

**HUAWEI TE80 Videoconferencing Endpoint
V100R001C01
Administrator Guide**

Issue 02
Date 2014-01-15

Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://enterprise.huawei.com>

About This Document

Before you use the product, refer to the product vendor for version mapping information and to confirm compatibility with other videoconferencing equipment.

This document describes how to install, configure, maintain, and troubleshoot the HUAWEI HUAWEI TE80 Videoconferencing Endpoint (TE80 or endpoint for short). It also provides step-by-step instructions on conferencing tasks.






Intended Audience

This document is intended for but not limited to endpoint administrators.

An endpoint administrator has access to all functions on the endpoint web interface and remote controlled user interface (UI).

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 02 (2014-01-15)

This issue is the second official release, which incorporates the following changes:

Modified section 3.1.2 "Setting IP Parameters."

Modified section 3.1.3 "Setting H.323 Parameters."

Modified section 3.1.5 "Setting Wi-Fi Parameters."

Modified section 4.2.1 "Configuring Video Output."

Modified section 4.2.4 "Setting Video Parameters."

Modified section 4.2.5 "Switching Between Screen Layouts."

Modified section 4.6 "Setting Camera Presets."

Modified section 5.1.3 "Setting Audio Parameters."

Modified section 5.4 "Adjusting Audio Effects."

Modified section 6.1 "Designating the Dual Streams."

Modified section 7.1 "Setting the Administrator Password."

Modified section 8.1 "Customizing the Home Screen."

Modified section 8.4 "Customizing the Option Bar."

Modified section 9.2 "Logging In to the Endpoint Web Interface."

Modified section 9.3.3 "Downloading an Air Content Sharing Client."

Added section 13.7 "Setting Network Diagnostics Parameters."

Issue 01 (2013-09-30)

This issue is the first official release.

Contents

About This Document	ii
1 Overview	1
1.1 Definition of an Endpoint Administrator	2
1.2 Requirements for an Endpoint Administrator	2
1.3 Related Documentation.....	错误! 未定义书签。
1.4 Safety Precautions	3
1.5 How to Obtain Help.....	9
2 Basic Configuration and Verification	10
2.1 Powering On or Off the Endpoint	10
2.2 Using the Wizard	12
2.3 Verifying the Basic Configuration	13
2.3.1 Call Test	13
2.3.2 Sound Test	14
2.3.3 Image Test.....	14
2.4 Power Management	15
3 Network	18
3.1 Connecting to an IP LAN Network.....	18
3.1.1 Checking Status Indicators of the LAN Port	18
3.1.2 Setting IP Parameters	19
3.1.3 Setting H.323 Parameters	22
3.1.4 Setting SIP Parameters.....	24
3.1.5 Setting Wi-Fi Parameters	27
3.2 Connecting to a 4E1 Network.....	31
3.2.1 Inserting a 4E1 Interface Card	31
3.2.2 Checking Status Indicators on the 4E1 Ports	33
3.2.3 Setting 4E1 Parameters.....	33
4 Display Device and Camera	35
4.1 Connecting a Display Device	35
4.2 Configuring a Display Device	39
4.2.1 Configuring Video Output	39
4.2.2 Adjusting the Picture Offset.....	44

4.2.3 Adjusting the Sampling Phase	44
4.2.4 Setting Video Parameters	45
4.2.5 Switching Between Screen Layouts.....	47
4.3 Connecting a Camera.....	48
4.4 Configuring Video Input	49
4.5 Selecting and Controlling a Camera	51
4.6 Setting Camera Presets	52
5 Microphone and Speaker	54
5.1 Connecting an Audio Input Device.....	54
5.1.1 Connecting a VPM220.....	55
5.1.2 Connecting a VPM220W	57
5.1.3 Setting Audio Parameters.....	59
5.2 Connecting an Audio Output Device	62
5.2.1 Connecting a Speaker	62
5.2.2 Placing an External Speaker	62
5.2.3 Adjusting the Speaker Volume	62
5.3 Connecting a Tuning Console.....	62
5.4 Adjusting Audio Effects.....	62
5.5 Enjoying Stereo Audio.....	64
6 Conference.....	65
6.1 Experiencing a Dual-Stream Conference.....	66
6.1.1 Designating the Dual Streams.....	66
6.1.2 Sharing a Presentation	67
6.1.3 Viewing the Combined Picture of the Presentation and the Video	67
6.2 Experiencing an MSUC Conference.....	68
6.3 Joining an Authentication Conference	70
6.4 Joining an HD-Video Conference over an IMS Network	72
6.5 Scheduling a Conference	75
6.6 Controlling a Conference.....	75
6.6.1 Conference Control for a Non-Chair Site	76
6.6.2 Conference Control for the Chair Site	77
6.7 Recording a Conference.....	80
6.8 Managing the Address Book.....	81
6.8.1 Configuring the Network Address Book.....	81
6.8.2 Managing the Local Address Book.....	84
6.8.3 Importing and Exporting an Address Book.....	86
6.8.4 Customizing a Site Template	87
6.9 Managing Captions	89
6.9.1 Specifying Caption Settings.....	89
6.9.2 Creating a Banner or Caption	91
7 Security.....	92

7.1 Setting the Administrator Password.....	92
7.2 Enabling Encryption.....	93
7.3 Supporting Remote Logins.....	94
7.4 Setting the Upgrade Password.....	96
7.5 Setting the Air Content Sharing Password.....	96
8 Screen Customization.....	98
8.1 Customizing the Home Screen.....	98
8.2 Customizing Onscreen Status Icons.....	100
8.3 Customizing Conference Control Functions to Be Displayed.....	100
8.4 Customizing the Option Bar.....	101
9 Embedded Web Management Interface.....	102
9.1 Web Browser.....	103
9.2 Logging In to the Endpoint Web Interface.....	104
9.3 Getting to Know Web Interface Functions.....	105
9.3.1 Importing and Exporting Settings.....	105
9.3.2 Importing License Files.....	106
9.3.3 Downloading an Air Content Sharing Client.....	106
9.3.4 Multi-View.....	108
9.3.5 Customizing Shortcut Bar and Desktop Icons.....	109
9.3.6 Accessing the Site Map.....	109
9.3.7 Importing a Certificate.....	109
9.3.8 Monitoring the Video.....	110
9.3.9 Using the Virtual Remote Control.....	110
10 Maintenance.....	111
10.1 Checking the Working Environment Periodically.....	111
10.2 Checking the Endpoint Periodically.....	112
10.3 Viewing System Status.....	112
10.4 Querying System Information.....	113
10.5 Querying Logs.....	113
11 Upgrading.....	115
11.1 Automatic Upgrade.....	116
11.2 Tool Upgrade.....	117
11.3 Upgrading the Endpoint Using the Bootrom System.....	120
11.4 Upgrading the Endpoint on Its Web Interface.....	121
12 Troubleshooting.....	122
12.1 Fault Diagnostics.....	122
12.2 Troubleshooting.....	125
12.3 Restoring Default Settings.....	135
13 Feature Configuration.....	136



13.1 Setting the Number Keys and Power Key on the Remote Control	137
13.2 Setting the Parameters for Placing and Answering Calls	137
13.3 Setting Advanced Conference Parameters	139
13.4 Setting SNMP Parameters.....	143
13.5 Setting QoS Parameters	145
13.6 Setting Network Diagnostics Parameters.....	147
13.7 Setting Network Diagnostics Parameters.....	148
14 Ports on the Rear Panel	151
A E1 and T1 Grounding Criteria	152
B Technical Specifications	153
C Status Icons.....	157
D Menus.....	160
E Terminology	162
F Acronyms and Abbreviations.....	168

1 Overview

About This Chapter

This document guides you through configuring, managing, maintaining, and troubleshooting the endpoint.

When using this document, note the following:

- Unless otherwise specified, the descriptions in this document are applicable to the TE80.
- Except chapters [9 Embedded Web Management Interface](#), [10 Maintenance](#), [12 Troubleshooting](#) and [13.4 Setting SNMP Parameters](#) which apply to the endpoint web interface, descriptions and configurations in this document apply to the endpoint user interface controlled by the remote control (remote controlled UI for short).
- To access the menu screen, press  on the remote control. You can find the option bar on the left of the menu screen. This option bar is configurable and is your interface for all functions except calling. For details about how to configure the option bar, see [8.4 Customizing the Option Bar](#).
- To prevent endpoint parameters from being modified by unauthorized users, anyone who wants to access the **Settings** screen and use the customized tool bar  on the menu screen must provide the administrator password if the password is not set to blank. For details about how to set the password, see [7.1 Setting the Administrator Password](#).

1.1 Definition of an Endpoint Administrator

An endpoint administrator is an enterprise employee who is responsible for managing and maintaining endpoint operations.

1.2 Requirements for an Endpoint Administrator

As an endpoint administrator, you must meet the following basic endpoint administrator proficiencies and be capable of collecting all information related to the endpoint and its working environment.

1.3 Related Documentation

This section lists the documentation that you may refer to when you perform routine operations and maintenance as well as answering questions from standard users.

1.4 Safety Precautions

For safety purposes, carefully read through these safety precautions and observe them during operation.

1.5 How to Obtain Help

When you encounter an endpoint issue, use the help on the endpoint web interface or contact technical support personnel.

1.1 Definition of an Endpoint Administrator

An endpoint administrator is an enterprise employee who is responsible for managing and maintaining endpoint operations.

An endpoint administrator has the following job responsibilities:

- Configures and manages the endpoint.
- Routinely maintains the endpoint.
- Troubleshoots the endpoint failures.
- Answers standard users' questions about endpoint use.

1.2 Requirements for an Endpoint Administrator

As an endpoint administrator, you must meet the following basic endpoint administrator proficiencies and be capable of collecting all information related to the endpoint and its working environment.

Basic Endpoint Administrator Proficiencies

- Windows operating system
- Gatekeeper (GK) and Session Initiation Protocol (SIP) servers
- Ethernet, TCP/IP, and Client/Server (C/S) model
- H.323, SIP, and H.320 protocols
- Safe and effective use of electronic devices
- Common maintenance tools
- Videoconferencing endpoint functions and services

Information About the Endpoint and Its Working Environment

Table 1-1 lists the endpoint and working environment information that must be collected, which helps you fulfill your job responsibilities and check the preparations for a recovery from an emergency.

Table 1-1 Information to be collected

Category	No.	Item	Description
Device information	1	Device location	Record the endpoint location in as much detail as possible so the endpoint can be quickly

Category	No.	Item	Description
			located.
	2	Networking condition	Record the network topology and hardware connection diagram that include every device.
	3	Endpoint information	List the IP address, user name, and password for the endpoint so you can quickly log in to the endpoint in case of an emergency. If you are not permitted to record the password for security reasons, memorize it.
Software and tools	4	Software versions and tools	List the software versions corresponding to the endpoint. Prepare troubleshooting tools.
Contact information	5	Purchased parts' service information	Record the manufacturer contact information, serial numbers, and manufacturers' warranty clauses for purchased parts.
	6	Technical support personnel's contact information	Maintain a list of technical support personnel with their contact information and responsibilities.
Spare parts	7	Spare parts	List all spare parts (including the spare parts that Huawei can provide) and corresponding procurement methods.
	8	Redundant or temporary devices	List all redundant or temporary devices in the system, such as standby file servers and database servers.

1.3 Safety Precautions

For safety purposes, carefully read through these safety precautions and observe them during operation.

Basic Precautions

- Keep the device dry and secure from collision during storage, transportation, and operation of the device.

- Do not attempt to dismantle the device by yourself. In case of any fault, contact the appointed maintenance center for assistance or repair.
- Without prior written consent, no organization or individual is permitted to make any change to the structure or safety and performance design of the device.
- While using the device, observe all applicable laws, directives, and regulations, and respect the legal rights of others.

Environmental Precautions

- Place the device in a well-ventilated place. Do not expose the device to direct sunlight.
- Install the device strictly according to the requirements of the manufacturer.
- Do not place any object on the top of the device. Reserve a minimum space of 10 cm at the four sides of the device for heat dissipation.
- Do not place the device on or near inflammable materials such as foam.
- Keep the device away from heat source or fire, such as a radiator or a candle.
- Keep the device away from any household appliances with strong electromagnetic fields, such as a microwave oven, refrigerator, or mobile phone.

Operating Precautions

- Do not allow children to play with the device or accessories. Swallowing the accessories may be fatal.
- Use the accessories such as the power adapter and battery provided or authorized only by the manufacturer.
- Ensure that the device does not get wet. If water gets into the device, disconnect the power supply immediately and unplug all the cables connected to the device, including the power cable, telephone cable, video cable, audio cable, network cable, and serial cable, and then contact the appointed maintenance center.
- Before plugging or unplugging any cable, shut down the device and disconnect the power supply. While plugging or unplugging any cable, ensure that your hands are dry.
- Do not step on, pull, or overbend any cable. Otherwise, the cable may be damaged, leading to malfunction of the device.
- Do not use old or damaged cables.
- In lightning weather, disconnect the device from the power supply and unplug all the cables connected to the device.
- Keep the power plug clean and dry, to prevent electric shock or other dangers.
- If the device is not used for a long time, disconnect the power supply and unplug the power plug.
- If smoke, sound, or smell is emitted from the device, stop using the device immediately, disconnect the power supply, unplug the power plug and other cables, and remove the batteries. Then, contact the appointed maintenance center for repair.
- Ensure that no object (such as metal shavings) enters the device through the heat dissipation vent.
- Before connecting any other cable, connect the ground cable of the device. Do not disconnect the ground cable until you have disconnected all the other cables.
- Ensure that the three-phase power socket is grounded properly. The neutral line and the live line cannot be connected inversely.

- Do not scratch or abrade the shell of the device. The shed painting may lead to skin allergy or malfunction of the device. If the shed painting material drops into the host, a short circuit may occur.

Cleaning Precautions

- Before cleaning the device, stop using it, disconnect the power supply, and unplug all the cables connected to the device, including the power cable, telephone cable, video cable, audio cable, network cable, and serial cable.
- Do not clean the device shell with any cleaning solution or cleanser spray. Use a piece of soft cloth to clean the device shell.

Battery Usage Precautions of the Remote Control

- Use only the recommended battery. Pay attention to the polarity of the batteries while installing them.
- If a battery does not fit in the device, do not apply force. Otherwise, the battery may leak or explode.
- To reduce the risk of explosion, do not use batteries of different types together. For example, do not use an alkaline battery and a Mn-Zn battery together. It is recommended that you use batteries provided or recommended by the manufacturer.
- Do not use a new battery with an old battery. When you replace batteries, replace all of them at the same time.
- If you are not going to use the device for a long time, remove all the batteries.
- If any battery leaks, emits smoke, or emits abnormal smell, stop using it immediately.
- If the battery fluid comes in contact with your skin or clothes, rinse with water immediately and seek medical assistance.
- If the battery fluid goes into your eyes, do not rub your eyes. Rinse your eyes with water immediately and seek medical assistance.

LCD Usage Precautions

- Do not expose the LCD to direct sunlight.
- Do not scratch or strike, apply force to, or place heavy objects on top of the LCD.
- Do not watch the LCD screen for extended periods of time. This may harm your eyes or blur your vision.

LCD Cleaning Precautions

- According to the instructions in the attached manual, use a piece of soft cloth to remove dust from the surface of the LCD.
- Do not clean the LCD with volatile solvents, such as alcohol, benzene, or a dilution agent. Do not keep the LCD in contact with a rubber or plastic materials for long periods of time. This will deteriorate the surface gloss of the LCD.

Wireless Product Usage Precautions

- Keep the wireless device away from magnetic storage devices, such as a magnetic card or a floppy disk to prevent loss of the stored information.
- Stop using the wireless device and disconnect it from the power supply in places where using of wireless devices is prohibited or using of a wireless device may lead to interference or danger.

- Unplug the wireless device from the endpoint and turn off the endpoint close to a high-precision controlled electronic device, such as an audio phone, a pacemaker, fire alarm, or an automatic gate. Otherwise, this will lead to malfunction of the electronic device.
- The user who uses an electronic assistant medical-treatment device needs to confirm with the service center regarding the effects of the radio wave on this device.
- Do not take the wireless device to the operation theater, Intensive Care Unit (ICU), or the Coronary Care Unit (CCU).
- When using the device, ensure that the antenna of the device is at least 20 cm away from all parts of your body.
- In the area with inflammable or explosive materials, turn off your wireless device and follow the relevant instructions given on the label to prevent an explosion or fire.
- Use your wireless device and its accessories in a clean and dust-free environment. Ensure that the wireless device does not come in contact with flame or a lit cigarette.
- Ensure that the wireless device and its accessories are dry.
- Do not drop, throw, or bend your wireless device.
- Do not place the wireless device and its accessories in areas with extreme temperatures.

Reduction of Hazardous Substances

This device is compliant with the EU Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation (Regulation No 1907/2006/EC of the European Parliament and of the Council) and the EU Restriction of Hazardous Substances (RoHS) Directive (Directive 2002/95/EC of the European Parliament and of the Council). For more information about the REACH compliance of the device, visit the website www.huaweidevice.com/certification. You are recommended to visit the website regularly for up-to-date information.

Statement on a Class A Product

This is a class A product. In a national environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Regulatory Compliance

The endpoint complies with the following European directives and regulations.

- 1999/5/EC (R&TTE)
- 2002/95/EC & 2011/65/EU (RoHS)
- EC NO. 1907/2006 (REACH)
- 2002/96/EC (WEEE)

The endpoint complies with Directive 2002/95/EC, 2011/65/EU and other similar regulations from the countries outside the European Union, on the RoHS in electrical and electronic equipment. The endpoint does not contain lead, mercury, cadmium, and hexavalent chromium and brominated flame retardants (Polybrominated Biphenyls (PBB) or Polybrominated Diphenyl Ethers (PBDE)) except for those exempted applications allowed by RoHS directive for technical reasons.

The endpoint complies with Regulation EC NO. 1907/2006 (REACH) and other similar regulations from the countries outside the European Union. Huawei will notify to the European Chemical Agency (ECHA) or the customer when necessary and regulation requires.

The endpoint complies with Directive 2002/96/EC on waste electrical and electronic equipment (WEEE). Huawei is responsible for recycling its end-of-life devices, and please contact Huawei local service center when recycling is required. Huawei strictly complies with the EU Waste Electrical and Electronic Equipment Directive (WEEE Directive) and electronic waste management regulations enacted by different countries worldwide. In addition, Huawei has established a system for recycling and reuse of electronic wastes, and it can provide service of dismantling and recycling for WEEE. By Huawei recycling system, the waste can be handled environmentally and the resource can be recycled and reused fully, which is also Huawei WEEE stratagem in the word. Most of the materials in the endpoint are recyclable, and our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

In accordance with Article 11(2) in Directive 2002/96/EC (WEEE), The endpoints were marked with the following symbol: a cross-out wheeled waste bin with a bar beneath as below:



FCC Part 15

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

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

If this device is modified without authorization from Huawei, the device may no longer comply with FCC requirements for Class A digital devices. In that a case, your right to use the device may be limited by FCC regulations. Moreover, you may be required to correct any interference to radio or television communications at your own expense.



CAUTION

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.



NOTICE

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the device is operated in a commercial environment.

This device generates, uses and radiates radio frequency energy. If it is not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

Operation of this device in a residential area is likely to cause harmful interference. In this case the user will be requested to correct the interference at his or her own expense.

Canada Regulatory Compliance

- RSS-Gen statement

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- RSS-210 statement:

This device complies with Industry Canada RSS-210. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio RSS-210. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- RSS-102 statement:

The device meets the exemption from the routine evaluation limits in section 2.5 of RSS 102 and compliance with RSS-102 RF exposure, users can obtain Canadian information on RF exposure and compliance.

Le dispositif rencontre l'exemption des limites courantes d'évaluation dans la section 2.5 de RSS 102 et la conformité à l'exposition de RSS-102 rf, utilisateurs peut obtenir l'information canadienne sur l'exposition et la conformité de rf.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Cet équipement est conforme à l'exposition aux rayonnements IC limites établies pour un environnement non contrôlé. Cet émetteur ne doit pas être Co-placé ou fonctionnant en même temps qu'aucune autre antenne ou émetteur. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre le radiateur et votre corps.

1.4 How to Obtain Help

When you encounter an endpoint issue, use the help contact technical support personnel.

Obtaining Technical Support

The Huawei support website is an efficient and real-time communication platform where you can obtain technical documents, submit technical questions, service requests, and troubleshooting questions, and provide feedback on Huawei products. To seek technical help over the Internet, please visit <http://enterprise.huawei.com>.

Provide the following information to help Huawei engineers answer your questions:

- Endpoint serial number (To view this number, choose **Advanced > Diagnostics > System Information > Version.**)
- Software version (To view this information, choose **Advanced > Diagnostics > System Information > Version.**)
- Network information (To view this information, choose **Advanced > Diagnostics > Status > Line Status.**)
- Diagnostic and troubleshooting measures you have taken

2 Basic Configuration and Verification

About This Chapter

Before using the endpoint, you must complete basic endpoint configuration, such as setting basic endpoint information and network parameters, and verify the configuration.

[2.1 Powering On or Off the Endpoint](#)

After connecting all the required devices, connect the power supply and then power on the endpoint.

[2.2 Using the Wizard](#)

The Wizard helps you quickly set the general, network, and camera parameters on your endpoint.

[2.3 Verifying the Basic Configuration](#)

After completing the basic configuration, you must verify it by performing call, sound, and image tests.

[2.4 Power Management](#)

The endpoint supports sleep mode. You can set its sleep time and automatic startup and shutdown time.

2.1 Powering On or Off the Endpoint

After connecting all the required devices, connect the power supply and then power on the endpoint.



NOTICE


- When the endpoint is powered on, ensure that the power cable is connected to the endpoint securely to prevent power disconnection.
- Before disconnecting the external power supply (for example, the power supply from a power socket), power off the endpoint properly.

Check whether the power cable and the power adapter are connected to the relevant devices properly. Ensure that:

- The voltage of the alternating current ranges from 100 V to 240 V and the frequency of the alternating current ranges from 50 Hz to 60 Hz.
- The sequence of and voltage difference between the live wire, neutral wire, and ground cable comply with the relevant international standards. In addition, ensure that the ground cable is properly grounded.

To power on the endpoint, slide the power switch on the rear panel to the ON position.

To power off the endpoint, perform either of the following operations:

- Press  on the remote control. Confirm the power-off action in the displayed dialog box.
- Slide the power switch on the rear panel to the OFF position.



NOTE

When the endpoint is powered off using the remote control, the indicator on the front panel turns orange, but the power switch on the rear panel is still in the ON position. To power on the endpoint again, press



on the remote control.

Depending on the endpoint's status, the indicators on the front panel may blink in different colors and at different rates, as listed in [Table 2-1](#) and [Table 2-2](#).

Table 2-1 Status indicator description


When the Status Indicator Is...	The Endpoint Is...
Blinking blue twice per second	Starting.
Steady blue	Working properly.
Blinking purple once every 2 seconds	In sleep mode.
Steady purple	Powered off (the power switch is ON, and the endpoint is powered off by pressing  on the remote control).
Blinking blue once	Responding to a remote control operation.
Blinking blue four times per second	Being updated.

Table 2-2 Alarm indicator description

When the Alarm Indicator Is...	The Endpoint Is...
Blinking red twice per second	Overheated.
Blinking red four times per second	Encountering a temperature fault. For example, the temperature sensor inside the endpoint cannot sense the current operating temperature, causing fast fan rotation speed and loud fan noise.

2.2 Using the Wizard

The Wizard helps you quickly set the general, network, and camera parameters on your endpoint.

Background

When configuring the endpoint for the first time, you can connect to the NMS server to configure the endpoint. If the NMS server has not been configured or obtaining the NMS server settings times out, perform the steps in this section to set the required parameters.

If a USB flash drive is provided with your endpoint, you can also load the configuration file from the USB flash drive to configure your endpoint.

Procedure

Step 1 Choose **Advanced > Settings > Installation > Wizard**.

