level to be recorded. The default endpoint log level is 9.

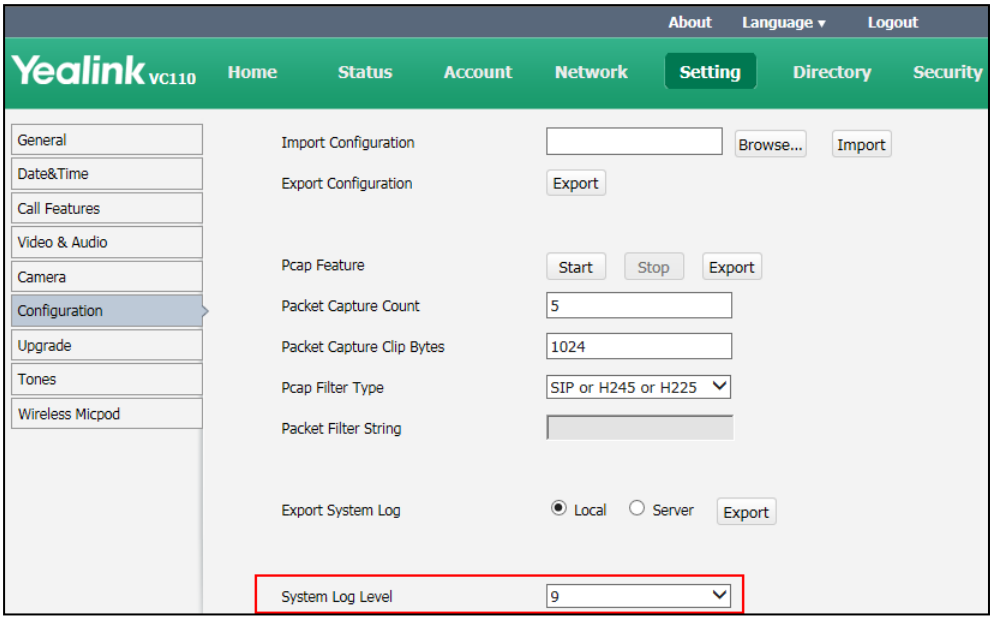
Endpoint log level parameters are described below:

Parameter	Description	Configuration Method
Export System Log	Specify where the endpoint log will be exported. **Valid values:** • **Local**-export the endpoint log to the local computer.	Web User Interface

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

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

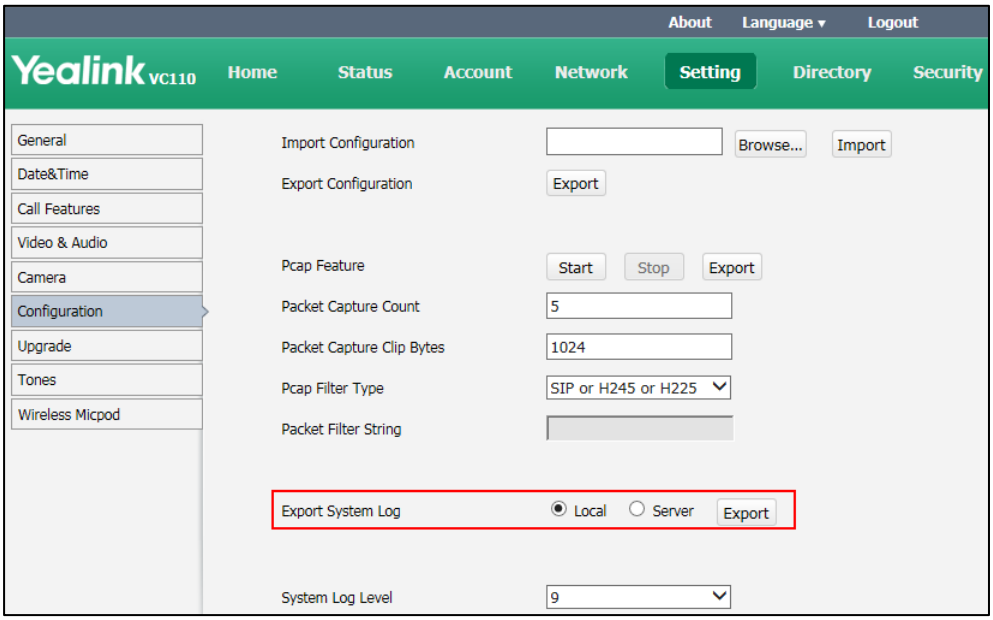
1. Click on **Setting->Configuration**.
2. Select the desired level from the pull-down list of **Endpoint System Level**.



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

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

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



3. Click **Export** to open the file download window, and then save the file to your local endpoint.

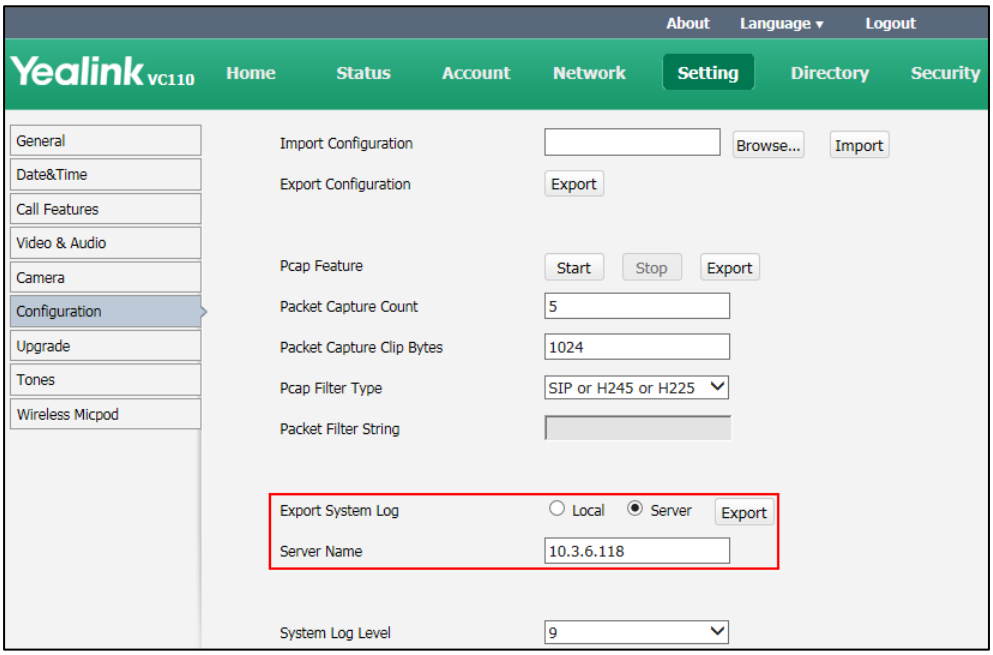
The following figure shows a portion of a log file:

```
  496 root       8876 SW  /yealink/bin/ggsvca_ipp
  497 root       8876 SW  /yealink/bin/ggsvca_ipp
  498 root       8876 SW  /yealink/bin/ggsvca_ipp
  499 root       8876 SW  /yealink/bin/ggsvca_ipp
  500 root       8876 SW  /yealink/bin/ggsvca_ipp
  501 root       8876 SW  /yealink/bin/ggsvca_ipp
  507 root      16424 SW  /yealink/bin/Screen.exe
  508 root      10344 SW  /yealink/bin/sipServer.exx
  509 root      10344 SW  /yealink/bin/sipServer.exx
  515 root      16424 SW  /yealink/bin/Screen.exe
  517 root      16424 SW  /yealink/bin/Screen.exe
  519 root      10344 SW  /yealink/bin/sipServer.exx
  521 root      16424 SW  /yealink/bin/Screen.exe
  522 root      16424 SW  /yealink/bin/Screen.exe
  523 root      16424 SW  /yealink/bin/Screen.exe
  524 root      10344 SW  /yealink/bin/sipServer.exx
  525 root            SW< [IRQ 45]
  526 root      10344 SW  /yealink/bin/sipServer.exx
  527 root      16424 SW  /yealink/bin/Screen.exe
  528 root      16424 SW  /yealink/bin/Screen.exe
  529 root      16424 SW  /yealink/bin/Screen.exe
 1147 root       1788 SWN sleep 1000
 1227 root      10120 SWN ConfigManApp.com
 1228 root       4624 SW  /yealink/bin/mini_httpd -p 80 -d /yealink/html -c cgi
 1229 root       2812 SWN sh -c cd /tmp;ifconfig >> Messages;ps >> Messages;tar
 1230 root       2812 RWN ps
Feb 29 06:01:09 mini_httpd[388]: mini_httpd.c(1510):child process 1227 exit!
Feb 29 06:01:12 mini_httpd[1232]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1232 exit!
Feb 29 06:01:12 mini_httpd[1233]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1233 exit!
Feb 29 06:01:12 mini_httpd[1234]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1234 exit!
```