The **General** screen is displayed.

Step 2 Set the general parameters described in [Table 2-3](#) and [Table 3-3](#).

Table 2-3 General parameters

Parameter	Description	Setting
Sites	Specifies the name of your site. The site name is superimposed on the local video. When your site joins a multipoint conference, this site name is displayed in the site list.	Default value: site
Language	Specifies the language for the remote controlled UI.	Default value: English
Time zone	Specifies the time difference between the local time and the Greenwich Mean Time (GMT). The endpoint automatically sets this parameter based on the country or region	Default value:

Parameter	Description	Setting
	where your site is located.	
Time format	Specifies the format in which time is displayed.	Default value: 24-hour
System time	Specifies the system time.	Set the system time to your local time to ensure appropriate use of system functions, such as joining conferences on time and recording accurate event occurrence time in logs.

Step 3 Select **Next**, Set the H.323 parameters described in [Table 3-4](#).

Step 4 Select **Next**. Set the Session Initiation Protocol (SIP) parameters described in [Table 3-5](#).

Step 5 Select **Next**. Set the video input parameters described in [Table 4-14](#).

Step 6 Select **Save**.

----End


2.3 Verifying the Basic Configuration

After completing the basic configuration, you must verify it by performing call, sound, and image tests.

2.3.1 Call Test

By performing a call test, you can check whether the network is functioning and whether the endpoint has registered with the GK or SIP server.

Procedure

Step 1 Press  on the remote control.

The call screen is displayed.

Step 2 In the text box, enter the IP address or number of a remote site.

Step 3 On the remote control, press  or **OK** to place a call to the remote site.

----End



NOTE

If you have selected the **Enable GK** or **Register with server** parameter and set other required

parameters but the endpoint fails to register with the GK or SIP server,



or



is

displayed in the lower right corner of the call screen.

Verification Result

- If you successfully place a call to the remote site using its IP address, the IP network is functioning properly.
- If you successfully place a call to an H.323 site, the endpoint has registered with the GK server.
- If you successfully place a call to a SIP site, the endpoint has registered with the SIP server.

2.3.2 Sound Test

By performing a sound test, you can check whether the audio input and output of the endpoint is correct.

Prerequisites

- The endpoint has been connected to an audio input device such as a microphone.
- The endpoint has been connected to an audio output device, such as a speaker, or connected to a television using an HDMI cable.

Procedure

Step 1 Choose **Advanced > Diagnostics > Sound and Color Bar Test** from the option bar.

Step 2 Select **Sound Test**.

----End

Verification Result

- If the speaker emits a "ding ding" tone when there is no audio input, the audio output of the endpoint is correct.
- If audio inputs, for example human voices, are received from the microphone and the speaker emits the voices, the audio input and output of the endpoint are correct.

2.3.3 Image Test

By performing an image test, you can check whether the video input and output of the endpoint is correct.

Prerequisites

The endpoint has been connected to video sources and a display device.

Procedure

Step 1 Choose **Advanced > Settings > Video > Common Settings > Video Input** from the option bar. Set the **Video Source** parameter to the video input ports to which video sources are connected.

Step 2 Check whether the videos from connected video sources are correctly displayed on the display device.

----End

Verification Result

This example assumes that a video source is connected to the 1 MAIN IN port on the endpoint. If the video delivered through the 1 MAIN IN port is correctly displayed on the display device after you select **1 MAIN IN**, the video input and output of the endpoint are correct.

2.4 Power Management


The endpoint supports sleep mode. You can set its sleep time and automatic startup and shutdown time.

To reduce power consumption, the endpoint can be configured to enter sleep mode after it has been in the idle state for a defined period of time.

Procedure

- Step 1** Choose **Advanced > Settings > General > Power supply**. Set the sleep and automatic startup and shutdown parameters described in [Table 2-4](#).

Table 2-4 Sleep and automatic startup and shutdown parameters

Parameter	Description	Setting
Shut Down	Specifies whether the endpoint can be powered off. If you disable this parameter, you can only restart the endpoint or place it in sleep mode by pressing  on the remote control.	The default value is Enable .
Enter sleep mode	Specifies the period after which the endpoint enters sleep mode if you do not perform any operations. If you set this parameter to Never , the endpoint will never automatically enter sleep mode.	The default value is After 10 min .
Wake-on-LAN	Specifies whether you can remotely wake up a standby or sleeping endpoint by sending Wake on LAN (WOL) messages. NOTE A standby endpoint indicates that the power switch on the endpoint's rear panel is in the ON position and that the endpoint is turned off by pressing the power key on the remote control.	This parameter is not selected by default.
Scheduled power-on	Specifies whether the endpoint automatically powers on at the	This parameter is not selected by default.


Parameter	Description	Setting
	<p>specified time.</p> <p>NOTE If you enable this function, you must also set Scheduled power-on time (hh:mm).</p>	
Scheduled power-on time	<p>Specifies the time when the endpoint automatically powers on.</p> <p>The value format depends on the value set for Time format.</p>	The default value is 0:0 , which corresponds to the 24-hour value for Time format .
Scheduled power-off	<p>Specifies whether the endpoint automatically powers off at the specified time.</p> <p>NOTE If you enable this function, you must also set Scheduled power-off time (hh:mm).</p>	This parameter is not selected by default.
Scheduled power-off time	<p>Specifies the time when the endpoint automatically powers off.</p> <p>The value format depends on the value set for Time format.</p>	The default value is 0:0 , which corresponds to the 24-hour value for Time format .

Step 2 Select Save.

The endpoint enters sleep mode, and the LED indicator blinks purple once every 2 seconds.

----End

NOTE

To directly place the endpoint in sleep mode, press  on the remote control and select **Sleep**.

Follow-up Procedure

The endpoint wakes up from sleep mode in response to any of the following conditions:

- You use the touch panel.
- An endpoint upgrade starts.
- A presentation source is connected to the endpoint.
- The camera forwards infrared signals to the endpoint.
- The WOL function is used.
- The clock matches the scheduled endpoint startup time.
- The endpoint receives a call.
- You use the remote control.
- You log in to the endpoint web interface.

When the clock matches the scheduled automatic shutdown time, the endpoint displays a dialog box and begins a 10-second countdown. If you select **No**, the endpoint will not power off. If you select **Yes**, or do not select any option within 10 seconds, the endpoint automatically powers off.

3 Network

About This Chapter

This chapter describes the hardware connection to network devices and the settings on relevant screens required when the endpoint is used in different communication networks.

3.1 Connecting to an IP LAN Network

To implement video communication over an IP local area network (LAN), you must connect the endpoint to the IP LAN.

3.2 Connecting to a 4E1 Network

Only the TE80 supports 4E1 functions. To implement video communication over a 4E1-line dedicated network, you must connect the TE80 to the network.

3.1 Connecting to an IP LAN Network

To implement video communication over an IP local area network (LAN), you must connect the endpoint to the IP LAN.

To connect to an IP LAN, use an IP network cable to connect the LAN 1 port on the endpoint's rear panel to the network port on a LAN device.

3.1.1 Checking Status Indicators of the LAN Port

The status indicators on the LAN port can quickly provide information about the current network connection.

There are two indicators working together to indicate the network connection, as shown in [Table 3-2](#).

Table 3-1 LAN status indicators of TE80

Indicator Status	Connection Status
The orange indicator blinks once at a time.	The LAN port is in 10 M network port mode.
The orange indicator blinks twice	The LAN port is in 100 M network port mode.

Indicator Status	Connection Status
at a time.	
The orange indicator blinks thrice at a time.	The LAN port is in 1000 M network port mode.
The green indicator is steady on.	The endpoint is connected to a network.
The green indicator blinks.	Data is being transmitted. The green indicator turns off each time a frame of data has been transmitted.
The green indicator is off.	No data is being transmitted or the network is not reachable.

3.1.2 Setting IP Parameters

To enable video communication over an IP LAN network, you must set the IP parameters of the endpoint, such as the DNS server address, network mode, and gateway IP address.

Procedure

Step 1 Choose **Advanced > Settings > Network > IP**. Set the parameters listed in [Table 3-3](#).

Table 3-2 IP parameters

Parameter	Description	Setting
Local IP address		
Network interface mode	<p>Specifies the working mode for the network ports on the endpoint.</p> <ul style="list-style-type: none"> • Auto detection: When accessing the network, the endpoint automatically negotiates with a remote network device to determine the optimal work mode. • 10 Mbps and half duplex: The data transmission rate is 10 Mbit/s, and data cannot be sent and received at the same time. • 10 Mbps and full duplex: The data transmission rate is 10 Mbit/s, and data can be sent and received at the same time. • 100 Mbps and half duplex: The data transmission rate is 100 Mbit/s, and data cannot be sent and received at the same time. • 100 Mbps and full duplex: The data transmission rate is 100 Mbit/s, and data can be sent and received at the 	<p>The default value is Auto detection.</p> <p>NOTE</p> <p>When you do not know the network port working mode of a remote network device, set this parameter to Auto detection. Otherwise, the endpoint may fail to access the network.</p>

Parameter	Description	Setting
	<p>same time.</p> <ul style="list-style-type: none"> • 1000Mbps and full duplex: The data transmission rate is 1000 Mbit/s, and data can be sent and received at the same time. 	
Hub network port mode	<p>The endpoint can function as a hub in this mode, enabling the devices connected to its two network ports to communicate with each other.</p> <p>When the endpoint is connected to the Internet, devices connected to the network ports on the endpoint can also access the Internet.</p>	The default value is Disable .
Connection type	<p>Specifies the mode in which the endpoint obtains an IP address.</p> <ul style="list-style-type: none"> • Static IP: The network administrator assigns an IP address to the endpoint. If you select this option, you must also set Local IP address, Subnet mask, and Gateway address. • Dynamic IP: When a DHCP server is available on the network, the endpoint automatically obtains an IP address using the Dynamic Host Configuration Protocol (DHCP). 	The default value is Static IP .
Local IP address	Specifies the endpoint IP address.	<p>The default value is 192.168.1.1</p> <p>Examples:</p> <ul style="list-style-type: none"> • IPv4: 192.168.1.10 • IPv6: 2000:0:0:0:200:55:26:1 <p>Obtain the IP address from the network administrator.</p>
Subnet mask	Specifies the subnet mask for the endpoint IP address. A subnet mask divides the IP address into a network address and a host address.	<p>The default value is 255.255.255.0</p> <p>Obtain the subnet mask from the network administrator.</p>
Gateway address	Specifies the gateway address that corresponds to the endpoint IP address.	<p>Examples:</p> <ul style="list-style-type: none"> • IPv4: 192.168.1.1 • IPv6: 2000:0:0:0:200:55:0:1 <p>Obtain the gateway address from the network administrator.</p>
IPv6	If you select IPv6, you must also set Connection type , Local IP address , Subnet prefix length , and Gateway address .	This parameter is not selected by default.

Parameter	Description	Setting
Subnet prefix length	Specifies the number of the digit 1 in a subnet mask that is converted into binary mode.	The default value is 0 .
PPPoE Dialing	Specifies whether the endpoint accesses broadband networks using dial-up connections. NOTE If you set this parameter to Enable , you must also set Dialing mode , User name , and Password .	The default value is Disable .
Dialing mode	Specifies the dial-up connection mode. The dial-up process complies with the Point-to-Point Protocol over Ethernet (PPPoE) protocol. To use a dial-up connection, in User name and Password enter the user name and password that are provided by your broadband access service provider. <ul style="list-style-type: none"> • Auto: When the endpoint starts, it automatically sets up a dial-up connection over the IP network. If the dial-up service is not free of charge, charging starts when the dial-up connection is established. • Manual: The endpoint uses the dial-up program to access To set up a PPPoE dial-up connection, choose Advanced > Utilities > PPPoE Dialing > Connect. 	The default value is Auto .
DNS server address 1 DNS server address 2 DNS server address 3	Specifies the DNS server IP address. After you set this IP address, domain names can be used for the GK server address and the SIP server address. The DNS server will translate the domain names to the IP addresses of the GK server and the SIP server.	Example: 202.98.192.67 Obtain the IP address from the network administrator.
Alternate IP address		
Alternate IP address Subnet mask	Specifies the alternate IP address of the endpoint. This IP address cannot be in the same network segment as Local IP address (described in the Local IP address section in this table) or the IP address of the gatekeeper (GK) server.	No default value is set for this parameter. Obtain the IP address from the network administrator.

Step 2 Select **Save**.

----**End**

3.1.3 Setting H.323 Parameters

The H.323 parameters must be set when the GK is used in the conference system.

Prerequisites

The GK is used in the conference system.

Context

When the GK is used in the conference system, the endpoint can be configured with a site number. Other endpoints that also have registered with the GK can then use the site number as well as the IP address to call your endpoint.



NOTE

The GK is the network isolator of the videoconferencing system and is used to manage the network bandwidth, endpoint authentication, and address translation. It enables calls to be made to fixed site names rather than changeable IP addresses.

Procedure

- Step 1** Choose **Advanced > Settings > Network > IP > H.323**, and then set the parameters listed in [Table 3-4](#).

Table 3-3 H.323 parameters

Parameter	Description	Setting
Enable GK	<p>Specifies whether the endpoint registers with the GK.</p> <ul style="list-style-type: none"> If this parameter is selected, when your endpoint starts, it registers with the specified GK. An endpoint that registers with a GK can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with GKs. A GK must be used to initiate a conference attended by IP and integrated services digital network (ISDN) sites. If this parameter is not selected, your endpoint does not register with the GK. To call another endpoint through H.323, your endpoint can only use the called endpoint's IP address. <p>NOTE If you select Enable GK, you must also set GK registration mode, Site number, H.323 ID, and Password.</p>	This parameter is not selected by default.
GK registration mode	<ul style="list-style-type: none"> Auto: Your endpoint automatically registers with an available GK on the network and obtains the GK address. Manual: You must set GK address, 	The default value is Auto .

Parameter	Description	Setting
	which specifies the GK with which you want your endpoint to register.	
GK address	Specifies the IP address or domain name of the server where the desired GK is installed. If you set this parameter to the domain name, you must enable the DNS server and set correct mapping information on the server. This parameter is mandatory only when GK registration mode is set to Manual .	Example: 192.168.1.10
Site number	Specifies the site number for your endpoint. If your endpoint registers with a GK, endpoints that also register with GKs can dial this site number to call your endpoint.	Enter a string of 1 to 32 digits. Example: 12345
H.323 ID	Specifies the name by which a GK identifies your endpoint after your endpoint registers with the GK.	The name can consist of digits, letters, and special characters, such as @ # %. Example: ab3@ For successful GK authentication, the name defined on your endpoint must be consistent with the name predefined on the GK.
Authentication user name	Specifies the user name used for H.323 authentication. This parameter is available only when encryption is enabled. To enable encryption, choose Advanced > Settings > Security > Encryption , and set Encryption to Enable .	Obtain the user name from your IP network service provider. This user name must be the same as the value of H.323 ID .
Password	Specifies the password your endpoint uses to register with a GK. The GK uses this password to authenticate your endpoint.	Obtain the password from your IP network service provider. For successful GK authentication, the password defined on your endpoint must be consistent with the password predefined on the GK.
Huawei GK	Specifies whether your endpoint uses a Huawei GK. If you do not select Huawei GK , some functions, such as Conference Control and SiteCall are unavailable on your endpoint.	This parameter is selected by default. Do not select this parameter if your endpoint needs to interwork with other manufacturers' devices.

Parameter	Description	Setting
HTTPS mode	<p>Specifies whether to upload SiteCall conference information using HTTPS encryption.</p> <ul style="list-style-type: none"> This parameter is available only when Huawei GK is selected. If this parameter is set to disabled, your endpoint will use the Transfer Control Protocol (TCP) to upload SiteCall conference information, which may be insecure. 	<p>This parameter is not selected by default.</p> <p>To improve communication security, select this parameter.</p>
Multipoint conference authentication	<p>Specifies whether to authenticate servers when the SiteCall function is used.</p> <p>This parameter is available only when HTTPS mode is selected.</p>	<p>This parameter is not selected by default.</p> <p>To improve communication security, select this parameter.</p>
Use VoIP gateway VoIP gateway address	<p>Specify whether your endpoint can place calls to the PSTN endpoints connected to the specified voice over IP (VoIP) gateway.</p> <p>If you select Use VoIP gateway, you must also set VoIP gateway address.</p>	<p>The Use VoIP gateway is not selected by default.</p>

Step 2 Select **Save**.

----End

3.1.4 Setting SIP Parameters

When the Session Initiation Protocol (SIP) is used for video communications, the SIP parameters of the endpoint, such as whether to register with the SIP server, must be set.

Prerequisites

Both parties of the conference support SIP.

Procedure

Step 1 Choose **Advanced > Settings > Network > IP > SIP**, and then set the parameters listed in [Table 3-5](#).

Table 3-4 SIP parameters

Parameter	Description	Setting
Register with server	<p>Specifies whether your endpoint registers with a SIP server.</p> <ul style="list-style-type: none"> If this parameter is selected, an endpoint that registers with a SIP 	<p>This parameter is not selected by default.</p>

Parameter	Description	Setting
	<p>server can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with SIP servers.</p> <ul style="list-style-type: none"> If this parameter is not selected, your endpoint does not register with the SIP server. To call another endpoint through SIP, your endpoint can only use the called endpoint's IP address. <p>NOTE If you select this parameter, you must also set Server address, Conference service number, Site number, User name, and Password.</p>	
Server address	<p>Specifies the IP address or domain name of the SIP server with which you want the endpoint to register.</p> <p>If you set this parameter to the SIP server domain name, enable the domain name server (DNS). If the DNS is not enabled, enable Proxy server.</p>	Example: 192.168.1.10
Conference service number	<p>Specifies the conference service number for your endpoint to initiate conferences over an IP multimedia subsystem (IMS) network.</p> <p>Set this parameter to the conference service number obtained from the administrator of the IMS network.</p> <p>NOTE For details about how to set parameters for interworking with the IMS and joining a conference on the IMS network, see 6.4 Joining an HD-Video Conference over an IMS Network.</p>	No default value is set for this parameter.
Enable proxy server	<p>Specifies whether to enable the proxy server.</p> <p>Select this parameter when the network environment requires the proxy server or when Server address is set to the SIP server domain name but the configured DNS server fails to resolve this domain name or the DNS server is not configured.</p> <p>NOTE If you select this parameter, you must also set Proxy server address, Site number, User name, and Password.</p>	<p>This parameter is not selected by default.</p> <p>Set this parameter based on the actual SIP network environment.</p>
Proxy server address	<p>Specifies the address of the proxy server. If you set Server address to the SIP</p>	Example: 192.168.1.10

Parameter	Description	Setting
	server domain name, set this parameter to the IP address bound to that domain name.	
Site number	Specifies the site number for your endpoint. If your endpoint registers with a SIP server, endpoints that also register with the SIP server can dial this site number to call your endpoint.	Enter a value containing any of the following: letters, digits, special characters such as @ # %. Example: 12345
User name	Specifies the user name for authentication registration.	Example: ab3@ Obtain the value of this parameter from the SIP server administrator.
Password	Specifies the password that your endpoint uses to register with a SIP server. For successful authentication on a SIP server, this password set on your endpoint must be the same as that set on the SIP server.	Obtain the value of this parameter from the SIP server administrator.
Server type	Specifies the SIP server type. <ul style="list-style-type: none"> • OCS: Select this option if your endpoint registers with the Microsoft Office Communications Server (OCS) or Microsoft Lync Server. • CISCO VCS: Select this option if your endpoint registers with the Cisco TelePresence Video Communication Server (VCS). • Standard: Select this option if your endpoint registers with other SIP servers. 	The default value is Standard .
Transmission type	Specifies the protocol used for SIP signaling transmission. <ul style="list-style-type: none"> • TCP: Use the Transmission Control Protocol (TCP) to implement transmission reliability. • UDP: Use the User Datagram Protocol (UDP) to implement transmission with reduced latency. • TLS: Use Transport Layer Security (TLS) to implement transmission security. If you select this option, you can import a root certificate from the Web interface when your endpoint registers with a SIP server. For details, see 9.3.7 Importing a 	The default value is UDP .

Parameter	Description	Setting
	Certificate .	
Video request handling	<p>Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference.</p> <ul style="list-style-type: none"> • Accept automatically: Your endpoint automatically accepts video requests from the remote endpoint. • Reject automatically: Your endpoint automatically rejects video requests from the remote endpoint. • Manual: Your endpoint prompts you to accept video requests from the remote endpoint. 	The default value is Manual .

Step 2 Select **Save**.

----End

3.1.5 Setting Wi-Fi Parameters

To use your endpoint to implement video communication over a Wi-Fi network, set the Wi-Fi parameters.

Setting Wi-Fi Client Parameters

When the Wi-Fi client function is enabled, your endpoint functions as a Wi-Fi client and access an available Wi-Fi network after connecting to a wireless router.

Step 1 Choose **Advanced > Settings > Network > Wi-Fi > Wi-Fi Client**. Select **Enable** for the **Wi-Fi Client** parameter.

Your endpoint automatically scans for available wireless routers and lists them in the **Wireless access point** list box.

If you need to set a static IP address for your endpoint, go to [Step 2](#). Otherwise, go to [Step 4](#).

Step 2 Select **Advanced**. On the displayed **Advanced Wireless Settings** screen, set IP parameters described in [Table 3-6](#).

Table 3-5 Wi-Fi parameters

Parameter	Description	Setting
Connection type	<p>Specifies the mode in which the endpoint obtains an IP address.</p> <ul style="list-style-type: none"> • Static IP: The network administrator assigns an IP address to the 	<p>The default value is Dynamic IP.</p> <p>Select Dynamic IP unless special network requirements are imposed.</p>

Parameter	Description	Setting
	<p>endpoint. If you select this option, you must also set Local IP address, Subnet mask, and Gateway address.</p> <ul style="list-style-type: none"> Dynamic IP: The endpoint automatically obtains an IP address over the Dynamic Host Configuration Protocol (DHCP). If you select this option, a DHCP server must be available on the network. 	
Local IP address	Specifies the IP address for the endpoint to connect to a wireless access point to implement communication.	<p>Example: 192.168.1.10</p> <p>This IP address and the IP address of the wireless access point must be on the same network segment. For example:</p> <p>If the IP address of the wireless access point is 192.168.1.100 and its subnet mask is 255.255.255.0, set Local IP address to 192.168.1.X. X can be any integer ranging from 0 to 255 except 100.</p>
Subnet mask	Specifies the subnet mask for the IP address of your endpoint. A subnet mask divides the IP address into a network address and a host address.	Example: 255.255.255.0
Gateway address	Specifies the gateway address that corresponds to the IP address of the endpoint.	Example: 192.168.1.1

Step 3 Select **Save**.

Step 4 From **Wireless access point**, select the wireless router you want to connect to.

Step 5 Press **OK** on the remote control. When prompted, enter the security key or password and select **Connect**.

When the endpoint is connected to the router, the Connection Status changes to .

----**End**

Setting Wi-Fi Hotspot Parameters

When the Wi-Fi hotspot function is enabled on the endpoint, other devices, such as VPM220Ws, tablets, and PCs, can access a Wi-Fi network by connecting to the endpoint.

Step 1 Choose **Advanced > Settings > Network > Wi-Fi > Wi-Fi Hotspot**. Select **Enable** for the **Wi-Fi Hotspot** parameter.

Step 2 Select **Advanced**. On the displayed **Advanced Wireless Settings** screen, set the advanced wireless network parameters described in [Table 3-7](#).