To export a log file to a syslog server via the web user interface:

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

3. Enter the IP address or domain name of the syslog server in the **Server Name** field.



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

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

Capturing Packets

The administrator can capture packets in two ways: capturing the packets via the web user interface or using the Ethernet software. Engineers can analyze the packets to troubleshoot problems.

Packets parameters are described below:

Parameter	Description	Configuration Method
Pcap Feature	Start and stop capturing packets or export the captured packets.	Web User Interface
Packet Capture Count	Configures the count of the number of packets to capture. **Default:** 5	Web User Interface
Packet Capture Clip Bytes	Configures the number of bytes (in kb) of the packet to capture. **Default:** 1024	Web User Interface
Pcap Filter Type	Configures the filter type of the packet to capture. **Valid Values:** • **Custom**—Customize the	Web User Interface

Parameter	Description	Configuration Method
	packet filter string. • **SIP or H245 or H225**—Capture SIP, H245 and H225 packets. • **RTP**—Capture RTP packets. **Default:** SIP or H245 or H225	
Packet Filter String	Customizes the packet filter string. **Syntax:** Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression **Protocol**: Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used. **Direction**: Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2". **Host(s)**: 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	Web User Interface

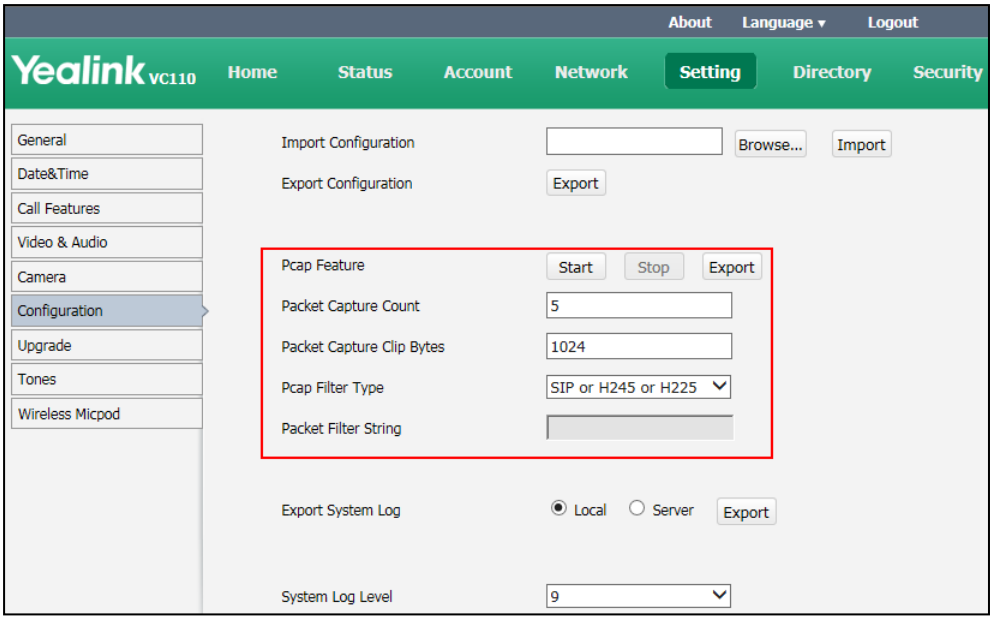
Parameter	Description	Configuration Method
	precedence and associate left to right. For example: "not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23". "not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)". **Example**: (src 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 Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8. **Default**: Blank **Note**: It only works if the parameter "Pcap Filter Type" is set to Custom.	