Table 3-6 Advanced wireless network parameters

Parameter	Description	Setting
SSID Number	Specifies the name of your endpoint's Wi-Fi network.	Default value for the TE80: TE80_wifi_ap The value is a string of 1 to 31 characters, consisting of digits, letters, and special characters, such as @ # %.
Channel	Specifies a channel that transmits data through Wi-Fi signals. If you select Auto , your endpoint automatically selects the optimal channel.	The default value is Auto . Retain the default value.
Identity authentication mode	The first parameter specifies the identity authentication mode used on the Wi-Fi network. The second parameter specifies the data encryption mode corresponding to the identity authentication mode adopted. <ul style="list-style-type: none"> OPEN: If you select this option for Encryption mode, the values available for Encryption mode are NONE and WEP. SHARE: If you select this option for Encryption mode, the value available for Encryption mode is WEP. WPA-PSK: If you select this option for Encryption mode, the values available for Encryption mode are TKIP and AES. WPA2-PSK: If you select this option for Encryption mode, the values available for Encryption mode are TKIP and AES. 	The default value is WPA2-PSK . Wi-Fi Protected Access (WPA) provides greater security than Wired Equivalent Privacy (WEP). Therefore, set Identity authentication mode to WPA-PSK or WPA2-PSK . NOTE When the endpoint is connected to a VPM220W, you must set Identity authentication mode to WPA-PSK or WPA2-PSK .
Encryption mode	Specifies the encryption method used on the Wi-Fi network. The required key types vary depending on your settings of	Default value: AES

Parameter	Description	Setting
	this parameter. If you set Encryption mode to NONE , the Wi-Fi network provided by your endpoint is open to everyone.	
Password	Specifies the password used by other devices to connect to your endpoint.	<p>The required password varies depending on your settings of Encryption mode.</p> <ul style="list-style-type: none"> • If you set Encryption mode to AES or TKIP, the default value of the password is Change_Me. • If you set Encryption mode to WEP, the default value of the password is wifi_ap_wep_1. • If you set Encryption mode to NONE, the Wi-Fi network provided by your endpoint is open to everyone.
Local IP address Subnet mask	Specify the IP address and subnet mask of your endpoint.	<p>Default values:</p> <ul style="list-style-type: none"> • Local IP address: 192.168.2.1 • Subnet mask: 255.255.255.0
DHCP	<p>Specifies whether your endpoint assigns IP addresses to devices connected to it.</p> <p>NOTE If you select this parameter, you must also set Start IP address and End IP address.</p>	This parameter is selected by default.
Start IP address End IP address	Specify the IP address segment for the devices connected to your endpoint.	<p>Default values:</p> <ul style="list-style-type: none"> • Start IP address: 192.168.2.10 • End IP address: 192.168.2.100

Step 3 Select Save.

In the **Connected devices** list box, you can view the MAC and IP addresses of all the devices connected to your endpoint.

----End

3.2 Connecting to a 4E1 Network

Only the TE80 supports 4E1 functions. To implement video communication over a 4E1-line dedicated network, you must connect the TE80 to the network.



NOTICE

- Do not connect outdoor cables directly to the TE80. If outdoor E1 lines (unbalanced) are led indoors, surge protectors are required. Any questions, contact technical support personnel.
- The connection of E1 lines must comply with grounding specifications. For details, see [A E1 and T1 Grounding Criteria](#).

A 4E1 interface card provides four balanced-output ports. If the TE80 has a 4E1 interface card installed, connect the TE80 to a 4E1-line dedicated network.

The ports of a 4E1 interface card can be used for any of the four E1 lines. There is no mapping between the ports and the four E1 lines on the local and the remote ends, so the lines can be connected to any of the ports at the local and remote ends, as long as all the four lines are connected.

3.2.1 Inserting a 4E1 Interface Card

To hold conferences over a 4E1 network, you must insert a 4E1 interface card into the corresponding interface slot at the back of the TE80.

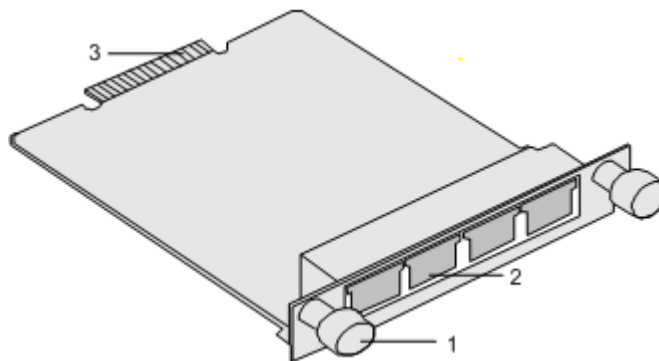


NOTICE

For safety reasons, insert the interface card only when the TE80 is powered off.

[Figure 3-1](#) shows the appearance of a 4E1 interface card, for your reference only.

Figure 3-1 4E1 interface card



1 Captive screw

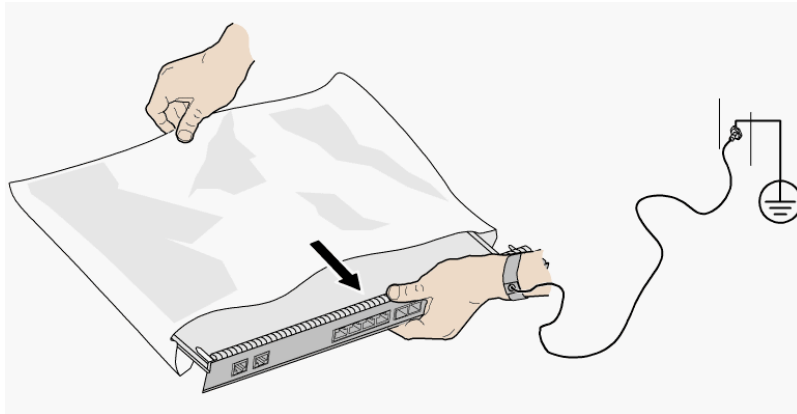
2 4E1 port (RJ45)

3 Edge connector

 **NOTICE**

To avoid damage to the interface card, implement antistatic measures before touching the card, such as wearing an ESD wrist strap, as shown in [Figure 3-2](#).

Figure 3-2 Wearing an ESD wrist strap



Insert the interface card, as shown in [Figure 3-3](#).

Figure 3-3 Inserting an interface card



Procedure

1. Loosen the two screws and remove the cover panel of the interface card slot.
2. Take out the interface card from its package. Slide the interface card into the card slot while keeping the side with components facing upwards.
3. Fasten the screws on the interface card.

3.2.2 Checking Status Indicators on the 4E1 Ports

The status indicators on the 4E1 ports can quickly provide information about the current network connection.

There are two indicators on the 4E1 port to indicate the network connection, as shown in [Table 3-8](#).

Table 3-7 Status indicator on the 4E1 port

Indicator Status	Connection Status
The orange indicator is on.	The lines are connected and the clocks on the lines are synchronous.
The green indicator is on.	A call can be placed.

3.2.3 Setting 4E1 Parameters

If 4E1 lines are used for video communication, you must set 4E1 parameters such as the account, password, clock mode, signaling mode, and sensitivity.

Prerequisites

Before setting 4E1 parameters, ensure that 4E1 lines are used by the TE80.

If the TE80 has a 4E1 interface card installed, the TE80 automatically detects the interface card type and displays the corresponding configuration screen. For parameter details, contact your network service provider.

Context

If 4E1 lines are faulty and if automatic backup is available, the endpoint uses the backup line preferentially, and then reduces the conference rate automatically. The endpoint can perform automatic backup, automatic rate reduction, or automatic rate increase in one second. During the process, erratic display may occur on the video and noise may exist. After two seconds, however, the video and the audio will be recovered and the conference rate remains unchanged.

Procedure

Step 1 Choose **Advanced > Settings > Network > 4E1/E1**. Set the parameters listed in [Table 3-9](#).

Table 3-8 4E1 parameters

Parameter	Description	Setting
Account Password	Specifies the user name and password the TE80 uses to place an H.320 call.	Obtain the user name and password from the videoconferencing system administrator.
Clock mode	Specifies the clock mode used by the TE80. The following clock	<ul style="list-style-type: none"> If the TE80 is connected to an MCU, set the MCU clock as the

Parameter	Description	Setting
	<p>modes are available:</p> <ul style="list-style-type: none"> • Preferred clock: The TE80 uses its internal clock and provides the clock to the endpoint connected to its 4E1 port. To place a point-to-point call, set Clock mode for either endpoint to Preferred clock. • Alternate clock 1/Alternate clock 2/Alternate clock 3/Alternate clock 4: The TE80 obtains a clock from any of these lines. 	<p>master clock and the TE80 clock as the slave clock.</p> <ul style="list-style-type: none"> • If the TE80 is connected to another endpoint, set one endpoint's clock as the master clock and the other's to slave clock.
Signaling mode	<p>Specifies the transmission mode for 4E1 signaling.</p> <p>The Cyclic Redundancy Check (CRC) is used to test the network quality, and CRC results indicate frame error rates. When you select an option that contains CRC4, the TE80 tests the network for bit errors.</p>	<ul style="list-style-type: none"> • To use channel associated signaling, select CAS. • To use common channel signaling, select CCS.
Sensitivity	<p>Specifies the sensitivity of the receive equalizer.</p> <p>Set this parameter based on the length of the 4E1 line used between the TE80 and the nearest network node such as a switch.</p>	<ul style="list-style-type: none"> • If the length of the 4E1 line used between the TE80 and the nearest network node exceeds 100 meters, select Long line. • If the length of the 4E1 line used between the TE80 and the nearest network node is less than 100 meters, you can select Long line or Short line. Long line is recommended because it provides a higher sensitivity.

Step 2 Select **Save**.

----End

4 Display Device and Camera

About This Chapter

To bring an impressive video experience, correctly connect video input and output devices to the video input and output ports on the endpoint and set the video input and output parameters.

4.1 Connecting a Display Device

When connecting display devices to the endpoint, choose cables based on the related ports.

4.2 Configuring a Display Device

Correctly setting video output parameters and adjusting video display parameters enable a display device to deliver superior video quality.

4.3 Connecting a Camera

You can view the video delivered by a camera only after correctly connecting the camera to the endpoint and setting the required video input parameters.

4.4 Configuring Video Input

Correct video input settings enable your endpoint to properly display video input from the video input ports.

4.5 Selecting and Controlling a Camera

If you have connected multiple video devices to the video input ports, you must select local and remote video sources from these devices. Then, you can control the local and remote cameras to view the desired video.

4.6 Setting Camera Presets

Camera presets are camera positions you store ahead of time. Each camera preset stores the camera pan, tilt, and zoom (PTZ) settings. You can easily control the camera by switching between its presets.

4.1 Connecting a Display Device

When connecting display devices to the endpoint, choose cables based on the related ports.

The video output formats vary according to port types. [Table 4-1](#), [Table 4-2](#), and [Table 4-3](#) describe the video output ports on the endpoint.

Table 4-1 Capabilities of the TE40's video output ports

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After Startup
1 MAIN OUT	1	HDMI	DVI and HDMI	By default, this port functions as the main output port, GUI port, and caption output port and is used to display the remote controlled UI, captions, and local video. This port can also be used to switch to combined pictures.
2 HDMI OUT	2	HDMI	DVI and HDMI	By default, this port functions as the auxiliary output port and is used to display the local video. When the Presentation display function is enabled, this port is used to display the local or remote presentation if a presentation source is connected to this port and display a black screen if no presentation source is connected to this port.
3 VGA OUT	3	VGA	VGA and YPbPr	By default, this port is used to display the local video.

Table 4-2 Capabilities of the TE50's video output ports

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After Startup
1 MAIN OUT	1	HDMI	DVI and HDMI	By default, this port functions as the main output port, GUI port, and caption output port and is used to display the remote controlled UI, captions, and

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After Startup
				local video. This port can also be used to switch to combined pictures.
2 HDMI OUT	2	HDMI	DVI and HDMI	By default, this port functions as the auxiliary output port and is used to display the local video. When the Presentation display function is enabled, this port is used to display the local or remote presentation if a presentation source is connected to this port and display a black screen if no presentation source is connected to this port.
3 VGA OUT	3	VGA	VGA and YPbPr	By default, this port is used to display the local video.
4 3G-SDI OUT	4	BNC	SDI	By default, this port is used to display the local video.
5 SD OUT	5	RCA	CVBS	By default, this port is used to display the local video.

Table 4-3 Capabilities of the TE80's video output ports

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After Startup
1 MAIN OUT	1	DVI-I	DVI, VGA, YPbPr, and HDMI	By default, this port functions as the main output port, GUI port, and caption output port and is used to display the remote controlled UI, captions, and local video. This port can also be used to switch to combined pictures.
2 PC OUT	2	DVI-I	DVI, VGA, YPbPr, and	By default, this port functions as the auxiliary

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After Startup
		HDMI	HDMI	output port and is used to display the local video. When the Presentation display function is enabled, this port is used to display the local or remote presentation if a presentation source is connected to this port and display a black screen if no presentation source is connected to this port. NOTE If you select HDMI and DVI as the output signal source, these two ports deliver the same video. If you select another type of signal source, only the DVI-I port delivers videos.
		HDMI	DVI and HDMI	
2 SD OUT	2 (DVI-I port)	DVI-I	S-VIDEO and CVBS	By default, this port is used to display the local video. Connect a display device to this port using a DVI-S-Video/VGA/CVBS cable.
3 DVR OUT	3	HDMI	DVI and HDMI	By default, this port is used to display the local video.
4 3G-SDI OUT	4	BNC	SDI	By default, this port is used to display the local video.

Selecting Between Ports

When you connect the endpoint to one or more display devices, select ports based on the content you want to view.

- Connecting to one display device
The 1 MAIN OUT port is recommended. Using the default endpoint settings, a display device connected to the 1 MAIN OUT port can show the local video, presentation, remote controlled UI, captions, and combined pictures.
- Connecting to two display devices
To show the video and presentation independently on two display devices, connect the two display devices to the 1MAIN OUT and 2 PC OUT ports if you are using the TE80 and to the 1 MAIN OUT and 2 HDMI OUT ports if you are using the TE50 or TE40. A

display device shows the local video when connected to the 1 MAIN OUT port and shows the presentation when connected to the 2 PC OUT port (or 2 HDMI OUT port). The **Presentation display** parameter must be enabled in order for this method to work. For details, see [4.2.1 Configuring Video Output](#).

The preceding information describes the recommended connection methods for default endpoint settings. Select ports based on the actual settings of your endpoint and the capabilities of its video output ports.

Selecting Between Cables

Use the cable that is provided to connect a display device to the endpoint based on the content to be displayed and the port on the display device.



NOTE

Please use the cables provided with the endpoint. Other cables may not be able to ensure the desired quality. Contact the device supplier to purchase appropriate cables.

4.2 Configuring a Display Device

Correctly setting video output parameters and adjusting video display parameters enable a display device to deliver superior video quality.

4.2.1 Configuring Video Output

After connecting all the video cables, correctly set the video output parameters, such as the output mode, resolution, refresh rate, and stretch mode, to deliver superior video quality.

Background

For details about the video output ports on various endpoint models, see [4.1 Connecting a Display Device](#).

[Table 4-6](#) list the resolutions supported by the video output ports in each output mode.

Although video is sharper at a higher resolution, the resolution you select must be supported by the display device used.

Table 4-4 Available video resolutions in each output mode of TE80

Output Mode	Video Resolution
1 MAIN OUT	
VGA	800 x 600 pixels, 1024 x 768 pixels, 1280 x 1024 pixels, UXGA (1600 x 1200), 1920 x 1200 pixels, 720p, and 1080p
YPbPr	720p, 1080i, and 1080p
DVI	800 x 600 pixels, 1024 x 768 pixels, 1280 x 1024 pixels, UXGA (1600 x 1200), 1920 x 1200 pixels, 720p, 1080i, and 1080p
HDMI	720p, 1080i, and 1080p
2 PC OUT	

Output Mode	Video Resolution
VGA	800 x 600 pixels, 1024 x 768 pixels, 1280 x 1024 pixels, UXGA (1600 x 1200), 1920 x 1200 pixels, 720p, and 1080p
YPbPr	720p, 1080i, and 1080p
DVI	800 x 600 pixels, 1024 x 768 pixels, 1280 x 1024 pixels, UXGA (1600 x 1200), 1920 x 1200 pixels, 720p, 1080i, and 1080p
HDMI	720p, 1080i, and 1080p
2 SD OUT	
CVBS	NTSC and PAL
S-VIDEO	NTSC and PAL
3 DVR OUT	
DVI	800 x 600 pixels, 1024 x 768 pixels, 1280 x 1024 pixels, UXGA (1600 x 1200), 1920 x 1200 pixels, 720p, 1080i, and 1080p
HDMI	720p, 1080i, and 1080p
4 3G-SDI OUT	
SDI	720p, 1080i, and 1080p

Although video is smoother at a higher refresh rate, the refresh rate you select must be supported by the display device used.

Table 4-7 lists the refresh rates available for each video resolution.

Table 4-5 Available refresh rates for each resolution

Video Resolution	Refresh Rate (Hz)
NTSC	60
PAL	50
800 x 600 pixels	56, 60, 72, 75, or 85
1024 x 768 pixels	60, 70, 75, or 85
1280 x 1024 pixels	60, 75, or 85
UXGA (1600 x 1200)	60
1920 x 1200 pixels	60

Video Resolution	Refresh Rate (Hz)
720p	<ul style="list-style-type: none"> 60, if the output mode is VGA 50 or 60, if the output mode is DVI, YPbPr, or HDMI
1080i	50 or 60
1080p	<ul style="list-style-type: none"> 60, if the output mode is VGA 24, 25, 30, 50, or 60, if the output mode is DVI, YPbPr, or HDMI

Procedure

Step 1 Choose **Advanced > Settings > Video > Common Settings > Video Output**. Set the common video output parameters described in [Table 4-8](#).

Table 4-6 Common video output parameters

Parameter	Description	Setting
GUI	<p>Specifies the video output port for the remote controlled UI.</p> <p>During a conference, you can configure your endpoint to display video on one display and the remote controlled UI on another display by setting this parameter to a value different from the value of Main output interface.</p>	The default value is 1 MAIN OUT .
Caption output	<p>Specifies the video output port for captions.</p> <p>NOTE This parameter takes effect only when the caption type is set to T.140.</p>	The default value is 1 MAIN OUT .
Main output interface	<p>Specifies the main output port.</p> <p>Only the main output port supports combined picture output. For details about the combined picture function.</p>	<p>The default value is 1 MAIN OUT.</p> <p>To ensure good video quality, retain the default value.</p>
Auxiliary output port	Specifies the auxiliary output port for preferentially displaying presentation.	<p>The default value of TE80 is 2 PC OUT.</p> <p>The default value of TE40 or TE50 is 2 HDMI OUT.</p> <p>Do not set Main output interface and Auxiliary output port to the same output port.</p>
Presentation display	Specifies whether the endpoint displays the video and presentation on separate	The default value is Disable .

Parameter	Description	Setting
	<p>displays.</p> <ul style="list-style-type: none"> When this parameter is disabled, the outputs from the Auxiliary output port and Main output interface are the same. When this parameter is enabled, the Auxiliary output port is used to display the local or remote presentation and display a black screen if no presentation source is connected. 	<p>Disable this parameter when only one display device is connected to the endpoint.</p>

Step 2 Select **Save**.

Step 3 Choose **Advanced > Settings > Video > Video Output**. Set the advanced video output parameters described in [Table 4-9](#).

Table 4-7 Advanced video output parameters

Parameter	Description	Setting
Name	<p>Specifies the output port name to help you identify ports during a conference.</p>	<ul style="list-style-type: none"> The default value for the 1 MAIN OUT port is 1 MAIN OUT. The default value for the 2 PC OUT port (only TE80) is 2 PC OUT. The default value for the 3 DVR OUT port (only TE80) is 3 DVR OUT. The default value for the 4 3G-SDI OUT port (only TE80) is 4 3G-SDI OUT. The default value for the 2 SD OUT port (only TE80) is 2 SD OUT.
Output mode	<p>Specifies the format for the video received by the display.</p> <p>Output modes vary according to video output ports. For details, see Table 4-4, Table 4-5, and Table 4-6.</p>	<p>Default values:</p> <ul style="list-style-type: none"> 1 MAIN OUT port: DVI if the TE80 is used. 2 PC OUT port (only for the TE80): DVI 3 DVR OUT port (only for the TE80): DVI 4 3G-SDI OUT port (only for the TE60 and TE80): SDI 2 SD OUT port (only for

Parameter	Description	Setting
		the TE80): CVBS
Video resolution	Specifies the resolution for each video output port. The available options vary depending on your settings of Output mode . Table 4-4 , Table 4-5 , and Table 4-6 list the resolutions supported by the video output ports in each output mode.	<ul style="list-style-type: none"> The default value for the 2 SD OUT port (only TE80) is NTSC. The default value for other ports is 1080p .
Refresh rate	Specifies the video refresh rate. The available options vary depending on your settings of Video resolution . Table 4-7 lists the refresh rates available for each video resolution.	The default value is 60Hz .
Stretch mode	Specifies how to adjust the aspect ratio to fit the video into the screen. <ul style="list-style-type: none"> Stretch: The aspect ratio is changeable. No stretch: The aspect ratio is not changeable. Intelligent stretch: Your endpoint crops the video to an appropriate size and stretches the video to full screen with the original aspect ratio. For example, to change a wide-screen video to a narrow-screen video, your endpoint crops the left and right edges of the wide-screen video and stretches the video to fill the screen. 	The default value is Stretch .
Automatic layout mode	Specifies how your endpoint displays the video and presentation. <p>NOTE Only the main output port supports this parameter.</p> <ul style="list-style-type: none"> Full screen: Your endpoint displays the video or presentation in full screen in the following priority sequence: remote presentation, local presentation, remote video, and local video. PIP: The Picture in Picture (PiP) function is enabled to display the video and presentation. 2 panes: The video and presentation are displayed in two panes. 3 panes (a) or 3 panes (b): The video and presentation are displayed in three panes. 	The default value is Full screen .
Small window	Specifies the position of the PiP window	The default value is Lower

Parameter	Description	Setting
position	on the screen. This parameter is available only when Automatic layout mode is set to PiP . NOTE Only the main output port supports this parameter.	right corner.
Display local video Display remote video Display Presentation	Specify the content to be display through a port. You can select these three parameters for video output ports, except Main output interface and Auxiliary output port.	Choose whether to display the local and remote videos and presentations based on your needs.

Step 4 Select **Save**.

----End

4.2.2 Adjusting the Picture Offset

If you find that the displayed video deviates from its normal position, adjust the picture offset.

Prerequisites

A VGA or YPbPr video signal source is connected to the endpoint.

Background

VGA or YPbPr Image offset may occur in video input or output, such as when the computer desktop is displayed on the display.

Procedure

Step 1 Choose **Advanced > Settings > Video > Image Offset**.

Step 2 Select a video input or output port.



NOTE

You can adjust the picture offset only for a video input or output port to which a VGA or YPbPr video signal source is connected. The ports to which other video signal sources are connected are unavailable for adjustment.

Step 3 Select **Horizontal offset** or **Vertical offset** and move the slider to make adjustments.

----End

4.2.3 Adjusting the Sampling Phase

If a blurring or slight jitter issue occurs in the video shown on the display device, adjust the sampling phase.

Prerequisites

A VGA or YPbPr video signal source is connected to the endpoint.

Background

Images input through a VGA or YPbPr port, such as the computer desktop, may suffer from blurring or slight jitter.

Procedure

Step 1 Choose **Advanced > Settings > Video > Sampling Phase**.

Step 2 Select the video input port you want to adjust.



NOTE

You can adjust the sampling phase only for a video input port to which a VGA or YPbPr video signal source is connected. The ports to which other video signal sources are connected are unavailable for adjustment.

Step 3 Move the slider to adjust the sampling phase.

----End

4.2.4 Setting Video Parameters

If the endpoint is connected to a Huawei HD camera, you can set the camera video parameters, including the video mode, noise reduction, and video resolution. You can view the video result of your settings on the display device connected to your endpoint.

Prerequisites

A Huawei HD camera has been connected to a video input port on the endpoint.

Background

The video parameters you can set vary according to the camera model connected to the endpoint. [Table 4-10](#) is for your reference only. To determine the camera model connected to the video input port, choose **Advanced > Settings > Video > Video Input**.

Procedure

Step 1 Choose **Advanced > Settings > Video > Video Parameters**.