To capture packets via the web user interface:

1. Click on **Setting**->**Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.

   If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Click **Start** to start capturing signal traffic.
6. Reproduce the issue to get stack traces.
7. Click **Stop** to stop capturing.

8. Click **Export** to open the file download window, and then save the file to your local endpoint.



To capture packets using the Ethernet software:

Connect the Internet ports of the endpoint and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic. You can also set mirror port on a switch to monitor the port connected to the endpoint.

Getting Information from Status Indicators

In some instances, status indicators are helpful for finding endpoint troubles. Status indicators may consist of the power LED, icons on the status bar of the display device or prompt messages.

The following shows two examples of obtaining the endpoint information from status indicators:

- If a LINK failure of the endpoint is detected, the icon will appear on the status bar of the display device, indicating the current network is not available.
- If the power LED does not light, it indicates the endpoint is not powered on.

For more information on the icons, refer to Icon Instructions on page 29.

Analyzing Configuration Files

Wrong configurations may have an impact on your endpoint use. You can export configuration file to check the current configuration of the endpoint and troubleshoot if necessary. For more information on how to export endpoint configuration, refer to Importing/Exporting Configuration on page 194.

Viewing Call Statistics

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Uplink Bandwidth and Downlink Bandwidth.
- **Video**: Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost(%).
- Protocol used during a call.
- Device information of the far site.
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost(%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.

Use the remote control to select **More**->**Call Statistics** during an active call to view call statistics.

Using Diagnostic Methods

The endpoint supports the following diagnostic methods:

- **Audio Diagnose**: Check whether the audio input device and audio output device are working properly.
- **Camera Diagnose**: Check whether the camera can pan and change focus normally.
- **Ping**: Check whether the endpoint can establish contact with the IP address that you specify.
- **Trace Route**: Display the route (path) and measure transit delays of packets across an Internet Protocol (IP) network.

To diagnose audio via the remote control:

1. Select **Menu**->**Diagnose** menu.
2. Select **Audio Diagnose**, and then press OK.
3. Speak into the microphone.
4. Check whether the microphone can pick up audio and play back the audio properly.

   If the endpoint plays back the audio normally, it means that audio works well.
5. Press OK to stop audio diagnostics.

To diagnose the camera via the remote control:

1. Select **Menu**->**Diagnose** menu.
2. Select **Camera Diagnose**, and then press OK.
3. Press navigation keys to adjust the camera position.

4. Press or to adjust the focus.

   If the camera can move and zoom normally, it means that the camera works properly.

5. Press the **Back** soft key to stop camera diagnose.

To diagnose network via the remote control:

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

   The display device displays the network diagnose information.

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

   It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.

Trace Route:

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

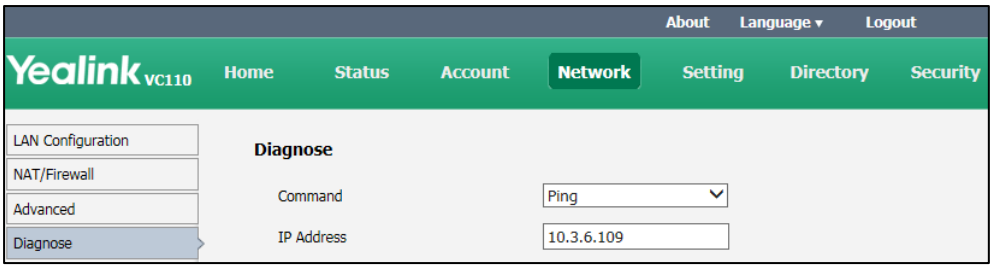
   The display device displays the network diagnose information.

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

   If the test is successful, the VC110 endpoint lists the hops between the endpoint and the IP address you entered. You can check whether congestion happens via the time cost between hops.

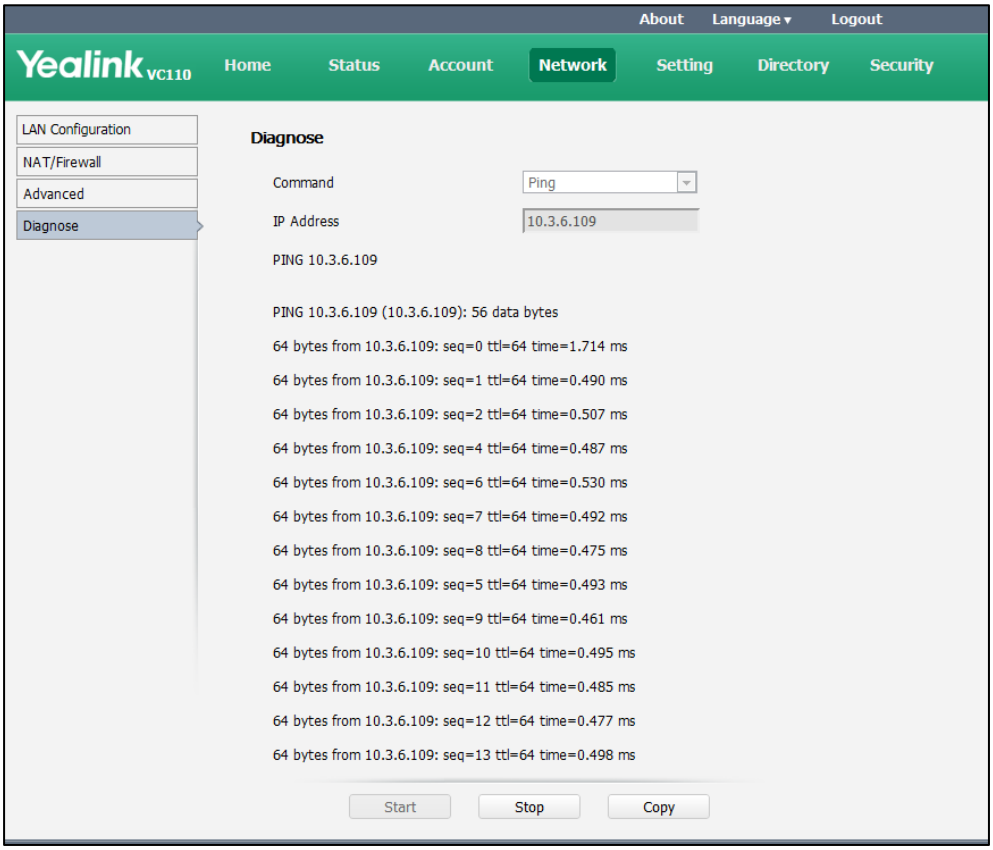
To diagnose network via the web user interface:

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



4. Click **Start** to start diagnosing.

The web page displays the diagnosis:



5. Click **Stop** to complete diagnosing.

   You can click **Copy** to copy the content to the clipboard.

Troubleshooting Solutions

This chapter provides general troubleshooting solutions to help you solve the problems you might encounter when using your endpoint.

Ensure that the endpoint has not been physically damaged when experiencing a problem. Check whether the cables are loose and the connections are correct and secure. These are common causes of problems.

If problems you encounter are not mentioned in this chapter, you can contact your distributor or Yealink FAE.

General Issues

Why is the display device black?

- Check whether the display device is connected properly to the VC110 all-in-one unit.
- Check whether the endpoint is in sleep mode. Press any key on the VCP40 phone or remote control to resume endpoint operation.
- Check whether the display device is in sleep mode or is turned off. Press the power button on the remote control or on the display device.
- Check whether you have selected the correct video input source. You can try to change video input source.

Why doesn′t the display device display time and date correctly?

- If you have configured the endpoint to obtain the time and date from the NTP server automatically, ensure that SNTP server and time zone are configured correctly in the endpoint and whether the connection between the endpoint and NTP server is working properly.
- If you have configured the endpoint to obtain the time and date manually, ensure that you have configured the time and date correctly.

Why doesn′t the remote control work?

- Check whether the endpoint is powered on.
- Check whether the positive and negative charges of the battery are connected correctly.
- Check whether the battery has sufficient power left.
- Check whether no special fluorescent or neon signs nearby.

Why does the endpoint fail to call the far site?

- Check whether the network of the near site is available.
- Check whether the network of the far site is available.
- Check whether the far site enables the DND feature.
- Check whether the accounts have been registered correctly, and the endpoint uses the appropriate account to call the far site.
- Ensure that the number you are calling is correct.