Step 2 Select the desired video input port such as the 1 MAIN IN port. Set the video parameters described in [Table 4-10](#).

Table 4-8 Video parameters

Parameter	Description	Setting
Picture mode	Specifies the output video display effect. <ul style="list-style-type: none">Standard: reproduces video more faithfully.Vivid: delivers brighter video with	The default value is Standard .

Parameter	Description	Setting
	<p>cooler colors.</p> <ul style="list-style-type: none"> • Natural: delivers video with warmer colors. • User defined: delivers video with custom settings. After you select this option, you can set the following parameters. <ul style="list-style-type: none"> – Aperture: sharpens video edges and contours to preserve the impression of clarity and fine details. Over-sharpening will make video less realistic. – Brightness: specifies the video output level that changes the brightness of the video displayed on the monitor. – Hue: adjusts the video color. – Saturation: adjusts the gray scale of each color. The higher the saturation, the brighter a color. 	
Exposure mode	<p>Specifies the mode of using natural light. You can select either of the following modes:</p> <ul style="list-style-type: none"> • Auto: The camera automatically selects the optimum configuration based on the surrounding environment. • Manual: You need to manually adjust Brightness gain, Shutter speed, and Iris. • Iris priority: When you manually adjust the aperture, the camera selects the corresponding shutter rate. • Shutter priority: When you manually adjust the shutter rate, the camera selects the corresponding aperture. This mode is mainly used to shoot moving objects. 	The default value is Auto .
White balance	<p>Specifies the white balance to enable the camera to accurately recognize the color white and deliver more vivid videos.</p> <ul style="list-style-type: none"> • Auto: • One-push: • Manual: 	The default value is Auto .
Noise reduction	<p>Removes noise artifacts from video. A larger value causes the video to have less</p>	The default value is Low .

Parameter	Description	Setting
	noise but detail may also be lost.	
Set output resolution automatically	Specifies whether the camera automatically sets the video output resolution.	The default value is Disable .
Video resolution	Specifies the video output resolution for the camera. This parameter is available only when Set output resolution automatically is set to Disable .	The default value is 1080p 60Hz .
Image inversion	Specifies whether the video input from the camera is rotated by 180 degrees. When the camera is hung, set this parameter to Enable .	The default value is Disable .

----End

4.2.5 Switching Between Screen Layouts

By adjusting the screen layout, you can view multiple videos on the same display device.

Only the main output port supports combined picture output. For details, see [Table 4-8 in 4.2.1 Configuring Video Output](#).

To adjust the screen layout, use either of the following methods:




- When the endpoint is not in use in a conference, press  on the remote control to switch between the full screen, Picture in Picture (PiP) and two-pane (larger pane on the left, larger pane on the top, or two panes in the same size) modes. When the endpoint is in use in a conference, press  on the remote control to switch between the full screen, PiP, two-pane (larger pane on the left, larger pane on the top, or two panes in the same size), and three-pane modes.
- When the endpoint is in use in a conference, select  from the option bar and select a desired layout from the following:
 - Remote video in full screen
 - Local video in full screen
 - Combination of the local video, remote video, local presentation, and remote presentation in PiP, two-pane, or three-pane mode

Figure 4-1 Screen layout example

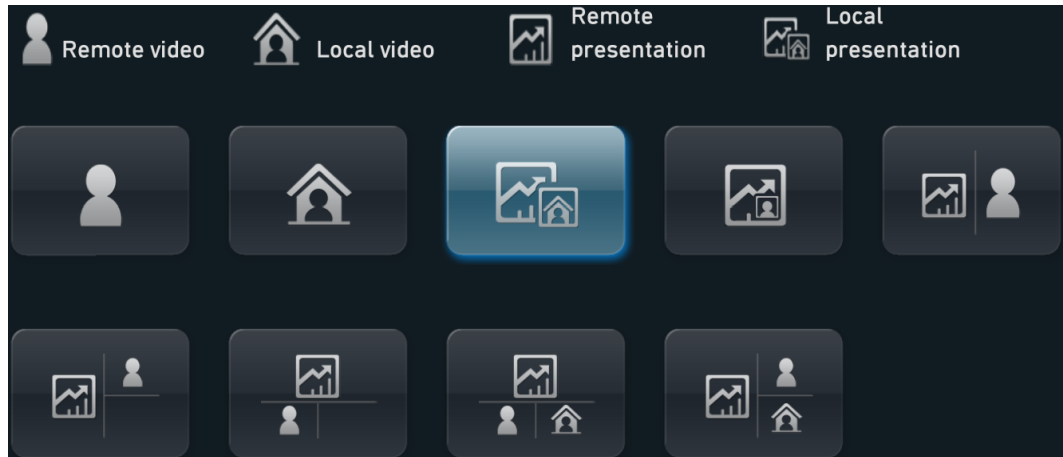


Figure 4-1 is for your reference. Icons displayed in the rectangle vary according to endpoint status. For example, the local and remote presentation icons are displayed only when the following conditions are met:

- A presentation source is connected to your site. When this happens, the icon for the local presentation is displayed.
- Your site receives a presentation shared by a remote site. When this happens, the icon for the remote presentation is displayed.

The icon for the local presentation disappears if the local presentation source is disconnected from the endpoint. The icon for the remote presentation disappears if the remote presentation sharing stops.

Before a conference starts, you can set the position of the PiP window on the screen. For details, see [Table 4-9](#) in [4.2.1 Configuring Video Output](#).

4.3 Connecting a Camera

You can view the video delivered by a camera only after correctly connecting the camera to the endpoint and setting the required video input parameters.

The endpoint supports various camera models, including the HUAWEI VPC600 HD camera (VPC600), HUAWEI VPC620 HD camera (VPC620), ViewPoint C500 HD camera (C500), HUAWEI VPC500 HD camera (VPC500), HUAWEI VPC520 HD camera (VPC520), HUAWEI VPC500S camera (VPC500S), HUAWEI VPC500E camera (VPC500E), SONY EVI-HD1, SONY EVI-D100, SONY EVI-D70, SONY D30/D31, SONY BRC-300P, SONY BRC-H700, SONY BRC-Z330, CANON V50, CANON VCC1, CANON VCC4, 3CCD, C200, GTP CAM, KX, PELCO, PTC100, SYYT, TAC, VCC-SW80P, and VCC-HD90P.

[Table 4-13](#) list the capabilities of the video input ports.

Table 4-9 Capabilities of the TE80's video input ports

Port Name on the UI	Port Number on the Rear Panel	Type	Receivable Input Format	Control	Description
1 MAIN IN	1	DVI-I	VGA, YPbPr, DVI, HDMI, CVBS, and S-VIDEO	Camera PTZ	The DVI-I and HD-VI ports are mutually exclusive and cannot be used at the same time.
		HD-VI	DVI(HW), HDMI(HW), and YPbPr(HW)	Camera PTZ	
2 PC IN	2	DVI-I	VGA, YPbPr, DVI, and HDMI	Camera PTZ	The DVI-I and Display Port ports are mutually exclusive and cannot be used at the same time.
		Display Port	DP and HDMI	Camera PTZ	
3 AUX IN	3	HDMI	DVI and HDMI	Camera PTZ	The HDMI and HD-VI ports are mutually exclusive and cannot be used at the same time.
		HD-VI	DVI(HW) and HDMI(HW)	Camera PTZ	
4 3G-SDI IN	4	BNC	SDI	Camera PTZ	None



NOTE

- PTZ is an acronym for Pan, Tilt, and Zoom. A PTZ camera supports panning, tilting, and zooming control.
- The HD-VI port can only be connected to the HUAWEI VPC600 or VPC620. After connecting this port to the HUAWEI VPC600 or VPC620, you can perform PTZ controls on and supply power to the HUAWEI VPC600 or VPC620 without additional cables.
- If you connect a port other than the HD-VI port to the camera, you must connect the cable used for transmitting VISCA control signals to the COM port on your endpoint to perform PTZ controls on the camera.

Each input port to be used for transmitting a video or a presentation can be specified on the user interface. For details, see section [6.1.1 Designating the Dual Streams](#).

Select a video input port on your endpoint based on the video format supported by the camera. Then connect the camera to your endpoint using the cable provided.

4.4 Configuring Video Input

Correct video input settings enable your endpoint to properly display video input from the video input ports.

Procedure

Step 1 Choose **Advanced > Settings > Video > Video Input**. Set the video input parameters described in [Table 4-14](#).

Table 4-10 Video input parameters

Parameter	Description	Setting
Name	Specifies the video input port name to help you identify ports during a conference.	Do not leave this parameter blank. Enter a string of 1 to 64 characters.
Camera type	Specifies the type of the camera connected. The endpoint supports cameras of multiple manufacturers and models.	The default value is VPC600/VPC620 . The control commands vary with different cameras. Therefore, select the camera type correctly to ensure that the camera can be controlled properly.
Serial port	Specifies the serial port that is connected to the camera control interface. You can select either COM1 or COM2 .	The default value for the 1 MAIN IN port is COM2 while that for other video input ports is None . Select the serial port that is being used. Otherwise, the camera cannot be controlled.
Initial position	Specifies the position of the camera after startup. <ul style="list-style-type: none"> Auto: The camera moves to its initial position after startup. Preset 1: The camera moves to the preset after startup. <p>NOTE Each camera preset stores the pan, tilt, and zoom settings of the camera. For how to set presets, see 4.6 Setting Camera Presets.</p>	The default value is Auto .
Moving speed	Specifies the movement and zoom speed for the camera at your site. <ul style="list-style-type: none"> Select Slow for accurate positioning. Select Fast for quick positioning. Select Medium for medium paced positioning. 	The default value is Medium .
Input source	Specifies the input source format.	The default value is Auto .
Mirroring	Specifies whether the endpoint displays a reflection of an input video, wherein the right and left sides of the original are	The default value is Normal .

Parameter	Description	Setting
	reversed. <ul style="list-style-type: none"> • Normal: The input video will not be reversed. • Horizontal: The endpoint displays a reflection of the input video, wherein the right and left sides of the original are reversed like the reflection of something seen in a mirror. 	
1080p PsF conversion	When the camera connected to the endpoint uses the Progressive segmented Frame (PsF) mode for transmitting signals, enable this function.	The default value is Disable .
Stretch mode	Specifies how your endpoint adjusts the input video based on the video encoding format. <ul style="list-style-type: none"> • Stretch: Stretch the video to full screen with an unfixed aspect ratio. • No stretch: Stretch the video to full screen with a fixed aspect ratio. Black borders may appear at the upper and lower or left and right edges of the display. • Intelligent stretch: Crop the video to an appropriate size and stretch the video to full screen with the original aspect ratio. For example, to change a wide-screen video to a narrow-screen video, your endpoint crops the left and right edges of the wide-screen video and stretches the video to fill the screen. 	The default value is No stretch .

Step 2 Select **Save**.

----**End**


4.5 Selecting and Controlling a Camera

If you have connected multiple video devices to the video input ports, you must select local and remote video sources from these devices. Then, you can control the local and remote cameras to view the desired video.

Selecting a Camera


If the endpoint is not in use during a conference, only the local camera can be selected. If the endpoint is in use during a conference, both the local and remote cameras can be selected.

Choose **Advanced Settings > Settings > Video > Common Settings > Video Input**. Set **Video Source Management** to **Allow**. Select a camera as follows:

Press  **23** on the remote control and select the desired camera from the list displayed in the lower right corner of the screen.



NOTE

The text in the upper left corner indicates the camera that is currently being controlled (local or remote). Press  on the remote control to toggle between the local and remote cameras.

Adjusting the Focal Length

You can change the magnification of distant objects by adjusting the focal length of the camera.

Step 1 On the option bar, select .

Step 2 Select **Adjust Focus** and adjust the focal length.

----End

Controlling a Camera


You can control pan, tilt, and zoom (PTZ) actions for a local or remote camera.

Before controlling a remote camera, ensure that **Remote control** has been set correctly for the remote site.





NOTE

Choose **Advanced Settings > Settings > Video > Common Settings > Video Input**. Set **Remote control** to **Allow**.


Step 1 Press  on the remote control.

Step 2 On the camera control screen, perform any of the following:

- Press navigation keys on the remote control to turn the camera lens.
- Press  to zoom in or  to zoom out.



NOTE

The text in the upper left corner indicates the camera that is currently being controlled (local or remote). Press  on the remote control to toggle between the local and remote cameras.

----End

4.6 Setting Camera Presets

Camera presets are camera positions you store ahead of time. Each camera preset stores the camera pan, tilt, and zoom (PTZ) settings. You can easily control the camera by switching between its presets.

If a camera supports PTZ functions, you can create and save a maximum of 30 camera presets. A camera preset remains valid until it is deleted or changed.

[Table 4-15](#) lists camera preset specifications.

Table 4-11 Camera preset specifications


Endpoint	Number of Camera Presets	Whether Data Is Lost After Restart
Local	30	No
Remote	Dynamically adjustable	Yes

Saving a Camera Preset

A camera preset stores the camera PTZ settings.

If you select a preset number that has already been saved as another preset, the new camera preset replaces the existing one.

To save a camera preset:


- Step 1** Set the camera lens position. For details, see [4.5 Selecting and Controlling a Camera](#).
- Step 2** On the option bar, select , **Save Preset**, and then a number. Press **OK** on the remote control to save the camera preset to the selected number.

----End

Moving a Camera to a Preset


If you have saved camera presets for the endpoint, you can tap a preset number to apply that preset to the camera.

To move a selected camera to a camera preset:

- Step 1** On the option bar, select  then **Switch Preset**.
- Step 2** Select a camera preset number and press **OK** the remote control to apply that preset to the camera.

----End

Deleting a Camera Preset

To delete a camera preset, select the preset number and press  on the remote control.

5 Microphone and Speaker

About This Chapter

Before using the endpoint, ensure that the microphones and speakers are correctly connected to the endpoint and that the audio parameters are correctly set.

5.1 Connecting an Audio Input Device

Before connecting the endpoint to an audio input device, you need to know each audio input port so you can make connections quickly and correctly.

5.2 Connecting an Audio Output Device

Knowledge of audio interfaces on the endpoint and the various types of audio interfaces can help in quickly and correctly connecting an audio output device to an audio output interface on the endpoint.

5.3 Connecting a Tuning Console

If a conference room requires multiple microphones or already has a tuning console for controlling microphones, you can connect the tuning console to the endpoint as the endpoint's audio input source.

5.4 Adjusting Audio Effects

You can adjust the audio effects, such as the audio input, sound effect, and volume.

5.5 Enjoying Stereo Audio

In dual-audio-channel mode, stereo effect audio can be enjoyed allowing users to accurately locate the direction from which the sound comes, gaining a true-to-life experience.

5.1 Connecting an Audio Input Device

Before connecting the endpoint to an audio input device, you need to know each audio input port so you can make connections quickly and correctly.

[Table 5-3](#) describe various audio input ports and their supported audio sources.

Table 5-1 TE80's audio input ports

Audio Input Port	Type	Supported Audio Feature
MIC 1	XLR (cannon connector)	One channel of analog audio input
MIC 2	XLR (cannon connector)	One channel of analog audio input
RCA L	RCA (RCA connector)	Left channel for line input
RCA R	RCA (RCA connector)	Right channel for line input
MIC HD-AI	Microphone array port	VPM220 microphone array
PSTN	PSTN port	PSTN signal

5.1.1 Connecting a VPM220

The endpoint can be used with a HUAWEI VPM220 microphone array (VPM220).

When installing a VPM220, do not point any microphone towards the speaker.

Status Indicators on the VPM220

VPM220 status indicators quickly provide working status information.

There are three indicators on top of the VPM220 at an interval of 120°. [Table 5-4](#) describes these three indicators.

Table 5-2 VPM220 status indicators

Indicator Status	VPM220 Status
All red	Microphones in all the three directions are muted.
All blue	Microphones in all the three directions are unmuted or working correctly.
All blue and blinking in turn clockwise	The VPM220 is connecting to the endpoint.
All off	The VPM220 is in sleep mode or disconnected from its power supply.

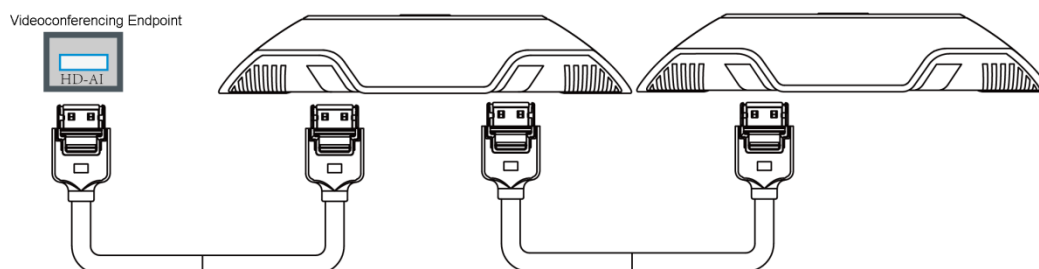
VPM220 Cascading

The VPM220 provides 360° sound pickup and an optimal pickup range of six meters. In a large conference room (of about 40 to 50 square meters) with only one VPM220, audio far from the VPM220 becomes problematic; cascaded VPM220s can help alleviate this problem. Dynamically cascading, connecting, or disconnecting VPM220s will not interrupt a conference.

The TE80 can be connected to two cascaded VPM220s.

Figure 5-1 shows the cascading of VPM220s.

Figure 5-1 Cascading of VPM220s



Using the Stereo Mode

To obtain better stereo effect, configure the mode for cascading VPM220s and their positions based on the actual conditions in your conference room.

Choose **Advanced > Settings > Conference > Advanced** and set the VPM220 mono or stereo mode. Table 5-5 describes each mode.

Table 5-3 VPM220 mono and stereo modes

Mode	Audio Protocol
Mono	G.719, G.729A, G.711A/U, G.722, G.728, and G.7221C (at any rate)
	AAC-LD or HWA-LD when mono mode is enabled
Stereo	AAC-LD or HWA-LD when stereo mode is enabled

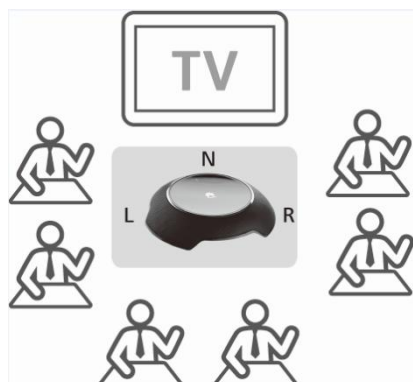
When multiple VPM220s are cascaded or when a single VPM220 works in mono mode, all the microphones in the VPM220 collect sounds. The VPM220 automatically transmits to the endpoint the best quality sound collected by one of the microphones.

Figure 5-2 shows the application of left and right audio channels when a single VPM220 works in stereo mode.

NOTE

L: The microphones are used to collect sounds for the left audio channel. R: The microphones are used to collect sounds for the right audio channel. N: No microphone is used. (The Huawei logo on the VPM220 should point to the display device.)

Figure 5-2 A single VPM220 working in stereo mode



To set the mode for cascading VPM220s:

Step 1 Choose **Advanced > Settings > Audio**.

Step 2 Based on the actual conditions in the conference room, set **Microphone array position** to **Horizontal** or **Vertical**.



NOTE

The default value is **Horizontal**.

Step 3 Select **Save**.

----End

5.1.2 Connecting a VPM220W

The endpoint can be connected to a HUAWEI VPM220W wireless microphone array (VPM220W) over a Wi-Fi network. The TE50 and TE40 can be connected to only one VPM220W while the TE80 can be connected to one or two VPM220Ws.

When installing a VPM220W, do not point any microphone towards the speaker.

Status Indicators on the VPM220W

VPM220W status indicators quickly provide VPM220W working status.

There are five indicators on top of the VPM220W and a charging status indicator on the charger base. [Table 5-6](#) describes these indicators.

Table 5-4 Status indicators on the VPM220W

Indicator Status	VPM220W Work Status
All three microphone indicators are steady red.	All the three microphones are turned off.
All three microphone indicators are steady blue.	All the three microphones are turned on.
All three microphone indicators are off.	The power switch of the VPM220W is turned off.

Indicator Status	VPM220W Work Status
All three microphone indicators are blue on and off gradually.	The VPM220W is in sleep state.
All three microphone indicators are blinking blue in a clockwise direction.	<ul style="list-style-type: none"> The VPM220W is connecting to the videoconferencing endpoint. The VPM220W is restarting.
All three microphone indicators are blinking blue twice simultaneously.	The VPM220W is preparing to send a videoconferencing endpoint a request for Wi-Fi Protected Setup (WPS) Push Button Configuration (PBC) authentication.
All three microphone indicators are blinking blue simultaneously.	The VPM220W is upgrading.
All three microphone indicators are blinking red twice in a clockwise direction.	The VPM220W is about to power off.
The Wi-Fi indicator is off.	<ul style="list-style-type: none"> The VPM220W is powered off. The VPM220W is connecting to a videoconferencing endpoint over Wi-Fi, and the Wi-Fi signal is strong.
The Wi-Fi indicator is steady red.	The VPM220W is connecting to a videoconferencing endpoint over Wi-Fi, and the Wi-Fi signal is weak.
The Wi-Fi indicator is blinking red.	The VPM220W is searching for Wi-Fi hotspots.
The battery indicator is off.	<ul style="list-style-type: none"> The battery level is sufficient (the battery can run another 30 minutes or more). The VPM220W is powered off.
The battery indicator is steady red.	The battery level is insufficient (the battery can run less than 30 minutes).
The charging status indicator is blue and is in breathing state.	The VPM220W is being recharged.
The charging status indicator is steady blue.	The VPM220W is fully charged.
The charging status indicator is off.	<ul style="list-style-type: none"> The VPM220W is not placed on the charger base. The VPM200W's power adapter is not connected to an AC power supply.

For more information, see the *HUAWEI VPM220W Microphone Array V100R001 Quick Start Guide* and *HUAWEI VPM220W Microphone Array V100R001 User Guide*.

Connecting the VPM220W to the Endpoint

The endpoint can be connected over a Wi-Fi network to a VPM220W for sound pickup.

Before connecting the VPM220W to the endpoint, you must enable the Wi-Fi hotspot and set Wi-Fi parameters as follows:

- Set **Identity authentication mode** to **WPA-PSK** or **WPA2-PSK**.
- Enable DHCP and set **Start IP address** and **End IP address**.

For details, see [Setting Wi-Fi Hotspot Parameters](#).

To connect the VPM220W to the endpoint:

Step 1 Press the power button at the bottom of the VPM220W to power it on.

The VPM220W automatically searches for an available Wi-Fi network.

- If the VPM220W was once connected to the endpoint, the connection between these two will automatically set up, so you can skip the following steps.
- If you are using the VPM220W for the first time or moving it outside the connected Wi-Fi network range, go to [Step 2](#) and [Step 3](#).

Step 2 Hold and press the button on top of the VPM220W for at least 3 seconds.

A confirmation dialog box is displayed on the remote controlled UI.

Step 3 Select **OK**.

The VPM220W then performs the Wi-Fi Protected Setup (WPS) Push Button Configuration (PBC) authentication with the videoconferencing endpoint in order to obtain an IP address.

----End

5.1.3 Setting Audio Parameters

Before using your endpoint to join a conference, set the audio parameters to gain the best possible audio experience.

Procedure

Step 1 Choose **Advanced > Settings > Audio**. Set the audio parameters described in [Table 5-7](#).

Table 5-5 Audio input parameters

Parameter	Description	Setting
MIC 1 MIC 2 (available only for the TE80)	Adjusts the microphone volume at your site. When you adjust this microphone volume, the volume heard at remote sites is adjusted accordingly.	These parameters are selected by default.
RCA L RCA R	Adjusts the input volume of the RCA port at your site. When you adjust this input volume, the volume heard at	These parameters are selected by default.

Parameter	Description	Setting
	remote sites is adjusted accordingly.	
HDMI L HDMI R	Adjusts the input volume of the HDMI port at your site. When you adjust this input volume, the volume heard at remote sites is adjusted accordingly. NOTE If you are using the TE80, this parameter is available only when you select the 3 AUX IN port as the HDMI input source.	These parameters are selected by default.
DP L (available only for the TE80) DP R (available only for the TE80)	Adjusts the input volume of the DP port at your site. When you adjust this input volume, the volume heard at remote sites is adjusted accordingly. NOTE This parameter is available only when you select the 2 PC IN port of the TE80 as the DP input source.	This parameter is selected by default.
LINE IN L (available only for the TE50) LINE IN R (available only for the TE50)	Adjusts the input volume of the LINE IN port at your site. When you adjust this input volume, the volume heard at remote sites is adjusted accordingly.	These parameters are selected by default.
Gain	Adjusts the volume for the MIC 1, MIC 2, RCA L, RCA R, HDMI L, HDMI R, DP L, DP R, LINE IN L, and LINE IN R ports.	Value range: -12 dB to +12 dB The default value is +0dB .
Volume indicator	Displays volume in real time.	No default value is set for this parameter.
Microphone array battery level	Displays the microphone array battery level in real time.	No default value is set for this parameter.
Microphone array position	Specifies the arrangement of cascaded microphone arrays.	Set this parameter based on the number and arrangement of microphone arrays. For details, see Using the Stereo Mode .
Switch controls	<ul style="list-style-type: none"> MIC array only: Your endpoint can receive audio signals collected by audio 	The default value is All audio inputs .

Parameter	Description	Setting
	<p>input devices, excluding the microphone array, when you turn off the microphone array.</p> <ul style="list-style-type: none"> • All audio inputs: Your endpoint cannot receive audio signals collected by any audio input devices when you turn off the microphone array. <p>To enable your endpoint to receive audio signals again, perform any of the following:</p> <ul style="list-style-type: none"> • Press the button on the microphone array to enable this function. • Press the microphone button on the remote control to turn on the microphone array only or all audio input devices, depending on your settings of Switch controls. • On the endpoint web interface, choose Device Control > Audio Control and select the audio input ports you want to enable. • On the remote controlled UI, choose Advanced > Settings > Audio > Audio Input and select the audio input ports you want to enable. 	
Wireless MIC power saving mode	<p>If you select this parameter, when the endpoint sleeps, the wireless microphone VPM220W also sleeps to save power. The VPM220W cannot be woken up when the endpoint is woken up. To wake up the VPM220W, press the mute button on it.</p> <p>If you do not select this parameter, when the endpoint sleeps, the VPM220W also sleeps to save power. In addition, the VPM220W can be woken up when the endpoint is woken up.</p>	The default value is Enable .

---End

5.2 Connecting an Audio Output Device

Knowledge of audio interfaces on the endpoint and the various types of audio interfaces can help in quickly and correctly connecting an audio output device to an audio output interface on the endpoint.

5.2.1 Connecting a Speaker

Connect the AUDIO OUTPUT RCA L/R port and the audio input port of a display device using an audio cable. In this way, the endpoint can use the built-in speaker of the display device (for example, a television which is usually equipped with a speaker) or it can be connected to an external speaker system, wherein the volume can be increased and a better audio effect can be obtained.

Use an audio cable to connect the AUDIO OUTPUT L/SPDIF port to a speaker to provide high-fidelity audio quality.



5.2.2 Placing an External Speaker

If the endpoint is connected to an external speaker, correctly placing the speaker helps to achieve the expected audio quality.

Note the following when placing an external speaker:

- If you are using a unidirectional microphone, the speaker and microphone must not face one another.
- If you are using an omnidirectional microphone, the distance between the speaker and microphone must be more than 1 meter.

5.2.3 Adjusting the Speaker Volume

Press  to increase the volume or  to decrease the volume. The adjustment affects the volume heard only at the local site.

5.3 Connecting a Tuning Console

If a conference room requires multiple microphones or already has a tuning console for controlling microphones, you can connect the tuning console to the endpoint as the endpoint's audio input source.

Connect the output interface of the tuning console to the RCA L/R audio input interface of the endpoint using an RCA audio cable.

5.4 Adjusting Audio Effects

You can adjust the audio effects, such as the audio input, sound effect, and volume.

Background

For details about how to adjust the audio input, see [5.1.3 Setting Audio Parameters](#). This section only describes how to adjust the sound effect and the volume.

Procedure

- Step 1** Choose **Advanced > Settings > Audio** and then set the parameters listed in [Table 5-8](#) and [Table 5-9](#).

Table 5-6 Sound effect parameters

Parameter	Description	Setting
Ringtone	Specifies the ringtone for incoming calls.	The default value is Default .
Locally output sound from AUDIO IN	Specifies whether to allow the audio input from the LINE IN port, the HDMI port or the RCA port to be heard at your site.	This parameter is not selected by default.
AUDIO IN remote output	Specifies whether to allow the audio input from the LINE IN port, the HDMI port or the RCA port to be heard at remote sites.	This parameter is selected by default.
SPDIF switch	Specifies whether you can hear sound from the local S/PDIF digital audio port at your site.	This parameter is not selected by default.
Bass Middle Treble	Adjusts the equalizers by moving the sliders.	Value range: -6 dB to +6 dB The default value is +0dB .

Table 5-7 Volume parameters

Parameter	Description	Setting
Speaker volume	Adjusts the speaker volume. To hear other sites, unmute the speaker. Otherwise, mute the speaker.	Press navigation keys on the remote control to move the slider. Value range: 0-15 The default value is 15 .
Left Right	Displays the current volume of the speaker's left and right audio channels.	No default value is set for this parameter.
Alert tone volume	Adjusts the alert tone volume.	Press navigation keys on the remote control to move the slider. Value range: 0-3 The default value is 3 .

Step 2 Select **Save**.

----End

5.5 Enjoying Stereo Audio

In dual-audio-channel mode, stereo effect audio can be enjoyed allowing users to accurately locate the direction from which the sound comes, gaining a true-to-life experience.

Background

For details about the VPM220, see [5.1.1 Connecting a VPM220](#).

Procedure

Step 1 Connect the endpoint to a microphone and a stereo acoustic system.



NOTE

During a conference, move the microphone only when required. Otherwise, the quality of the stereo audio heard by remote sites is affected.

Step 2 Choose **Advanced > Settings > Audio > Audio Input**. Select audio input sources.



NOTE

All available audio input sources are selected by default.

Step 3 Select **Save** to return to the **Settings** screen.

Step 4 On the **Settings** screen, choose **Conference > Advanced Settings** and set **Audio protocol** to **AAC_LD** or **HWA-LD**. Then, set **Audio channels** to **Two**.

----End

6 Conference

About This Chapter

You can create a conference or answer an incoming call to join a conference.

6.1 Experiencing a Dual-Stream Conference

During a dual-stream conference, two independent video stream channels, that is, the video and the presentation, can be transmitted; furthermore, two channels of video from the local site can be transmitted or two channels of video from a remote site can be received at the same time.

6.2 Experiencing an MSUC Conference

Huawei videoconferencing systems can be used in the Microsoft Unified Communications (MSUC) environment. Register the endpoint (networked with MSUC) with a Lync Server using SIP. After that, the endpoint can place calls to Lync clients, receive calls from Lync clients, and view Lync clients' online status.

6.3 Joining an Authentication Conference

If you do not know how many sites are expected to join the conference, set the number of anonymous sites and hold an authentication conference. A site can join the authentication conference by calling the specified conference access number.

6.4 Joining an HD-Video Conference over an IMS Network

The endpoint can join an HD video conference over an IMS network.

6.5 Scheduling a Conference

On your endpoint, you can schedule a specific time to hold a conference.

6.6 Controlling a Conference

During a multipoint conference, you can control the video and audio of the participating sites using conference control functions.

6.7 Recording a Conference

Your endpoint can record conferences if your site is the chair site.

6.8 Managing the Address Book

The address book stores site information. You can add, edit, and delete site entries.

6.9 Managing Captions

You can create a caption on your endpoint. In addition, you can share the caption with remote sites during a conference.

6.1 Experiencing a Dual-Stream Conference

During a dual-stream conference, two independent video stream channels, that is, the video and the presentation, can be transmitted; furthermore, two channels of video from the local site can be transmitted or two channels of video from a remote site can be received at the same time.

6.1.1 Designating the Dual Streams

You need to choose the input sources and output destinations for the video and presentation.

Background

If multiple video-source devices are connected to the video input ports on the endpoint, you can choose a channel of video as the source of the local video and another channel as the source of the local presentation.

The endpoint adopts difference policies to deliver the video and presentation based on on-site situations:

- In single-screen display mode, if no presentation is shared during a conference, remote sites view the conference video of the local site; if a presentation is shared, both the local and remote sites view the presentation.
- In dual-screen mode, the display device connected to the main output port delivers the video while the display device connected to the auxiliary output port delivers the presentation.
- During the layout switch in combined picture or continuous presence mode, remote sites can always view the conference video of the local site.

Selecting the Video Source

Choose **Advanced > Settings > Video > Common Settings > Video Input**. On the displayed screen, set **Video Source** to a video feed.

Selecting the Presentation Source

Choose **Advanced > Settings > Video > Common Settings > Video Input**. On the displayed screen, set **Presentation Source** to a video feed.

Selecting the Output Destinations for the Video and Presentation

By default, the endpoint comes with one display device and uses the main output port to deliver both the video and presentation. If two display devices are connected to the endpoint, you can set the endpoint to separately display the video and presentation on the two display devices.

One display device: Based on the default endpoint settings, the display device connected to the 1 MAIN OUT port can show the video, presentation, remote controlled UI, captions, and combined pictures.

Two display devices: To show the video and presentation independently on two display devices, connect the two to the 1 MAIN OUT and 2 PC OUT ports if you are using the TE80 or to the 1 MAIN OUT. A display device shows the video when connected to the 1 MAIN OUT port and shows the presentation when connected to the 2 PC OUT port (or 2 HDMI OUT port). The **Presentation display** parameter must be enabled in order for this to work. For details, see [4.2.1 Configuring Video Output](#).

6.1.2 Sharing a Presentation

A computer can be connected to the endpoint to share files, and the remote sites can view both your video and the desktop contents of the computer.

Prerequisites

The video source of the presentation has been configured.

The presentation sharing function has been enabled, and the presentation parameters have been set. By default, the endpoint has the presentation sharing function enabled, and the default presentation parameter settings support presentation sharing. To modify these parameters, see [13.3 Setting Advanced Conference Parameters](#).

Background

You can select either of the following modes for sharing a presentation:

- **Auto:** The endpoint automatically sends the video along with the presentation. This mode is available only when **Presentation mode** is set to **Live**.
- **Manual:** You can use the remote control to share a presentation.


For details, see [Table 13-3](#) in [13.3 Setting Advanced Conference Parameters](#).


However, in live mode, the endpoint does not support presentation sharing using SIP.

On a Microsoft unified communications (MSUC) network, the endpoint does not support presentation sharing.



Procedure

Press  on the remote control to share a presentation.

To stop sharing a presentation, press  on the remote control.

you can also select  on the option bar to share a presentation.

6.1.3 Viewing the Combined Picture of the Presentation and the Video

During a conference, a combined picture of the video and the presentation can be viewed by pressing  on the remote control or selecting  from the option bar.

For details, see section [4.2.5 Switching Between Screen Layouts](#).

6.2 Experiencing an MSUC Conference

Huawei videoconferencing systems can be used in the Microsoft Unified Communications (MSUC) environment. Register the endpoint (networked with MSUC) with a Lync Server using SIP. After that, the endpoint can place calls to Lync clients, receive calls from Lync clients, and view Lync clients' online status.

Background

After the endpoint joins the MSUC network, the following can be implemented.

- The endpoint and Lync clients can place calls to each other.
 - During a point-to-point call, switching between audio-only and video calls is available on both the endpoint and Lync client.
 - The endpoint supports call forwarding on Lync clients. For example, if calls to Lync A has been set to be forwarded to Lync B, then after a call between Lync A and endpoint C is set up, endpoint C automatically disconnects from Lync A and calls Lync B.
- From **Address Book** you can view Lync clients' online status.
To view a Lync client's online status, you must save that Lync client to the local address book. For details, see [Searching the LDAP Network Address Book for Sites](#).

The following describes how the endpoint places a call to the Lync client.

Procedure

Step 1 Register the endpoint with the MSUC network.

1. Choose **Advanced > Settings > Network > IP > SIP**.
2. Set the SIP parameters for interworking with the MSUC and registering the endpoint with the Lync Server. [Table 6-1](#) describes the related parameters.

Table 6-1 SIP parameters



Parameter	Description	Setting
Register with server	Specifies whether your endpoint registers with a Lync Server. An endpoint that registers with a Lync Server can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with Lync Servers. NOTE If you select this parameter, you must also set Server address , Site number , User name , and Password .	Select this parameter.
Server address	Specifies the IP address or domain name of the Lync Server with which you want	Example 1: 192.168.1.10

Parameter	Description	Setting
	the endpoint to register. If you set this parameter to the Lync Server domain name, enable the domain name server (DNS). If the DNS is not enabled, enable Proxy server .	Example 2: lync.zdtest.com
Conference service number	-	You do not need to set this parameter.
Enable proxy server	-	You do not need to set this parameter.
Proxy server address	-	You do not need to set this parameter.
Site number	Specifies the site number for your endpoint. If your endpoint registers with a Lync Server, endpoints that also register with the Lync Server can dial this site number to call your endpoint.	Example: 123@zdtest.com Obtain this value from the Lync Server administrator.
User name Password	Specifies the user name for authentication registration.	Example: lync_1@zdtest.com Obtain the value of this parameter from the Lync Server administrator.
Server type	Specifies the SIP server type. <ul style="list-style-type: none"> • OCS: Select this option if your endpoint registers with the Microsoft Office Communications Server (OCS) or Microsoft Lync Server. • CISCO VCS: Select this option if your endpoint registers with the Cisco TelePresence Video Communication Server (VCS). • Standard: Select this option if your endpoint registers with other SIP servers. 	Set this parameter to OCS .
Transmission type	Specifies the protocol used for SIP signaling transmission. <ul style="list-style-type: none"> • TCP: Use the Transmission Control Protocol (TCP) to implement transmission reliability. • UDP: Use the User Datagram Protocol (UDP) to implement transmission with reduced latency. • TLS: Use Transport Layer Security (TLS) to implement transmission security. 	Only TCP and TLS transmission are supported.

Parameter	Description	Setting
Video request handling	<p>Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference.</p> <ul style="list-style-type: none"> • Accept automatically: Your endpoint automatically accepts video requests from the remote endpoint. • Reject automatically: Your endpoint automatically rejects video requests from the remote endpoint. • Manual: Your endpoint prompts you to accept video requests from the remote endpoint. 	The default value is Manual .

3. Select **Save**.

Step 2 Place a call from the endpoint to the Lync client.

1. Press  on the remote control.
The **Call** screen is displayed.
2. In the text box, enter the Lync client number.
3. Press **OK** or  on the remote control.

----End

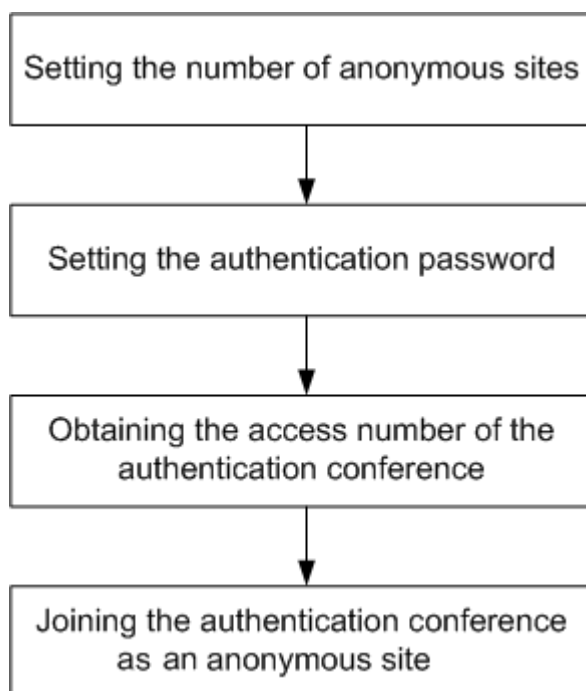
6.3 Joining an Authentication Conference

If you do not know how many sites are expected to join the conference, set the number of anonymous sites and hold an authentication conference. A site can join the authentication conference by calling the specified conference access number.

Background

[Figure 6-1](#) outlines the procedure for joining an authentication conference.

Figure 6-1 Procedure for joining an authentication conference




- Setting the number of anonymous sites: Set the number of anonymous sites when initiating a conference.
- Setting the authentication conference password: When initiating the conference, set **Conference control password**, which functions as the authentication conference password. Anonymous sites must enter this password to join the conference. If **Conference control password** is left blank, anonymous sites can join the conference without entering any password.
- Obtaining the access number of the authentication conference: When a conference starts, endpoints that have joined the conference can view the conference access number by choosing **Advanced > Diagnostics > Status > Conference**. On the displayed screen, the value of **Remote number** is the conference access number. Anonymous sites can obtain the conference access number and authentication password from the SMC administrator or chair site using other methods.
- Joining the authentication conference as an anonymous site: Anonymous PSTN sites can join the conference by dialing the audio access number, and anonymous IP sites can join the conference by dialing the video access number.

Prerequisites

- You have confirmed with the SMC administrator that the conference you want to join has available resources for anonymous sites.
- You have obtained the following from the calling party or SMC administrator: video (or audio) authentication conference access number and authentication conference password.
- The site has registered with the GK server.

Procedure

Step 1 Press  on the remote control.

The **Call** screen is displayed.

Step 2 In the text box, enter the access number of the authentication conference.

Step 3 Press **OK** or  on the remote control.

If the authentication conference is password-protected, the endpoint plays an interactive voice response (IVR), prompting you to enter the password. If the conference is not password-protected, you can join the conference after selecting the desired language.

----End

6.4 Joining an HD-Video Conference over an IMS Network

The endpoint can join an HD video conference over an IMS network.

Background

Borne by the standard IP protocol, IMS uses VoIP applications based on the standard SIP applications of the 3GPP to provide fixed and mobile multimedia services for operators. Integrating MCUs can enhance the functionality of the Huawei IMS HD videoconferencing solution.

Prerequisites

You have obtained the required authentication information from the IMS administrator: unified access number, conference ID, and conference password.



NOTE

Endpoint users can obtain the required authentication information allocated by the IMS through emails, text messages, notices, or other methods.

Procedure

Step 1 Register the endpoint with the network where the IMS is located.

1. Choose **Advanced > Settings > Network > IP > SIP**.
2. Set the parameters for interworking with the IMS described in [Table 6-2](#).


Table 6-2 SIP parameters

Parameter	Description	Setting
Register with server	Specifies whether your endpoint registers with an IMS server. Only endpoints that have registered with IMS servers can join the IMS network. An endpoint that registers with an IMS server can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with IMS	Select this parameter.

Parameter	Description	Setting
	<p>servers.</p> <p>NOTE</p> <p>If you select this parameter, you must also set Server address, Conference service number, Site number, User name, and Password.</p>	
Server address	<p>Specifies the IP address or domain name of the IMS server with which you want the endpoint to register.</p> <p>If you set this parameter to the IMS server domain name, enable the domain name server (DNS). If the DNS is not enabled, enable Proxy server.</p>	<p>IP address example: 192.168.1.10</p> <p>Domain name example: huawei.com</p> <p>It is recommended that you set Server address to the domain name of the IMS server with which you want the endpoint to register.</p>
Conference service number	<p>Specifies the conference service number for your endpoint to initiate conferences over an IP multimedia subsystem (IMS) network.</p>	<p>Set this parameter to the conference service number obtained from the IMS network administrator.</p>
Enable proxy server	<p>Specifies whether to enable the proxy server.</p> <p>You must enable the proxy server when using the IMS network.</p>	<p>Select this parameter.</p>
Proxy server address	<p>Specifies the address of the proxy server.</p> <p>If you set Server address to the IMS server domain name, set this parameter to the IP address bound to that domain name.</p>	<p>Example: 192.168.1.10.</p>
Site number	<p>Specifies the site number for your endpoint.</p> <p>If your endpoint registers with an IMS server, endpoints that also register with the IMS server can dial this site number to call your endpoint.</p>	<p>The parameter value must contain only digits.</p> <p>Example: 12345</p>
User name Password	<p>Specifies the user name for authentication registration.</p>	<p>The value can contain digits, letters, and special characters, such as @ # %.</p> <p>Example: +0867552842007@huawei.com</p> <p>Obtain the value of this parameter from the IMS server administrator.</p>
Server type	<p>Specifies the SIP server type.</p> <ul style="list-style-type: none"> • OCS: Select this option if your endpoint registers with the Microsoft 	<p>Set this parameter to Standard.</p>

Parameter	Description	Setting
	<p>Office Communications Server (OCS) or Microsoft Lync Server.</p> <ul style="list-style-type: none"> • CISCO VCS: Select this option if your endpoint registers with the Cisco TelePresence Video Communication Server (VCS). • Standard: Select this option if your endpoint registers with other SIP servers. 	
Transmission type	<p>Specifies the protocol used for SIP signaling transmission.</p> <ul style="list-style-type: none"> • TCP: Use the Transmission Control Protocol (TCP) to implement transmission reliability. • UDP: Use the User Datagram Protocol (UDP) to implement transmission with reduced latency. • TLS: Use Transport Layer Security (TLS) to implement transmission security. 	<p>Set this parameter to UDP. The IMS network only supports UDP transmission.</p>
Video request handling	<p>Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference.</p> <ul style="list-style-type: none"> • Accept automatically: Your endpoint automatically accepts video requests from the remote endpoint. • Reject automatically: Your endpoint automatically rejects video requests from the remote endpoint. • Manual: Your endpoint prompts you to accept video requests from the remote endpoint. 	<p>The default value is Manual.</p>

3. Choose **Save**.

Step 2 Press  on the remote control to display the **Call** screen.

Step 3 In the text box, enter the conference unified access number.

Step 4 On the remote control, press **OK** or  to initiate the conference.

Enter the required authentication information, such as the conference ID and password, as prompted.

----End

Result

After the IMS authenticates the password, the endpoint can join an HD video conference over an IMS network.

6.5 Scheduling a Conference

On your endpoint, you can schedule a specific time to hold a conference.

Background

You can schedule H.323 or 4E1 conferences on the endpoint.

Prerequisites

- To schedule an H.323 conference:
 - The endpoint is not in use during a conference.
 - The endpoint has registered with a GK, and the **Huawei GK** parameter has been selected. For details, see [3.1.3 Setting H.323 Parameters](#).
 - **Conference line type** has been set to **Auto** or **H.323**. For details, see [13.3 Setting Advanced Conference Parameters](#).

To schedule a 4E1 conference:

- The endpoint is not in use during a conference.
- A SiteCall account has been set on the endpoint. For details about how to set a SiteCall account, see [3.2.3 Setting 4E1 Parameters](#).
- **Conference line type** has been set to **4E1**. For details, see [13.3 Setting Advanced Conference Parameters](#).

Procedure

Step 1 Choose **Advanced > Conference Schedules > Conference**.

Step 2 Schedule a conference using either of the following methods:

- Select a conference from **Conference**, set **Start time** and **Conference duration** (ranging from 30 minutes to 360 minutes), and select **Schedule**.
- Select **Create**. Set the site and conference parameters, set **Start time** and **Conference duration**, and select **Schedule**.

----End

When the conference is scheduled, you can view its information or delete it on the **Conference Schedules** screen.

6.6 Controlling a Conference

During a multipoint conference, you can control the video and audio of the participating sites using conference control functions.

6.6.1 Conference Control for a Non-Chair Site

Non-chair sites have access to only four conference control functions: Request chair, Request floor, View site, and Revoke chair.



NOTE

The Revoke chair function is available only to the site that initiates or pays for a conference.

Viewing a Site

During a conference, the function to view a site is unavailable when the function to broadcast a site or continuous presence is used.