- Check whether the far site rejects your call.
- Check whether the firewall blocks the inbound traffics from the other site.
- Check whether the far site has already up to maximum call-in limitation.
- If the near site is forced to use encryption, ensure that the far site enables encryption too. For more information on call encryption, refer to Secure Real-Time Transport Protocol on page 185 and H.235 on page 188.
- Ensure that the far site supports the same call protocol as the near site.

Why does the endpoint fail to call the far site via IP address?

- Ensure that at least one call protocol is enabled on both sites. For more information, refer to Configuring SIP Settings on page 99 and Configuring H.323 Settings on page 105.
- Ensure that the network is connected correctly.
- Ensure that the network is configured correctly. For more information, refer to Configuring LAN Properties on page 50.
- Ping the IP address of the far site. Contact your system administrator if it fails. For more information, refer to Using Diagnostic Methods on page 208.

Why doesn't the status bar of the display device display IP address?

- Check whether the network is available.
- Check whether the LAN property is configured correctly. For more information on LAN property configuration, refer to Configuring LAN Properties on page 50.
- Check whether the endpoint has enabled the hide IP address feature. For more information on disabling the hide IP address feature, refer to Hide IP Address on page 135.
- Check whether the endpoint has configured firewall and NAT correctly. For more information on, refer to Configuring the Endpoint for Use with a Firewall or NAT on page 75.

Why does the network keep losing packets?

- Check whether the network is available and the LED indicator on the left of the Internet port illuminates green.
- Try to use the low speed connection to check whether packets are lost. Deficient bandwidth is an important reason for packet loss.
- Check the configuration of the network speed and duplex mode on the endpoint, switch and router.

Camera Issues

Why can´t I adjust the camera angle and focus?

- You can adjust the camera when the endpoint is idle or during a call. The camera cannot be adjusted when the endpoint is in the menu screen.
- Ensure that the batteries in the remote control are in good working condition, and installed correctly.
- Aim the remote control at the sensor when operating the unit.
- Ensure that no objects are obstructing the sensor on the front of the camera.
- Ensure that the LED on the front of the camera flashes green when you use the remote control to operate the unit.
- Ensure that what you are controlling is the local camera.
- Reboot the endpoint.
- If the above suggestions cannot solve your problem, perhaps the remote control is broken. You can contact your endpoint administrator for help.

Why can´t adjust the remote camera during an active call?

- Use the remote control to control the local camera to check whether the remote control can be used normally.
- Ensure that the far site has enabled the far-end camera control feature. For more information, refer to Far-end Camera Control on page 151.
- Ensure that what you are controlling is the remote camera. Select **More**->**Near/Far Camera** during an active call and then select the remote video image.
- Ensure that the far site supports the same call protocol as the near site. For more information, refer to Camera Control Protocol on page 153.

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information on packet loss, refer to Viewing Call Statistics on page 208.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

Video & Audio Issues

Why can' t I hear the audio during a call?

- Ensure that the local audio output device is connected correctly.
- Use audio diagnose to check whether the audio device is working normally.
- Ensure that the ringer volume is not set to the minimum.
- Check whether the far site is muted.

Why can' t the far site hear the local audio?

- Ensure that the local audio input device is connected correctly.
- Check whether the near site is muted.
- Check whether the endpoint has enabled the auto answer mute feature.

Why can' t I hear the other site clearly during a call?

- Ensure that the speaker volume of the far site is not set too low.
- Muffled audio reception from the far side may be caused by highly reverberant rooms. Speak in close proximity to the phone.
- Adjust the priority order for your audio codec if you have chosen a low-bandwidth audio codec to be first. For more information, refer to Codecs on page 112.
- For best results, ensure that the caller is using a Yealink VC110 video conferencing endpoint. Audio quality from your VC110 video conferencing endpoint will vary when calling a non-Yealink endpoint. For more information, refer to Video Size Mode on page 121.
- Dust and debris may cause audio quality. Do not use any kind of liquid or aerosol cleaner on the phone. A soft, slightly damp cloth should be sufficient to clean the top surface of the phone if necessary.