- You view the sites connected to their own MCUs or MCUs of the same level only.
- You can choose to view a single site.
- You can view continuous presence during a conference if the conference supports Continuous presence .



NOTE

During multipoint conferences hosted by standalone MCUs, the endpoint supports multiple continuous presence views.

Request Chair

The conference chair site can use more conference control functions than other sites.

Only non-chair sites can request chair control rights when no chair site exists in a conference. Audio-only sites cannot request chair control rights.

The conference access number is required when a site requests chair control rights. Obtain this number from the SMC administrator or the calling party.

Request Floor

If a non-chair site wants to speak during a conference, the site can request the floor from the chair site.

This function is available only when a chair site exists in the conference. After a site requests the floor, the request is submitted to the chair site. The chair site can then determine whether to give the floor to the site.

- If the chair site gives the floor to the site, the site is broadcast, and all the sites, except the chair site and the site given the floor, are muted.
- If the chair site does not give the floor to the requesting site, the conference status remains unchanged.

Revoke Chair

When chair control rights are revoked, no chair site exists in the conference. Sites in the conference can then request to chair the conference.

Only the site that initiates or pays for the conference can revoke chair control rights.

6.6.2 Conference Control for the Chair Site

Only one site can chair a conference. Another site can chair the conference only after the current chair site releases its chair control rights or the chair control rights is revoked.

The chair site has access to various conference control functions, such as viewing sites, enabling or disabling voice activation, adding sites, setting continuous presence, releasing chair control rights, ending the conference, and broadcasting sites.

View Site

The chair site has full access to view the participant sites in the conference except when the endpoint is broadcasting sites in turn.

- You can view any sites residing on the local MCU and MCUs cascaded to the local MCU.
- You can choose to view a single site or multiple sites in turn at preset intervals.
- You can view a site even when another site is being broadcast in continuous presence.

Broadcast Site

The chair site can broadcast any of the participant sites (except for an audio-only site) in a conference and broadcast multiple sites (including the chair site) in turn at preset intervals.

When a site is broadcast, all non-chair sites are limited to viewing the broadcast site while the chair site can view any site in the conference.

To stop broadcasting, select **Stop** or **Discussion** using the remote control.

The **Stop** function is available when a site is being broadcast. When the chair site stops broadcasting sites, all the sites in the conference can view any other sites.

Give Floor

Using this function, the chair site can give the floor to a site and mute all the other sites.

After the chair site gives the floor to a site, the video and sound of this site are broadcast, and all the sites are muted, except the chair site and the site given the floor. To give the floor to a site, access the **Give Floor** screen, scroll to the site, and press **OK** on the remote control.

To take back the floor, select **Discussion**.

Lock Presentation

During a conference, the chair site can lock the presentation sharing right of a single site or the entire conference.



NOTE

Before using this function, ensure that the MCU and service software used along with your endpoint support this function.

- To lock the presentation sharing right of a single site, select **Lock Conference** and then that site. After the chair site locks the presentation sharing right of a site, only the site can share its presentation. To enable the other sites to share presentations, unlock the presentation sharing right of the site.

- To lock the presentation sharing right of a conference, select **Lock Conference**. After the chair site locks the presentation of the conference, any site in the conference can share a presentation only when no other site is doing so.

Call Site

You can place a call to a site that is not in the conference. The site joins the conference after answering the call.

To call all absent sites included in the conference site list into the conference, select **Call All** on the **Call Site** screen.

Disconnect Site

The chair site can disconnect a participant site from the conference. The site exits the conference automatically upon being disconnected.

Delete Site



During a conference, the chair site can delete a site that is present in or absent from the conference.

After being deleted, the site is removed from the site list and not related to the conference any more. To enable the site to join the conference again, the chair site must add the site to the conference by using the **Add Site** function.

Mute/Unmute MIC

After you have muted the microphone of a site, the other sites in the conference cannot hear the site. To reverse that, unmute the site microphone.



Depending on the microphone status of a remote site, you can mute or unmute the remote microphone after selecting the site:

- : indicates that the microphone of the site is not muted. You can press **OK** to mute the microphone.
- : indicates that the microphone of the site is muted. You can press **OK** to unmute the microphone.

Mute/Unmute Speaker

After you have muted the speaker of a site, the site cannot hear the current conference. To enable the site to hear the conference, unmute the speaker.

Depending on the speaker status of a remote site, you can mute or unmute the remote speaker after selecting the site:

- : indicates that the speaker of the site is not muted. You can press **OK** to mute the speaker.
- : indicates that the speaker of the site is muted. You can press **OK** to unmute the speaker.

Continuous Presence

The continuous presence function simultaneously displays the videos of two or more sites on the same display device. The number of sites to be displayed and the layout of the site videos vary depending on continuous presence modes.



NOTE

This function is available only when continuous presence resources have been reserved for the conference.

To set continuous presence:

Select a pane. From the drop-down list box in the displayed dialog box, select the site whose video you want to display in the pane.

If a site already exists in the pane selected, the site is displaced by the site you just select.

To delete all the sites from continuous presence views, select **Delete All**.

Revoke Presentation

During a dual-stream conference where the **Presentation** mode is adopted, if a non-chair site is sharing its presentation, the chair site can revoke the presentation sharing right of this site.

A site stops sharing its presentation after its presentation sharing right is revoked.

Voice Activation

Voice activation is used in discussion mode. When voice activation is enabled, the site with the highest volume is displayed to other sites in the conference.

Based on your experience, set **Sensitivity** to enable voice activation.

- If the volume of one or more sites exceeds the voice activation threshold, the video of the site with the highest volume is broadcast.
- If the voice activation threshold is not exceeded, the conference status does not change.

To disable voice activation, select **Disable** from the **Voice Activation** drop-down list box.

Release Chair

A non-chair site can request chair control rights only after the chair site releases the chair control rights.

Discussion

The chair site can enable the discussion function to cancel certain ongoing site control or conference control operations, such as broadcasting sites.

This function is used to cancel the following operations performed by the chair site:

- Broadcast site
- Mute Speaker
- Mute Microphone
- Give floor

In discussion mode:

- Audio: All sites have unmuted microphones, and the audio from all these sites is mixed and broadcast to every site.
- Video: The video viewed by each site does not change and each site can view the video of any other site.

Add Site

During a conference, the chair site can add sites to the current conference.

If a site is successfully added to the conference, the site becomes a participant of the conference. You can add a site no matter whether it included or not included in the address book.


Extend Conference

This function enables you to extend a conference that is not likely end as scheduled.

Before extending a conference, ensure that the videoconferencing resources and your account balance are sufficient. To increase the chances of success, extend the conference by a maximum of 30 minutes at a time.

End Conference

If a conference is complete before the scheduled time, you can use this function to end it in advance.

To end a conference, select **End Conference** on the **Conference Control** screen or press  on the remote control. Then confirm your action.

6.7 Recording a Conference

Your endpoint can record conferences if your site is the chair site.

Prerequisites

- The recording server is online.



NOTE

Check the recording server's online status from SMC (Service Management Center).

- Your endpoint is in a multipoint conference hosted by a standalone MCU, such as the HUAWEI VP9660.
- The ongoing multipoint conference supports recording.
- Your site is chairing the conference.

Background

If you are using a standalone MCU to schedule or initiate a conference, you must select **Support recording** when setting conference parameters.

Procedure

Step 1 Select **Control Recording** from the option bar.

Step 2 Select **Start**.

The recording starts.

----End

Follow-up Procedure

To stop recording, select **Stop**.

6.8 Managing the Address Book


The address book stores site information. You can add, edit, and delete site entries.

The address book saves time because you do not need to enter site information to initiate a conference and prevents entry of incorrect IP addresses.



NOTE

You can save sites listed in the conference history to the address book. To do so, choose **Advanced** >

Address Book > **Conference History** and select  next to the desired sites.

6.8.1 Configuring the Network Address Book

A network address book stores the addresses of the sites in the videoconferencing system. You can download a network address book to update the entries in the local address book in batches.

Network address books can be stored on:

- File Transfer Protocol over SSL (FTPS) or File Transfer Protocol (FTP) server
- LDAP server

Configuring the FTPS or FTP Network Address Book

Step 1 Choose **Advanced** > **Settings** > **Network** > **Network Address Book** > **Network Address Book**. Set the network address book parameters described in [Table 6-3](#).

Table 6-3 Network address book parameters

Parameter	Description	Setting
Enable network address book	Specifies whether to enable the network address book. If you enable this function, set the other parameters listed in this table.	This parameter is not selected by default.
Synchronize automatically	Specifies whether your endpoint automatically downloads site entries from the network address book to the local address book when it is powered on.	This parameter is not selected by default.
FTPS	Specifies whether to use FTPS to encrypt data through the SSL and ensure data	This parameter is selected by default.

Parameter	Description	Setting
	integrity. If FTPS is not used, the endpoint uses FTP, which is insecure.	To improve communication security, retain the default value.
Local records prevail if duplicates exist	Specifies whether the following function is enabled: If some entries in the network address book on the FPTS or FTP server already exist in the local address book, these entries remain unchanged when the local address book is updated.	This parameter is not selected by default.
Clear local records during update	Specifies whether your endpoint automatically clears the local address book when updating the local address book.	This parameter is not selected by default.
Prompt users during update	Specifies whether a message is displayed to prompt you to update the local address book if the versions of the network and local address books are different. When you confirm the update, site information in the network address book is downloaded to the local address book.	This parameter is selected by default.
Server address	Specifies the IP address of the server that stores the network address book.	No default value is set for this parameter.
File path	Specifies the save path to the network address book on the server.	No default value is set for this parameter.
User name Password	Specify the user name and password your endpoint uses to access the network address book.	No default value is set for this parameter.

Step 2 Select **Save**.

----End

Downloading the FTPS or FTP Network Address Book

After you select **Synchronize automatically**, the endpoint automatically downloads the latest network address book each time it is powered on. For details about the **Synchronize automatically** parameter, see [Table 6-3 in Configuring the FTPS or FTP Network Address Book](#).

If you have not selected this function, select **Update** on the **Address Book** screen to update the FTPS or FTP network address book.



NOTE

The downloaded address book is saved in vCard format. The file name extension is vcf.

Configuring the LDAP Network Address Book

Step 1 Choose **Advanced > Settings > Network > Network Address Book > LDAP Server**. Set the LDAP server parameters described in [Table 6-4](#).

Table 6-4 LDAP server parameters

Parameter	Description	Setting
Server address	Specifies the LDAP server IP address.	No default value is set for this parameter.
Port	Specifies the port used to connect to the LDAP server.	The default value is 389 .
Base DN	Specifies the distinguished name (DN) of the entry at which a specified search starts.	No default value is set for this parameter.
Authentication type	Specifies the type of LDAP server authentication. <ul style="list-style-type: none"> • General: Use the user name and password for authentication. • Secured: Perform authentication, including authentication on digital certificates, based on the Secure Sockets Layer (SSL) protocol. If you select this value, you must also set Domain name. • Anonymous: No authentication is performed. The LDAP server is accessible to all users. 	The default value is General .
SSL encryption	Specifies whether the SSL protocol is used to encrypt data streams sent to and received from the LDAP server.	This parameter is not selected by default.
User name Password	Specifies the user name and password used for LDAP server authentication.	Their default values are both admin . The value can contain digits, letters, and special characters, such as @ # %.
Domain name	Specifies the domain name used for LDAP server authentication. This parameter is mandatory only when Authentication type is set to Secured .	No default value is set for this parameter.
Synchronize automatically	Specifies whether your endpoint regularly updates the LDAP Address Book entries in the local address book. If you select this parameter, you must also set Automatic update interval and Local records prevail if duplicates exist .	This parameter is selected by default.

Parameter	Description	Setting
Local records prevail if duplicates exist	Specifies whether the following function is enabled: If some entries in the network address book on the LDAP server already exist in the local address book, these entries remain unchanged when the local address book is updated.	This parameter is not selected by default.
Automatic update interval	Specifies the interval for updating the LDAP Address Book entries in the local address book.	The default value is 24 h .




Step 2 Select **Save**.

----End

Searching the LDAP Network Address Book for Sites

After the LDAP server parameters are set, your endpoint can communicate with the LDAP server. On the **Address Book** page, you can search for sites stored in the LDAP network address book. Select the sites you want to save to the local address book and click **Save**. [Table 6-5](#) lists the online status icons for LDAP sites.

Table 6-5 Online status icons

Icon	Description
	Available
	Busy
	Offline

6.8.2 Managing the Local Address Book

You can add, delete, or edit site information in the local address book.

To view the local address book, choose **Advanced > Address Book** on the remote controlled UI, or click the **Address Book** tab on the endpoint web interface.

To quickly add, delete, or search for address book entries, it is recommended that you perform these operations on the endpoint web interface where you can click the **Help** tab for instructions on how to operate the local address book.

Background

Sites and site groups you add to the local address book are automatically saved to the respective lists on the **Address Book** screen.


The following parameters are important site attributes: **Name**, **Number**, **Rate**, **Type**, and **IP address**. Table 6-6 lists these parameters.

Table 6-6 Site parameters

Parameter	Description	Setting
Category	Specifies the category of the site.	The default value is Ordinary site . <ul style="list-style-type: none"> • Ordinary site: Select this option for a traditional videoconferencing site. • Telepresence site: Select this option for a Huawei telepresence site. • CT site: Select this option for a Cisco TelePresence site.
Type	Specifies the line the site uses to access the videoconferencing network. <ul style="list-style-type: none"> • If you select IP, your endpoint uses the protocol specified Preferred IP protocol to call the site. • If you set Category to CT site, the available value for this parameter is SIP. 	The default value is H.323 .
Number	Specifies the site number used to place calls between sites. <ul style="list-style-type: none"> • IP, T1, 4E1, basic rate interface (BRI), and H.323 phone site numbers are allocated by the videoconferencing service provider. • PSTN site numbers are telephone numbers. 	No default value is set for this parameter.
IP address	Specifies the site IP address. NOTE This parameter is unavailable if you set Category to IP address .	No default value is set for this parameter.
Rate	Specifies the call rate for the line selected for a remote endpoint. The call rates supported vary depending on the type of the site you want to call.	The default value is 8Mbps . Select the highest available call rate.
URI	Specifies the uniform resource identifier (URI) of the site, for example, abcd@huawei.com . NOTE This parameter is available only when Type is set to IP , H.323 , or SIP .	No default value is set for this parameter.

Adding a Site

Step 1 On the **Address Book** screen, select **All Sites**.

Step 2 If no site is displayed, select **Add site**. If sites are displayed, select  next to any site.

Step 3 In **Create Site**, name the site you want to add.


Step 4 Set the site parameters described in [Table 6-6](#).

Step 5 Select **Save**.

----End

Creating a Group

Step 1 On the **Address Book** screen, select **All Groups**.

Step 2 If no group is displayed, select **Add Group**. If groups are displayed, select  next to any group.

Step 3 In **Create Group**, name the group.

Step 4 Select the sites you want to add to the group.

After being selected, a site has a check mark (√) displayed before it and is listed in the group box.


Step 5 Select **Save**.

----End

Modifying a Site Entry

Select a site or group, press **OK** on the remote control, and modify the site or group settings.

Deleting a Site Entry

Select  next to the desired site or group to delete it from the address book.

Searching for a Site Entry

Enter the search criteria in the **Search** text box. The displayed query results are filtered in real time based on what you enter.

For example, after you enter 12 in the text box, sites whose names, site numbers, or IP addresses containing the number 12 are displayed in the site list. To perform an exact search for a site, enter the whole name of the site in the text box.

6.8.3 Importing and Exporting an Address Book

From the endpoint web interface, you can export an address book to the local computer or a server. This facilitates site information editing. You can also import a modified address book

to the endpoint after which the records in the address book are displayed on the address book page.

Background

The exported address book is saved to a file in vCard format. The file name extension is vcf.

For example, you can export the address book of endpoint A, modify the records in the address book, and then import these records to the address book of endpoint B.

The exported contacts file may contain personal information. Keep the file in a safe location to prevent personal information disclosure.

Exporting an Address Book

To export an address book:

Step 1 Log in to the web interface of endpoint A. Choose **Address Book > Address Book**.

Step 2 Select **Export from Local Address Book**.

Step 3 Select a character encoding format for the address book.

- **International:** The character set is UTF-8.
- **Local:** The character set is GB2312.

It is recommended that you retain the default value **International**.

Step 4 Save the records to file A.

----End

Modifying Records in the Address Book

After exporting the address book of endpoint A to file A, modify its records as follows:

Use a text editor to open file A. Based on the notes of the parameters in the file, modify file A so that it applies to endpoint B. Save the modified file as file B.

Importing the Address Book

To import the address book to endpoint B:

Step 1 Log in to the web interface of endpoint B. Choose **Address Book > Address Book**.

Step 2 Click **Import to Local Address Book** and select file B to import.


Step 3 Click **Import**.

----End

6.8.4 Customizing a Site Template

A site template is used to group sites for easy site management. In this template, the sites are identified by their site names.

Creating a Site Template

- Step 1** Log in to the endpoint web interface. Choose **Address Book > Site Template**.
- Step 2** Click **Create**.
- Step 3** In **Template Name**, enter a template name, for example, **test**.
- Step 4** Add a group to the template, as the **test** template in the following example:
1. Click **Create Group**.
The **Add group** group is displayed under **Group Name**.
 2. Double-click the **Add group** group and change the group name to, for example, **group1**.
- Step 5** Add sites to the new group, as the **group1** group in the following example:
- Select **group1** under **Group Name**. Click **Add from Address Book** to add sites from the address book, or click **Add Temporary Site** to add temporary sites.
- Step 6** Repeat [Step 4](#) to add another group to the template.
- Step 7** Repeat [Step 5](#) to add sites to the new groups.
- Step 8** Click **Save**.
- After being saved, a site template is displayed under **Template Name**.
- When one of the sites in the site template is in a conference, the site template name is listed in the  drop-down list box on the **Conference Control** page.
- End

Editing a Site Template

- Step 1** Log in to the endpoint web interface. Choose **Address Book > Site Template**.
- Step 2** From the **Template Name** drop-down list box, select the site template you want to edit. Click **Edit**.
- Step 3** Modify the settings of the site template.
- Step 4** Click **Save**.
- End

Deleting a Site Template

- Step 1** Log in to the endpoint web interface. Choose **Address Book > Site Template**.
- Step 2** Select the site template you want to delete.
- Step 3** Click **Delete**.
- End

6.9 Managing Captions

You can create a caption on your endpoint. In addition, you can share the caption with remote sites during a conference.

Your endpoint supports T.140 and non-T.140 captions. [Table 6-7](#) describes the differences between these caption types.

Table 6-7 Comparison between non-T.140 and T.140 captions

Non-T.140 Caption	T.140 Caption
Superimposed on the video of your site and sent with the video to remote sites	Not superimposed on the video of your site, sent to remote sites, and displayed on remote displays
Can be sent and received by Session Initiation Protocol (SIP) and H.323 endpoints	Can be sent and received by H.323 endpoints only
Can be sent and received by all endpoints	Can be sent and received only by endpoints that support T.140 captions
Can be sent only from endpoints in a conference	Can be sent from any of the following in a conference: <ul style="list-style-type: none"> Endpoint used at the chair site SMC2.0 Endpoint used by either party during a point-to-point call

6.9.1 Specifying Caption Settings

Caption settings include the caption font size, color, and background.

Procedure

- Step 1** Choose **Advanced > Settings > Display > Caption**. Set the caption parameters described in [Table 6-8](#).

Table 6-8 Caption parameters

Parameter	Description	Setting
Font size	Specifies the font size for banners and middle and bottom captions.	Default values: <ul style="list-style-type: none"> For banners, the default value is Largest. For middle and bottom captions, the default value is Medium.
Background color	Specifies the background color of banners and middle and bottom captions in any of 64	Default values: <ul style="list-style-type: none"> For banners, the default

Parameter	Description	Setting
	colors.	<p>color is red.</p> <ul style="list-style-type: none"> For middle and bottom captions, the default color is gray.
Font color	Specifies the foreground color of banners and middle and bottom captions in any of 64 colors.	The default color is white.
Transparency	Specifies banner or caption transparency.	The default value is Half transparent .
Scrolling speed	Specifies the percentage of the banner or bottom caption height to the entire screen.	The default value is 10% .
Effect	Specifies the display effect for banners and middle and bottom captions.	<p>Default value:</p> <ul style="list-style-type: none"> For banners, the default value is Center. For middle captions, the default value is Scroll upward. For bottom captions, the default value is Scroll leftward.
Scrolling speed	Specifies the scroll rate for middle and bottom captions.	<p>Adjust the rate based on the preview.</p> <p>The default value is Fast.</p>
Font Type	Specifies the font type of captions.	The default value is Boldface .
Line spacing	Specifies the vertical spacing between lines when there are multiple lines of middle captions.	The default value is Small .
Bold	Specifies whether banners or captions are displayed in bold.	<ul style="list-style-type: none"> For banners, this parameter is selected by default. For middle and bottom captions, this parameter is not selected by default.
Sharing mode	Specifies the type of the caption to be shared, T.140 or non-T.140. For the differences between T.140 and non-T.140 captions, see Table 6-7 .	The default value is T.140 .

Step 2 Select **Save**.

----End

6.9.2 Creating a Banner or Caption

You can create and preview a banner or caption on your endpoint.

Procedure

Step 1 Choose **Advanced > Utilities**.

The **Utilities** screen is displayed.

Step 2 Select **Middle Caption, Banner**, or **Bottom Caption**.

Step 3 Select **New** and compose the desired banner or caption.

----**End**


After a banner or caption is created, you can preview, share, or edit it.

7 Security

About This Chapter

To improve communication security, you can encrypt conferences, set or change conference passwords, and disable remote access to the endpoint.

7.1 Setting the Administrator Password

To prevent endpoint parameter settings from being modified by unauthorized users, anyone who wants to access the **Settings** screen and use the customized tool bar  on the menu screen must provide the administrator password if the password is not set to blank.

7.2 Enabling Encryption

On an IP network, which is neither quality-guaranteed nor secure, encryption can be used to increase video communication security.

7.3 Supporting Remote Logins

You can specify whether remote users can log in to the endpoint to manage it using the endpoint web interface, SSH, or Telnet.


7.4 Setting the Upgrade Password

You can set the password required to upgrade the endpoint software using the upgrade tool.

7.5 Setting the Air Content Sharing Password

When connecting to the endpoint, an air content sharing client must provide the predefined password.

7.1 Setting the Administrator Password

To prevent endpoint parameter settings from being modified by unauthorized users, anyone who wants to access the **Settings** screen and use the customized tool bar  on the menu screen must provide the administrator password if the password is not set to blank.

Procedure

- Step 1** Choose **Advanced > Settings > Secured > Password**. Set the administrator password parameters described in [Table 7-1](#).

Table 7-1 Administrator password parameters

Parameter	Description	Setting
Current password New password Confirm password	Specifies the new administrator password for the remote controlled UI.	The default value is 12345678 . The password contains a maximum of 32 characters. To improve device security, set a password at your first login. If you set this password to blank, no password is required when you access the Settings screen.
Encryption advanced settings	Specifies whether to encrypt the Advanced Settings screen of the remote controlled UI. If this parameter is enabled, you must enter the administrator password to access the Advanced screen. If this parameter is disabled, the administrator password is required only when you select Settings on the Advanced screen.	This parameter is not selected by default.

- Step 2** Select **Save**.

----End

7.2 Enabling Encryption

On an IP network, which is neither quality-guaranteed nor secure, encryption can be used to increase video communication security.

Background

Encryption can be H.235 or SRTP encryption.

Both parties involved in communication must support encryption; otherwise, encryption fails.

Procedure

- Step 1** Choose **Advanced > Set > Security > Encryption** and select an encryption policy.

- **Disable:** No stream is encrypted.
- **Enable:** Stream encryption is mandatory. If you select this option, the endpoint can only attend encrypted conferences. If a remote site is also encryption capable, an encrypted conference is initiated upon successful call connection with the remote site. If the remote site is encryption incapable, the call to the remote site fails.
- **Maximum interconnectivity:** Media streams are encrypted only when a call is set up. If you select this option for the local site, the conferences between the local and remote sites are not encrypted only when **Disable** is selected for the remote sites.

Step 2 Choose **Save**.

----End

7.3 Supporting Remote Logins

You can specify whether remote users can log in to the endpoint to manage it using the endpoint web interface, SSH, or Telnet.

Web-based Login

Step 1 Choose **Advanced > Settings > Secured > Web Login**. Set the web-based login parameters described in [Table 7-2](#).

Table 7-2 Web-based login parameters

Parameter	Description	Setting
Web Login	Specifies whether a remote user can log in to the endpoint web interface to perform operations such as setting endpoint parameters, controlling the endpoint, and viewing the endpoint status. If you select this parameter, you must also set the administrator user name and password.	This parameter is selected by default.
Administrator name Current password New password Confirm password	Specify the user name and password used to log to the endpoint web interface.	The administrator name cannot be left blank and contains a maximum of 64 case-sensitive characters. In New password , enter a string of 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character. The default administrator name is admin . The default administrator password is Change_Me .

Parameter	Description	Setting
		To protect against unauthorized access, change the password at your first login.
SSL encryption	Specifies whether to enable Security Socket Layer (SSL) encryption to improve transmission security. When SSL encryption is enabled, the touch panel must use Hypertext Transfer Protocol Secure (HHTPS) to connect to the endpoint.	When the data to be transferred must be highly secured, it is recommended that you select SSL encryption . This parameter is selected by default.
Monitor video	Specifies whether to allow remote users to log in to the endpoint web interface to view local and remote videos and presentations and take pictures. For details, see 9.3.8 Monitoring the Video .	This parameter is not selected by default. NOTICE This function involves privacy protection. Ensure that its use complies with local laws and regulations.

Step 2 Select **Save**.

----End

SSH and Telnet Login

Step 1 Choose **Advanced > Settings > Secured > SSH/Telnet**. Set the SSH and Telnet login parameters described in [Table 7-3](#).

Table 7-3 SSH and Telnet login parameters

Parameter	Description	Setting
Telnet Login	Specifies whether remote users can log in to the endpoint in Telnet mode for maintenance and configuration purposes, such as querying system logs and status information. NOTICE If the computer you use to telnet to your endpoint runs Linux, specify the Telnet port on the endpoint by running telnet endpoint IP address port number . For example, run telnet 10.11.12.123 23 where 23 is the port number.	This parameter is selected by default. The default user name and password for telnetting to the endpoint are debug and Change_Me respectively. To protect against unauthorized access, change the password at your first login.
SSH	Specifies whether to enable SSH, which improves transmission	This parameter is selected by default.

Parameter	Description	Setting
	security and prevents information disclosure.	The default user name and password for logging in to the endpoint in SSH mode are debug and Change_Me respectively. To protect against unauthorized access, change the password at your first login.



NOTE

- A maximum of three users is allowed to simultaneously log in to the endpoint in SSH mode.
- A maximum of seven users is allowed to simultaneously log in to the endpoint in SSH and Telnet modes.

Step 2 Select **Save**.

----End

7.4 Setting the Upgrade Password

You can set the password required to upgrade the endpoint software using the upgrade tool.

Step 1 Choose **Advanced > Settings > Secured > Upgrade password**. Set the upgrade password parameters described in [Table 7-4](#).

Table 7-4 Upgrade password

Parameter	Description	Setting
Upgrade password	Specifies the password required to upgrade your endpoint software using the upgrade tool.	Default value: Change_Me The password contains 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character. To improve device security, set a password at your first login.

Step 2 Choose **Save**.

----End

7.5 Setting the Air Content Sharing Password

When connecting to the endpoint, an air content sharing client must provide the predefined password.

Background

For details about how to download and use an air content sharing client, see [9.3.3 Downloading an Air Content Sharing Client](#).

Procedure

Step 1 Choose **Advanced > Settings > Security > Air content sharing**. Set the air content sharing password described in [Table 7-5](#).

Table 7-5 Air content sharing password

Parameter	Description	Setting
Password	Specifies the password an air content sharing client uses to connect to the endpoint.	Default value: Change_Me The password contains 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character. To improve device security, set a password at your first login.

Step 2 Choose **Save**.

----End

8 Screen Customization

About This Chapter

You can customize the menu option bar, conference control functions, and status icons.

8.1 Customizing the Home Screen

You can customize the home screen, such as specifying whether the site name, IP address, system time, or date is displayed.

8.2 Customizing Onscreen Status Icons

You can customize which status icons are displayed on the home screen, helping you quickly understand the endpoint's status.

8.3 Customizing Conference Control Functions to Be Displayed

You can customize the conference control functions you want to display on the **Conference control** screen to quickly access these functions.

8.4 Customizing the Option Bar

You can customize icons on the option bar to facilitate access to the corresponding screens.

8.1 Customizing the Home Screen

You can customize the home screen, such as specifying whether the site name, IP address, system time, or date is displayed.

Choose **Advanced > Settings > Display > Personalize**. Set the custom parameters described in [Table 8-1](#).

Table 8-1 Custom parameters

Parameter	Description	Setting
Transparency	Specifies the transparency of the background image displayed on the remote controlled UI. If you set this parameter to Opaque , the background image is not displayed on	The default value is 15% .

Parameter	Description	Setting
	operation screens except for the call and menu screens. If you set this parameter to any other value, you can vaguely see the background image on all operation screens.	
Display IP address	Specifies whether to display the local IP address on the conferencing screen.	This parameter is selected by default.
Select conference controls	Specifies the conference control functions you want to display on the Conference Control screen.	None
Site name	Specifies the site name you want to be superimposed on the video of your site when it displays to other sites. When your site joins a multipoint conference, this site name is displayed in the site list.	The default value is site .
Display position	Specifies the position where your site name is superimposed on the video of your site.	The default value is Lower right corner .
Display duration	Specifies the duration for displaying a site name.	The default value is Always display .
Display time and zone	Specifies whether the time zone and time are superimposed on the local video sent to remote sites. The time zone and time are not displayed on the local video shown on the display device at your site.	This parameter is not selected by default.
Font color	Specifies the color in which a site name is displayed.	The default color is white.
Font size	Specifies the font size for the site name display.	The default value is Medium .
Font Type	Specifies the typeface of a site name. This parameter is available only when Language is set to 中文.	The default value is Boldface .
Bold	Specifies whether a site name is displayed in bold.	This parameter is not selected by default.
Set the horizontal offset	Fine-tunes the site name's position left or right on the local video.	Value range: 0-96. The default value is 48 .
Set the vertical offset	Fine-tunes the site name's position up or down on the local video.	Value range: 0-96. The default value is 48 .

8.2 Customizing Onscreen Status Icons

You can customize which status icons are displayed on the home screen, helping you quickly understand the endpoint's status.

Packet Loss Rate Icon



To set thresholds (A and B) for the packet loss rate, choose **Advanced > Settings > Display > Packet Loss Threshold**.

By comparing the packet loss rate on the current network with threshold A and threshold B, the endpoint determines whether to display the packet loss rate icon on the remote controlled UI. The policy is as follows:



NOTE

Threshold A must be less than threshold B. Their value ranges are 0.1% to 100%. The default values for threshold A and threshold B are **1%** and **5%**, respectively.

- If the packet loss rate is less than or equal to threshold A, no packet loss rate icon is displayed.
- If the packet loss rate is between threshold A and threshold B,  is displayed.
- If the packet loss rate is greater than or equal to threshold B,  is displayed.

Other Icons

A status icon is displayed on screens if the following conditions are met:

- You have set the icon as follows:
Choose **Advanced > Settings > Display > Icon** and select the icon.
- The function or the condition that corresponds to the status icon has been enabled.

For details about common status icons, see [C Status Icons](#).

8.3 Customizing Conference Control Functions to Be Displayed

You can customize the conference control functions you want to display on the **Conference control** screen to quickly access these functions.

Background

The following conference control functions are displayed by default: **Continuous Presence**, **Discussion**, **Give floor**, **Voice activation**, **Add site**, **Request floor**, **Enable Chair Control**, **Lock conference**, and **Restore Auto Continuous Presence**.

Procedure

Step 1 Choose **Advanced > Settings > Display > Personalize > Select conference controls**. Select the conference control functions you want to display on the **Conference control** screen.




Step 2 Select **Save**.

----End

8.4 Customizing the Option Bar

You can customize icons on the option bar to facilitate access to the corresponding screens.


Background

- To hide the option bar
Press the left arrow key, , or  on the remote control.
- To show the option bar
Press  on the remote control.

Procedure

Step 1 Press  on the remote control.

The menu screen is displayed.

Step 2 Select  on the option bar to display the **Customize Option Bar** screen.

 **NOTE**

If the administrator password is not set to blank, to access the **Customize Option Bar** screen, you must enter the administrator password whose default value is **12345678**.

Step 3 Select the icon you want to move and select **Up** or **Down**.

To show or hide an icon on the option bar, use the remote control to select or deselect the icon.

Step 4 Select **OK**.

----End

9 Embedded Web Management Interface

About This Chapter

The built-in web server of the endpoint allows you to operate the endpoint in web mode, for example, to set endpoint parameters, control the endpoint, and view endpoint status.

The features for operating the endpoint using the web interface include the following:

- A computer is used to access the IP network where the endpoint is located.
- When you log in to the endpoint using the web interface, the endpoint web pages are displayed.
- A maximum of 10 users can log in to the endpoint web interface simultaneously. The administrator can configure the endpoint, while standard users can customize only personal settings.
- A user who uses the remote control to operate the endpoint has more rights than a user who logs in to the endpoint using the endpoint web interface. The former can grant control rights to or revoke the control rights of the latter.
- On the endpoint web interface, you can import and export address books and configuration files.
- You can import license files on the endpoint web interface.
- You can download an air content sharing client from the endpoint web interface.
- The multi-view function is supported on the endpoint web interface.
- With regard to inputting information in quantity, such as adding sites to an address book, using the endpoint web interface is more convenient than using the remote control.

9.1 Web Browser

Before using the endpoint web interface for remote management, configure the web browser on your computer.

9.2 Logging In to the Endpoint Web Interface

To remotely manage the endpoint in web mode, log in to its web interface.

9.3 Getting to Know Web Interface Functions

The functions provided by your endpoint are reorganized on its web interface so you can conveniently use them with a web browser.

9.1 Web Browser

Before using the endpoint web interface for remote management, configure the web browser on your computer.

Background

The web interface can run on Microsoft Internet Explorer, Mozilla FireFox, and Google Chrome. Microsoft Internet Explorer 8.0 is recommended. If you use other browsers or versions, the user interface (UI) display may appear slightly different. The web interface will still work as expected.



NOTE

Before you begin, ensure that the latest patches for the operating system and browser are installed.

Before running the endpoint web interface on a web browser, configure the browser. The following description uses Window XP as an example to describe how to configure Microsoft Internet Explorer 8.0 and FireFox 3.6. The methods for configuring other browser versions are similar.

Procedure

- Step 1** Start Internet Explorer.
- Step 2** From the Internet Explorer menu bar, choose **Tools > Internet Options**. In the displayed **Internet Options** dialog box, click the **Security** tab.
- Step 3** In the bottom of the tab, click **Custom level**.
- Step 4** In the displayed **Security Settings** dialog box, set all options under **Downloads** and **Scripting** to **Enable**. Click **OK**.
- Step 5** (Optional) On the **Security** tab, click **Trusted sites** and then **Sites**.
The **Trusted sites** dialog box is displayed.
- Step 6** (Optional) In the **Add this website to the zone** text box, enter the IP address of your endpoint. Then click **Add**.
- Step 7** (Optional) Click **OK**.
- Step 8** Click the **Privacy** tab. Move the slider to display the **Medium** level.
- Step 9** Click **OK**.

The configuration is complete.

----End



NOTE

To ensure that information can be properly displayed, if you choose to skip [Step 5](#) through [Step 7](#), choose **Tools > Pop-up Blocker > Turn Off Pop-up Blocker** from the menu bar of Internet Explorer.

To set Firefox, do the following:

Start the Firefox. On the menu bar, choose **Tools > Options**. On the **Main** tab, select **Show the Downloads window when downloading a file**. On the **Privacy** tab, select **Accept cookies from sites**. Then select **OK**.

9.2 Logging In to the Endpoint Web Interface

To remotely manage the endpoint in web mode, log in to its web interface.

Prerequisites

The correct security certificate has been imported into the endpoint. For details about how to import a security certificate, see [9.3.7 Importing a Certificate](#).

You have enabled the web login function. For details about how to enable the function, see [7.3 Supporting Remote Logins](#).

Procedure

Step 1 Open Internet Explorer.

Step 2 In the address box, enter the endpoint IP address, such as **10.10.10.10**.

Step 3 Press **Enter**.

The login page is displayed.

Step 4 Fill in **User name** and **Password**.



NOTE

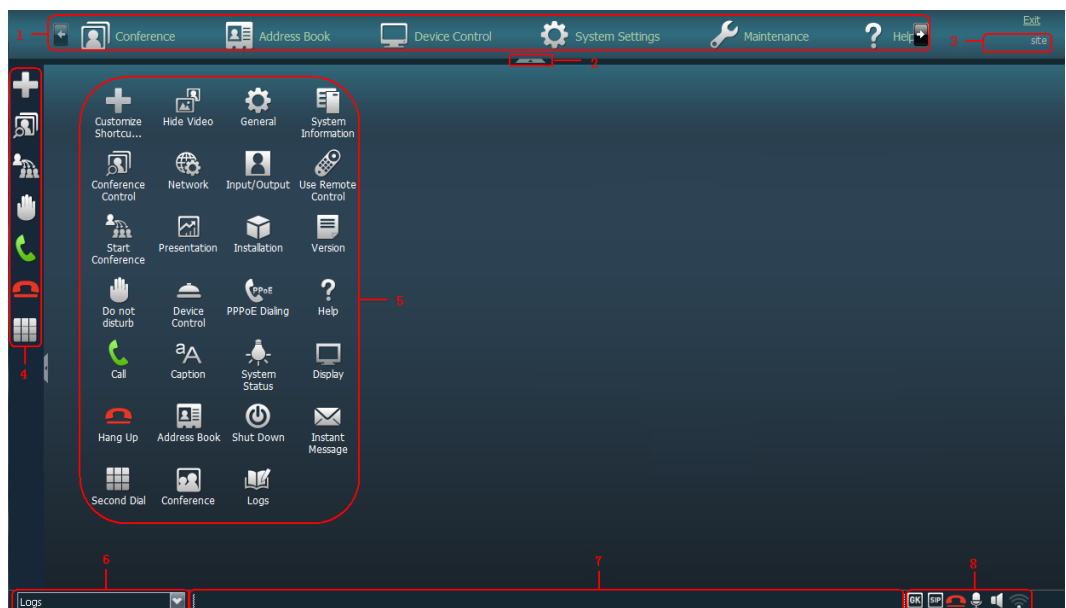
The default user name and password are **admin** and **Change_Me** respectively.

Step 5 From the **Language** drop-down list, select a language.

Step 6 Select **Log In**.

The home page is displayed, as shown in [Figure 9-1](#).

Figure 9-1 Home page of the endpoint web interface



1 Menu bar

2 Expand/Collapse
button

3 Area for displaying your
site name

4 Shortcut bar

- 5 Desktop icons 6 Area for displaying logs 7 Area for displaying messages 8 Status icons

----End



NOTE

To ensure data security, after accessing the endpoint web interface, close the browser and delete browser caches.

9.3 Getting to Know Web Interface Functions

The functions provided by your endpoint are reorganized on its web interface so you can conveniently use them with a web browser.

The following are the functions unique to the web interface:

- Importing and exporting an address book, see [6.8.3 Importing and Exporting an Address Book](#).
- Importing and exporting settings
- Importing a license file
- Downloading an air content sharing client
- Setting the multi-view mode
- Customizing the shortcut bar and desktop icons
- Providing the site map
- Customizing site templates (For details, see [6.8.4 Customizing a Site Template](#).)
- Monitoring the video
- Importing a certificate
- Using the virtual remote control
- Setting SNMP parameters (For details, see [13.4 Setting SNMP Parameters](#).)
- Upgrading the endpoint by importing upgrade files (For details, see [11.4 Upgrading the Endpoint on Its Web Interface](#).)

9.3.1 Importing and Exporting Settings

On the endpoint web interface, you can import and export settings. If your endpoint is restored to its default settings, you can import previously exported settings.

Procedure

Step 1 Log in to the endpoint web interface. Choose **System Settings** > **Installation**.

The **Installation** page is displayed.

Step 2 Select **Import/Export Settings**.

The **Import/Export Settings** page is displayed.

Step 3 Select **Export Settings** to export or **Import Settings** to import.

----End

9.3.2 Importing License Files

Some functions on your endpoint, such as Wi-Fi and recording, require license files.

Prerequisites

You have obtained the latest license files.



NOTE

From <http://enterprise.huawei.com>, you can use your contract number and device serial number to download license files.

Background

Your endpoint can start properly even when no license file is loaded on it or the existing license file has expired. After startup, you can load a valid license file, set parameters, and upgrade software.

When a license file is updated, the original license file expires. For example, after you purchase an official license, the trial license will expire.

Procedure

Step 1 Log in to the endpoint web interface. Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import License**.

The **File upload dialog** dialog box is displayed.

Step 3 Click **Select File**, select the license file you want to import and click **Import**.

Step 4 Click **Back** when **OK** is displayed.

----End

9.3.3 Downloading an Air Content Sharing Client

You can download an air content sharing client from the endpoint web interface. With this client, you can connect your endpoint to presentation sources and share presentations without the use of any physical ports.

Prerequisites

- You have enabled the web login function. Choose **Advanced > Settings > Secured > Web Login** and select **Web Login**.
- An air content sharing client is not available when you are using the remote desktop.
- A computer for air content sharing must run any of the following operating systems:
 - 32-bit Windows Vista
 - 64-bit Windows Vista
 - 32-bit Windows 7

- 64-bit Windows 7
- 32-bit Windows XP

Background

An air content sharing client supports coded transmission resolutions of 720p and 1024 x 768 pixels and a maximum frame rate of 15 fps.

If the computer and endpoint are on the same LAN, you can share your desktop as a presentation without using a VGA cable to connect the video output port on the computer to the presentation input port on the endpoint.

You cannot connect multiple computers to the same endpoint to implement air content sharing. For example, if two computers A and B are available in a conference and their desktops are required to be shared as presentations in turn during the conference, you can separately install air content sharing clients on these two computers. When the desktop of computer A is required to be shared as the presentation, connect computer A to the endpoint. When the presentation sharing stops, disconnect computer A from the endpoint and connect computer B to the endpoint to share computer B's desktop as the presentation.

You can download an air content sharing client only on the login page of the endpoint web interface. If you have logged in to the endpoint web interface, click **Exit** on the upper right corner to display the login page. Then, you can download an air content sharing client on that page. You can also enter the IP address of another endpoint in the address box of Internet Explorer and download an air content sharing client on the login page of that endpoint's web interface.

Procedure

- Step 1** Open Internet Explorer.
 - Step 2** In the address box, enter the endpoint IP address, such as **10.10.10.10**.
 - Step 3** Press **Enter**.
The login page is displayed.
 - Step 4** On the upper left corner, click **Download Air Content Sharing Client**.
The **Downloads** dialog box is displayed.
 - Step 5** Click **Save** and select a save path for the air content sharing client.
- End


Usage of an Air Content Sharing Client

- Step 1** Double-click the installation program of the air content sharing client and complete the installation by following onscreen instructions.



The icon of the air content sharing client is displayed on the desktop when the installation is complete.



- Step 2** Double-click  .

The air content sharing dialog box is displayed.

Step 3 Connect the client to an endpoint using either of the following methods:

- In the list of endpoint search results, double-click the desired endpoint.
- Enter the IP address of the desired endpoint and click **Connect**.

Step 4 (Optional) In the displayed dialog box, enter the password and click **Connect**.

The default password is **Change_Me**. For details, see [7.5 Setting the Air Content Sharing Password](#).



NOTE

The "An Air Content Sharing source device requests to connect to your endpoint. Accept?" message is displayed on the endpoint web interface and remote controlled UI. Select **Accept** on either the endpoint web interface or remote controlled UI. The client successfully connects to the endpoint without any passwords.

- If your endpoint is not used in a conference, the computer desktop is sent to your endpoint as a presentation when the connection succeeds.
- If your endpoint is used in a conference, the computer desktop is sent to remote sites when the connection succeeds.

----End

To stop air content sharing, click **Stop**.

To disconnect the air content sharing client from the endpoint, click **Disconnect**.

9.3.4 Multi-View

With the multi-view function, you can view multiple local videos in Picture in Picture (PiP) or split-screen mode on one display.

Procedure

Step 1 Log in to the endpoint web interface. Choose **Device Control** > **Device Control** and click the **Multi-View** tab.

Step 2 Set **Multi-view mode** to any of the following:

- PiP
- 2 panes
- 3 panes
- 3 panes

Step 3 Specify input sources for the multi-view mode you selected.

Step 4 Click the **Video Control** tab.

Step 5 In the **Video Input Source** area, set **Video Source** to **Multi-View**.

----End

9.3.5 Customizing Shortcut Bar and Desktop Icons

You can customize the shortcut bar and desktop icons on the endpoint web interface so you can conveniently perform desired operations using these icons.

Background

The following procedure uses customizing shortcut bar icons as an example.

Procedure

Step 1 Log in to the endpoint web interface. Choose **System Settings > Display**.

Step 2 Click the **User defined** tab.

Step 3 Click **Shortcut Bar Icons**.

The **Shortcut Bar Icons** dialog box is displayed.

Step 4 Add or delete shortcut bar icons.

Step 5 Click **Save**.

----End

9.3.6 Accessing the Site Map

You can quickly navigate to a desired page using the site map.

To access the site map:

Log in to the endpoint web interface. Choose **Help > Site Map**.

9.3.7 Importing a Certificate

You can import client, server, and SiteCall certificates into your endpoint. These certificates can be used to identify users, certificate authorities, and servers to improve communication security.

Prerequisites

- **Client certificate:** You have obtained the required certificate from the SIP server administrator or downloaded it from a certificate authority.
- **Server certificate:** You have downloaded the required certificate from a certificate authority.
- **Multipoint conference certificate:** You have obtained the required certificate from the GK server administrator.

Procedure

Step 1 Log in to the endpoint web interface. Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import Certificate**.

The **File upload dialog** dialog box is displayed.

Step 3 Select the desired certificate type.



NOTE

- To import a certificate for authentication calls and when the endpoint functions as the server, select **Client certificate**.
- To import a certificate for authentication registration or calls and when the endpoint functions as a client (for example, TLS-based registration), select **Server certificate**.
- To import a certificate used for SiteCall security, select **Multipoint conference certificate**.

Step 4 Select the certificate you want to import and click **Import**.

Step 5 Click **Back** when **OK** is displayed.

----End

9.3.8 Monitoring the Video


To ensure that a conference runs smoothly, you may need to monitor how the endpoint operates and whether the local and remote videos are displayed properly in the conference room. From the endpoint web interface, you can capture photos and view local and remote videos and presentations.

The web login and video monitoring functions have been enabled. For details, see [Web-based Login](#) in [7.3 Supporting Remote Logins](#).

Log in to the endpoint web interface. Choose **Device Control > Video Control**. View the video or presentation of the local or remote site. You can then click **Capture**. In the displayed window, right-click the captured picture and choose **Save Picture As** to save the picture.



NOTE

When you are on the **Video Control** page,  appears on the endpoint display to indicate that video monitoring is enabled.

9.3.9 Using the Virtual Remote Control

You can use the virtual remote control on the endpoint web interface to control the endpoint.

Log in to the endpoint web interface. Choose **Device Control > Use remote control**. Click the keys on the virtual remote control to operate the endpoint.