Why is the voice quality poor?

Users may receive poor voice quality during a call, such as intermittent voice, low volume, echo or other noise. It is difficulty to diagnosis the root causes of the voice anomalies. The possible reasons are:

- Users sit too far from or near to the microphone.
- The audio pickup device is moved frequently.
- Intermittent voice is probably caused by voice packet loss or jitter. Voice packet

loss may occur due to network congestion. Jitter may occur due to information reorganization of the transmission or receiving equipment, such as, delay processing, retransmission mechanism or buffer overflow.

- Noise devices, such as computers or fans, may make it difficult to hear each other's voices clearly.
- Wires may also cause this problem. Replace the old with the new cables, and then reconnect to check whether the new cables provide better connectivity.

Why can´t I view the local video image?

- Check whether the near site camera is connected to the VC110 all-in-one unit correctly.
- Check whether camera is powered on, and the LED indicator illuminates green.
- Check whether the camera is selected for the current video input source.
- Check the screen layout to see whether the remote video image is shown in full size.

Why can´t I view the menu?

- Check whether the Display1 port of VC110 all-in-one unit is connected to the HDMI port on the display device.

Why can´t I start presentation?

- Check whether a PC is connected to the VC110 all-in-one unit.
- Check whether the PC is sending a signal.
- Check the call statistics to see whether the endpoint is sharing content.
- Ensure that dual-stream is configured correctly. For more information, refer to Dual-Stream Protocol on page 145.

Endpoint Maintenance

How to prevent monitor burn-in?

Refer to your monitor's documentation for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Ensure that static images are not displayed for long periods.
- Be aware that meetings that last more than an hour without much movement can

have the same effect as a static image.

- Configure the automatic sleep time to be 1 hours or less.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

How to reboot the endpoint?

When you do one of the following, the endpoint will reboot:

- Reboot endpoint
- Reset endpoint
- Upgrade firmware
- Configure some features need to take effect after a reboot

You can reboot the endpoint in the following ways:

- Select **Menu**->**Advanced (default password: 0000)** ->**Reboot & Reset**->**Reboot**, and then press (OK).
- Log into web user interface and click on **Setting**->**Upgrade**->**Reboot,** and then click **Confirm**.

Why does the endpoint fail to upgrade?

- Ensure that the firmware is different from the firmware currently in use.
- Ensure that the downloaded firmware applies to the endpoint.
- Ensure that the endpoint is powered on normally, and the network is available during the upgrade process.
- When upgrading firmware via the web user interface, ensure that the web user interface is not refreshed or closed during the upgrade process.

Appendix

Appendix A: Time Zones

Time Zone	Time Zone Name
−11:00	Samoa
−10:00	United States-Hawaii-Aleutian
−09:30	French Polynesia
−09:00	United States-Alaska Time
−08:00	Canada(Vancouver, Whitehorse)
−08:00	Mexico(Tijuana, Mexicali)
−08:00	United States-Pacific Time
−07:00	Canada(Edmonton, Calgary)
−07:00	Mexico(Mazatlan, Chihuahua)
−07:00	United States-Mountain Time
−07:00	United States-MST no DST
−06:00	Canada-Manitoba(Winnipeg)
−06:00	Chile(Easter Islands)
−06:00	Mexico(Mexico City, Acapulco)
−06:00	United States-Central Time
−05:00	Bahamas(Nassau)
−05:00	Canada(Montreal, Ottawa, Quebec)
−05:00	Cuba(Havana)
−05:00	United States-Eastern Time
−04:30	Venezuela(Caracas)
−04:00	Canada(Halifax, Saint John)
−04:00	Chile(Santiago)
−04:00	Paraguay(Asuncion)
−04:00	United Kingdom-Bermuda(Bermuda)
−04:00	United Kingdom(Falkland Islands)
−04:00	Trinidad&Tobago
−03:30	Canada- New Foundland(St.Johns)
−03:00	Denmark-Greenland(Nuuk)
−03:00	Argentina(Buenos Aires)
−03:00	Brazil(no DST)
−03:00	Brazil(DST)
−02:30	Newfoundland and Labrador
−02:00	Brazil(no DST)
−01:00	Portugal(Azores)
0	GMT

Time Zone	Time Zone Name
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+02:00	Syria(Damascus)
+03:00	East Africa Time
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)

Time Zone	Time Zone Name
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)
+04:30	Afghanistan(Kabul)
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+05:45	Nepal(Katmandu)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+06:30	Myanmar(Naypyitaw)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+08:00	Russia(Irkutsk, Ulan-Ude)
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:00	Russia(Yakutsk, Chita)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+11:00	Russia(Srednekolymask Time)
+11:00	Norfolk Island
+12:00	New Zealand(Wellington, Auckland)
+12:00	Russia(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)
+13:00	Tonga(Nukualofa)
+13:30	Tonga Chatham Islands
+14:00	Kiribati

Appendix B: Trusted Certificates

Yealink IP phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA - G1 (EV)
- Thawte Primary Root CA - G2 (ECC)
- Thawte Primary Root CA - G3 (SHA256)
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Universal Root Certification Authority

Note Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to Transport Layer Security on page 178.

Index

Numeric

802.1x Authentication 66

A

About This Guide v
Auto Answer 116
Auto Refuse Timeout 123
Automatic Sleep Time 134
Audio Output Device 138
Audio Input Device 140
Adjusting MTU of Video Packets 143
Administrator Password 174
Attack Defense in Public Network 189
Analyzing Configuration Files 207
Appendix A: Time Zones 217
Appendix B: Trusted Certificates 220

B

Backlight of VCP40 Conferencing Phone 126
Bandwidth 119

C

Configuring Network 49
Configuring LAN Properties 50
Configuring Network Settings Manually 55
Configuring Network Speed and Duplex Mode 57
Configuring the Endpoint for Use with a Firewall or NAT 75
Configuring Call Preferences 99
Configuring SIP Settings 99
Configuring H.323 Setting 104
Codecs 109
Call Type 113
Call Match 117
Configuring Endpoint Settings 125
Configuring Camera Settings 147
Camera Control Protocol 153
Call History 166
Configuring Security Features 173
Configuring Packets 204
Camera Issues 213

D

DHCP 50
Do Not Disturb 114
Dual-Stream Protocol 145
Dual Screen 169

F

Far-end Camera Control 151

G

Getting Started 35
Getting Information from Status Indicators 207
General Issues 211

H

H.323 Tunneling 71
H.460 Firewall Traversal 88
History Record 118
Hide IP Address 135
H.235 188

I

In This Guide v
Icon on Display Device 29
Icon on VCP40 Video Conferencing Phone 31
Intelligent Firewall Traversal 90
Importing/Exporting Configuration 194
Index 222

K

Key Tone 137

L

LED Instructions 31
LLDP 60
Language 127
Local Directory 159
LDAP 162

M

Mix Sending146

N

NAT 78

P

Packaging Contents 3
Powering the Endpoint On and Off 41
Placing a Test Call from the Yealink Video Conferencing Endpoint 47
Preparing the Network 49

Q

Quality of Service 91

R

Reserved Ports 75
Ringback Timeout 123
Remote Control 133
Relog Offtime 136
Resetting to Factory 194

S

Endpoint Component Instructions 3
Endpoint Installation 41
Endpoint Startup 43
Setup Wizard 43
Site Name 125
Search Source List in Dialing 168
Secure Real-Time Transport Protocol 185
SNMP 196
Endpoint Maintenance Issues 215

T

Table of Contents vii
Time and Date 127
Tones 154
Transport Layer Security 178
Troubleshooting 201
Troubleshooting Methods 201
Troubleshooting Solutions 208

U

User Interfaces 31
User Mode 173
Upgrading Firmware 193
Using Diagnostic Methods 208

V

VC110 Video Conferencing Endpoint
Introduction 1
VoIP Principles 1
VC110 All-in-One Unit 7
VCP40 Video Conferencing Phone 7
VCM60Video Conferencing Wireless Microphone 11
VCR10 Remote Control 24
VCM30 Video Conferencing Microphone Array 24
VLAN 59
VPN 94
Video Size Mode 121
Viewing Log Files 201
Viewing Call Statistics 208
Video & Audio Issues 214

W

Web User Interface 33
Web Server Type 176