10 Maintenance

About This Chapter

You must periodically check the working environment, cable connection, communication network connection, and audio-visual input and output of your endpoint. This ensures that the endpoint and its peripheral equipment work properly.

10.1 [Checking the Working Environment Periodically](#)

To ensure that your endpoint can function properly, check the working environment periodically.

10.2 [Checking the Endpoint Periodically](#)

For preventive maintenance purposes, you need to check the audio, video, and communication cables periodically.

10.3 [Viewing System Status](#)

Knowing system status at any given time helps to better maintain the endpoint.

10.4 [Querying System Information](#)

System information helps you maintain your endpoint.

10.5 [Querying Logs](#)

Your endpoint logs all non-query events in real time, including user activities and commands. The logs help with device maintenance, fault identification, and auditing.

10.1 Checking the Working Environment Periodically

To ensure that your endpoint can function properly, check the working environment periodically.

[Table 10-1](#) lists the items to be checked.



NOTICE

If any of the items does not meet the requirements, power off the endpoint and take measures to improve the environment. Ensure that the endpoint is used only when all the listed items meet the requirements.

Table 10-1 Checking the working environment

Item	Requirement
Operating temperature	0 °C to 40 °C
Operating humidity	10% to 80% RH

10.2 Checking the Endpoint Periodically



For preventive maintenance purposes, you need to check the audio, video, and communication cables periodically.

- Periodically (once a week is recommended) check that the cables connecting peripheral equipment and the power supply to the endpoint are securely connected.
- Periodically (once a week is recommended) check whether the communication cables connected to the endpoint work properly.
- Power on the endpoint and call some other endpoints using different methods, such as calling over a broadband network. If a call cannot be set up, verify that the cables are connected correctly and securely and the communication parameters are set correctly. If the problem persists, contact the videoconferencing network administrator to check the network.

10.3 Viewing System Status

Knowing system status at any given time helps to better maintain the endpoint.

Use any of the following methods to access the **Status** screen and view system status:

- Press  on the remote control and select **Status**.
- Select  from the option bar.
- Choose **Advanced > Diagnostics > Status**.

The following information is displayed on the **Status** screen:

- **Line status:** includes the local IP addresses and network port modes of LAN1 and LAN2, MAC address, WLAN IP address, whether to enable the GK, H.323 site number, whether to enable SIP, SIP site number, whether to connect 4 x E1 lines, and camera status and uptime.

- Call status: includes the line rate, video resolution, video rate (frame rate), presentation resolution, presentation rate (frame rate), audio rate, video packet loss rate, presentation packet loss rate, audio packet loss rate, conference participating duration, and presentation token. This information is displayed only after the endpoint joins a conference.
- Conference parameters: includes the call bandwidth, video protocol, video bandwidth (frame rate), audio protocol, audio bandwidth, presentation protocol, presentation bandwidth (frame rate), remote site number, media stream encryption, conference number for video access, conference number for audio access, ISDN trunk number, conference number for ISDN access, and password for conference authentication. This information is displayed only after the endpoint joins a conference.
- Input port status: includes the video information of all video input and USB1 and USB2 ports as well as air content sharing information.
- 4 x E1 line status (applicable only to the TE80)

10.4 Querying System Information

System information helps you maintain your endpoint.

Choose **Advanced** > **Diagnostics** > **System Information**. On the displayed **System Information** screen, you can check:

- Version information
- Specification information
 - Audio and video protocols and video resolutions supported by your endpoint
 - Network ports provided by your endpoint and the maximum bandwidth supported by each port
 - Whether your endpoint supports the Session Initiation Protocol (SIP)
 - Whether your endpoint supports dual stream, namely, the video and presentation
 - Whether your endpoint supports signaling and media stream encryption
 - Whether your endpoint is interoperable with Lync
 - Whether your endpoint supports recording, Scalable Video Coding (SVC), Wi-Fi, and public switched telephone network (PSTN)
 - Maximum presentation resolution and codec capability of your endpoint
 - Connection status to the network diagnostics client
 - ESN
 - Valid term of the license

10.5 Querying Logs

Your endpoint logs all non-query events in real time, including user activities and commands. The logs help with device maintenance, fault identification, and auditing.

Your endpoint can store a maximum of 100,000 log records. When the memory for recording logs is full, new logs can still be recorded. The latest log will simply replace the oldest one.

Choose **Advanced** > **Diagnostics** > **Logs**. Then select the log you want to view.

Logs are sorted by time. You can turn pages to view more entries. To display the details of a log, scroll to the log and select **Details**.

Each log contains the following information:

- Event time
- Event level
- Endpoint-defined event type
- Event details

To search for a log, select **Query** and specify the search criteria.

11 Upgrading

About This Chapter

Your endpoint supports the following software upgrade methods: automatic, using upgrade tools, using the bootrom system, and from the endpoint web interface.



NOTICE

During the upgrade, do not power off the endpoint to prevent irreversible faults.

[Table 11-1](#) describes the differences between the four upgrade methods.

Table 11-1 Endpoint upgrade methods

Upgrade Method	Description
Automatic upgrade	With the automatic upgrade function enabled and automatic upgrade parameters set, your endpoint obtains upgrade files from the specified server and installs the upgrade files when the preset upgrade interval arrives. For details, see 11.1 Automatic Upgrade .
Tool upgrade	Download the upgrade software to a computer, connect the computer to the endpoint directly or over the LAN, and upgrade the endpoint. For details, see 11.2 Tool Upgrade .
Upgrade using the bootrom system	If upgrading the endpoint using its normal system fails due to a power failure or other causes, you can use the bootrom system to complete the upgrade. For details, see 11.3 Upgrading the Endpoint Using the Bootrom System .
Upgrade from the endpoint web interface	On the endpoint web interface, manually upgrade the endpoint or set it to upgrade automatically. For details, see 11.4 Upgrading the Endpoint on Its Web Interface .

Before the upgrade, complete the following:

- Read the Release Notes to understand the contents to be upgraded and precautions required to be taken during the upgrade.
- Obtain the current software version.
- Back up the settings on the endpoint, such as the communication settings and address book.

11.1 Automatic Upgrade

With the automatic upgrade function enabled and automatic upgrade parameters set, your endpoint obtains upgrade files from the specified server and installs the upgrade files when the preset upgrade interval arrives.

11.2 Tool Upgrade

You can use a computer to locally upgrade the endpoint.

11.3 Upgrading the Endpoint Using the Bootrom System

If upgrading the endpoint using its normal system fails, you can use the bootrom system to complete the upgrade.

11.4 Upgrading the Endpoint on Its Web Interface

You can update the endpoint software from the web interface.

11.1 Automatic Upgrade

With the automatic upgrade function enabled and automatic upgrade parameters set, your endpoint obtains upgrade files from the specified server and installs the upgrade files when the preset upgrade interval arrives.

Procedure

Step 1 Choose **Advanced > Settings > Installation > Auto Upgrade Settings**.

Step 2 Set the automatic upgrade parameters described in [Table 11-2](#).

Table 11-2 Automatic upgrade parameters

Parameter	Description	Setting
Auto upgrade	Specifies whether the automatic upgrade function is enabled. If you select this parameter, you must also set Upgrade interval , Server address , User name , and Password . Your endpoint will obtain upgrade files from the specified server and install them when the preset upgrade interval is reached.	This parameter is not selected by default.
Enable wireless MIC auto update	Specifies whether to automatically update an upgradable wireless microphone VPM220W after it is connected to the endpoint.	This parameter is selected by default.

Parameter	Description	Setting
Upgrade interval	Specifies the upgrade interval. This parameter is available only when Auto upgrade is selected.	The default value is 0.5 h . Value range: 0.5 h to 24 h.
Server address	Specifies the IP address of the server that stores the upgrade files for your endpoint.	This parameter cannot be left blank. Example: http://200.55.55.100/
User name Password	Specify the user name and password your endpoint uses to access the server.	No default value is set for this parameter.

Step 3 Choose **Save**.

----**End**

11.2 Tool Upgrade

You can use a computer to locally upgrade the endpoint.

Prerequisites

Before the upgrade, ensure that:

- The target software is saved to the computer.
- The computer is connected to the endpoint using a straight-through cable, crossover cable, or switch.
- You have obtained the upgrade password. The default upgrade password is **Change_Me**. For details, see [7.4 Setting the Upgrade Password](#).

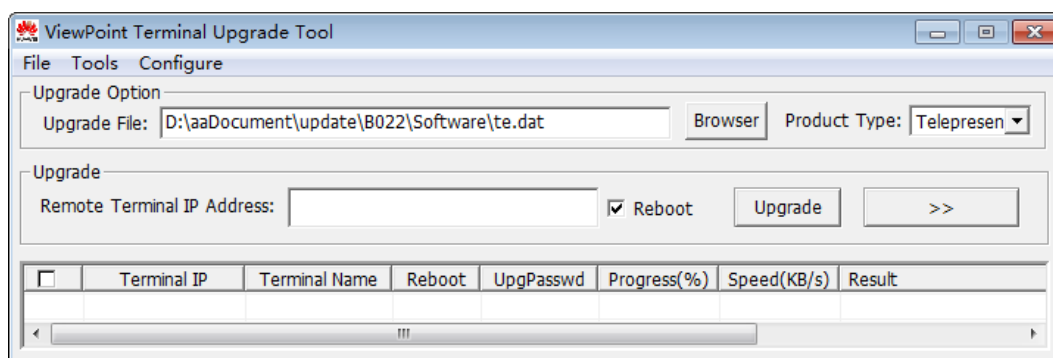
Upgrading a Single endpoint

Step 1 Power on the computer and endpoint.

Step 2 Extract the compressed software upgrade package on the computer.

Step 3 Run **UpgMaster.exe** to display the window shown in [Figure 11-1](#).

Figure 11-2 Upgrading a single endpoint



Step 4 (Optional) Click **Browser** and select the **te.dat** file.



NOTE

By default, the path of the **te.dat** file is displayed in **Upgrade File**.

Step 5 In **Remote Terminal IP Address**, enter the endpoint IP address, such as 10.10.10.10.



NOTE

If **Reboot** is selected, the endpoint automatically restarts after the upgrade.

Step 6 Click **Upgrade**.

Step 7 In the displayed dialog box, enter the upgrade password and click **OK**.

----End

Upgrading Multiple Endpoints in Batches

Step 1 Power on the computer and endpoint.

Step 2 Extract the compressed software upgrade package on the computer.

Step 3 Run **UpgMaster.exe** to display the window shown in [Figure 11-1](#).

Step 4 (Optional) Click **Browser** and select the **te.dat** file.

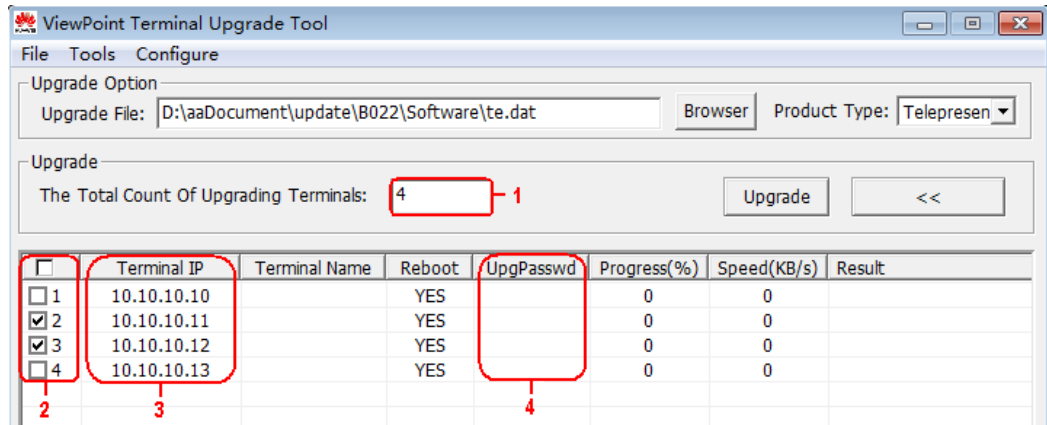


NOTE

By default, the path of the **te.dat** file is displayed in **Upgrade File**.

Step 5 Click  shown in [Figure 11-1](#) to display the window as shown in [Figure 11-2](#).

Figure 11-3 Upgrading multiple endpoints in batches



- Step 6** In area 1 shown in Figure 11-2, enter the number of the endpoints you want to upgrade, for example, 4.
- Step 7** In area 3 shown in Figure 11-2, enter the IP addresses of the endpoints you want to upgrade.
- Step 8** In area 4 shown in Figure 11-2, enter the upgrade passwords of the endpoints you want to upgrade.
- Step 9** In area 2 shown in Figure 11-2, select the endpoints you want to upgrade and click **Upgrade**.

 **NOTE**

To improve upgrade efficiency when the network bandwidth is insufficient, you can press **Ctrl+ALT+C** in the window shown in Figure 11-1, and then set the upgrade policy in the displayed window.

----End

Upgrading Specified Software Modules

- Step 1** Power on the computer and endpoint.
- Step 2** Extract the compressed software upgrade package on the computer.
- Step 3** Run **UpgMaster.exe** to display the window shown in Figure 11-1.
- Step 4** (Optional) Click **Browser** and select the **te.dat** file.

 **NOTE**

By default, the path of the **te.dat** file is displayed in **Upgrade File**.

- Step 5** Press **Ctrl+ALT+P** to display the **Pack Upgrade File** window.
- Step 6** In the **upgrade file list** area, select the software modules you want to upgrade.
- Step 7** Click **Pack File** to pack the selected software modules into a .dat file. Save the file to the computer, for example, save the file as **tepart.dat** to the computer.
- Step 8** In the displayed dialog box, click **OK**.
- Step 9** (Optional) In the window shown in Figure 11-1, click **Browser** and select the **tepart.dat** file you saved in Step 7.



NOTE

The path displayed in **Upgrade File** automatically changes to the path of the **tepart.dat** file.

Step 10 In **Remote Terminal IP Address**, enter the endpoint IP address, such as 10.10.10.10.

Step 11 Click **Upgrade**.

Step 12 In the displayed dialog box, enter the upgrade password and click **OK**.

----End

11.3 Upgrading the Endpoint Using the Bootrom System

If upgrading the endpoint using its normal system fails, you can use the bootrom system to complete the upgrade.

Prerequisites

- A copy of the target software is available on the computer.
- The computer is connected to the endpoint directly or over a LAN.
- You have obtained the upgrade password. The default upgrade password is **Change_Me**. For details, see [7.4 Setting the Upgrade Password](#).

Background

The bootrom system is used for upgrades when the endpoint software malfunctions. This method can be repeatedly used and ensures successful software upgrades provided that there are no hardware failures.

Procedure

Step 1 While the endpoint is restarting or powering on, press and hold the RESET button for 10 seconds.

The endpoint enters the bootrom system.



NOTE

At this time, the endpoint has two IP addresses available: the static IP address of the normal system and the default IP address (192.168.1.1). If the normal system IP address cannot be used for connection setup or the endpoint fails to obtain any IP address because of the dynamic IP address or other causes, you can use the default IP address for upgrades.

Step 2 Use Telnet to log in to the endpoint. Run the **mnt upgswitch on** command to enable the bootrom system upgrade function.



NOTE

- The bootrom system upgrade function is disabled by default.
- The default administrator user name and password for telnetting to the endpoint are **debug** and **Change_Me** respectively.

Step 3 Extract the compressed software upgrade package on the computer.

Step 4 Run the upgrade program **UpgradeTool.exe**.

The upgrade dialog box is displayed.

Step 5 (Optional) Click **Browser** and select the **te.dat** file.



NOTE

By default, the path of the **te.dat** file is displayed in **Upgrade File**.

Step 6 In **Remote Terminal IP Address**, enter your endpoint IP address, for example, 192.168.1.1. Then click **Upgrade**.

Step 7 In the displayed dialog box, click **OK** to start the upgrade.

Step 8 Restart the endpoint.

----End

11.4 Upgrading the Endpoint on Its Web Interface

You can update the endpoint software from the web interface.

Prerequisites

The upgrade file has been copied to your computer.



NOTICE

Do not close the endpoint web interface during the upgrade as doing so causes an upgrade failure.

Procedure

Step 1 Log in to the endpoint web interface. Choose **Maintenance > Upgrade**.

The **File upload** dialog box is displayed.

Step 2 Click **Select File** and select the **te.dat** file on your computer.

Step 3 Click **Import**.

The endpoint starts the upgrade.

----End

The endpoint automatically restarts when the upgrade is complete.

12 Troubleshooting

About This Chapter

This chapter describes how to diagnose and troubleshoot endpoint faults.

12.1 Fault Diagnostics

On the endpoint, you can perform the following diagnostic tests: sound and color bar tests, network tests, loopback tests, and remote control tests.

12.2 Troubleshooting

This section describes the problems you might encounter when using your endpoint and provides solutions.

12.3 Restoring Default Settings

If customized endpoint settings do not bring expected effects (for example, the display device fails to deliver images because of incorrect input or output port settings), use the **Restore Default** function to restore your endpoint to its default settings.

12.1 Fault Diagnostics

On the endpoint, you can perform the following diagnostic tests: sound and color bar tests, network tests, loopback tests, and remote control tests.

Choose **Advanced** > **Diagnostics**. Use the diagnostics methods available on the displayed **Diagnostics** screen.

[Figure 12-1](#) shows the endpoint diagnostics model.

Figure 12-1 Diagnostics model

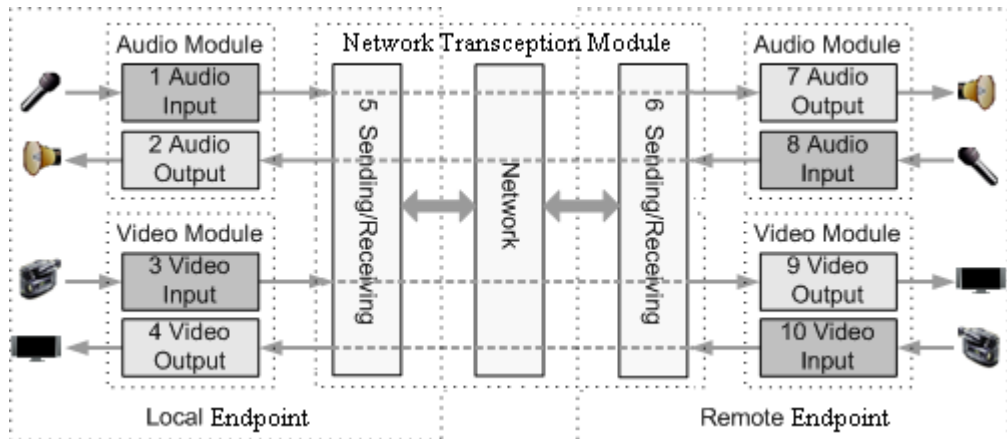


Figure 12-1 shows the diagnostics of three modules: audio module, video module, and network transception module.

Audio signals are transmitted in the following signal path:

- Local microphone → 1 → 5 → Communication network → 6 → 7 → Remote speaker
- Local speaker ← 2 ← 5 ← Communication network ← 6 ← 8 ← Remote microphone

Video signals are transmitted in the following signal path:

- Local camera → 3 → 5 → Communications network → 6 → 9 → Remote display device
- Local display device ← 4 ← 5 ← Communications network ← 6 ← 10 ← Remote camera

Sound and Color Bar Tests

Table 12-1 describes sound and color bar tests.

Table 12-1 Sound and color bar tests

Test	Item to Be Tested	Signal Stream
Sound	2 audio output	2 → Speaker
Color bar	4 video output	4 → Display device

- To perform a sound test, choose **Sound & Color Bar Test > Sound Test**. While the test audio stored on your endpoint plays, check the sound quality.
- To perform a color bar test, choose **Sound & Color Bar Test > Color Bar Test**. While seven color bars are displayed on the display device, check the color display quality.

Loopback Tests

During a loopback test, your endpoint transmits audio or video data through a channel to simulate actual working conditions and tests whether the output is satisfactory. You can

perform a local loopback test to check the network connection at your site or a remote loopback test to check the network connection at a remote site. While a remote loopback test is being performed, data is transmitted from your site to a remote site and then back to your site. [Table 12-2](#) describes loopback tests.



CAUTION

- To enable your endpoint to communicate with other endpoints, stop the loopback test.
- You cannot perform a loopback test on remote video during a dual-stream conference.

Table 12-2 Loopback tests

Test	Item to Be Tested	Signal Stream
Audio loopback	Local audio module	Microphone → 1 → 2 → Speaker
Video loopback	Local video module	Camera → 3 → 4 → Display device
Digital loopback	Local audio and video modules	The endpoint performs local audio and video loopback tests simultaneously.
Remote audio loopback	<ul style="list-style-type: none"> • Remote audio module • Network transmission 	Microphone → 1 → 5 → 6 → 7 → 8 → 6 → 5 → 2 → Speaker
Remote video loopback	<ul style="list-style-type: none"> • Remote video module • Network transmission 	Camera → 3 → 5 → 6 → 9 → 10 → 6 → 5 → 4 → Display device
Remote digital loopback	<ul style="list-style-type: none"> • Remote audio and video modules • Network transmission 	The endpoint performs remote audio and video loopback tests simultaneously.

Network Tests


Table 12-3 Network tests

Test	Item to Be Tested	Signal Stream
Network	IP access	Endpoint → LAN or public network

Before a network test, ensure that your endpoint is connected to an IP network and IP parameters are set correctly.

- If your endpoint is on a public network: In **IP address**, enter an IP address that is in a different network segment from your endpoint IP address. Then select **Start**. If the test is successful, the gateway settings and IP address of your endpoint are correct.
- If your endpoint is on a private network: In **IP address**, enter a public IP address. Then select **Start**. If the test is successful, the gateway settings, NAT address, and IP address of your endpoint are correct.

Remote Control Tests

Test the keys on the remote control to check whether they are functioning properly. If only some of the keys are tested, you can exit the **Remote Control Test** screen by pressing and holding  on the remote control.

When all the keys are tested, the **Remote Control Test** screen automatically exits.

The normal operating distance of the remote control is 6 meters. Its performance may be affected under strong light.

If the remote control does not work, verify that:

- The endpoint is powered on.
- The positive and negative charges of the battery are connected correctly.
- The battery has sufficient power left.
- There are no special fluorescent or neon signs nearby.

12.2 Troubleshooting

This section describes the problems you might encounter when using your endpoint and provides solutions.

Web Interface

Table 12-4 lists the troubleshooting methods for problems that may arise on the endpoint web interface.

Table 12-4 methods for troubleshooting endpoint web interface problems

Problem	Possible Cause	Solution
A message is displayed to indicate that your endpoint failed to connect to the Internet or download images.	The latest patches for the operating system or Internet Explorer are not installed.	Install the latest patches for the operating system and Internet Explorer.
	The security level of Internet Explorer is too high, or your endpoint IP address has not been added to the list of trusted sites.	<ol style="list-style-type: none"> 1. From the Internet Explorer menu bar, choose Tools > Internet Options. 2. Click the Security tab, Trusted sites, and then Sites. 3. In Add this Web site to the zone, enter your endpoint IP address. Then click Add. 4. Click OK.
Button text is not fully displayed.	Internet Explorer is set to ignore the font styles specified on web pages. In this case, the font specified by your endpoint cannot be recognized.	<ol style="list-style-type: none"> 1. From the Internet Explorer menu bar, choose Tools > Internet Options. 2. Under Appearance on the General tab, click Accessibility. 3. In the Accessibility dialog box,

Problem	Possible Cause	Solution
		deselect all options. 4. Click OK .
If Internet Explorer 6 is used, the endpoint web interface responds to operations slowly.	The JavaScript engine of Internet Explorer 6 is not upgraded, or the required patches are not installed.	<ul style="list-style-type: none"> • Install Microsoft Windows Script 5.7 (recommended). • Install the patches.
The records of the local address book cannot be exported.	The pop-up blocker is enabled on your browser.	<ul style="list-style-type: none"> • If Internet Explorer is used: On the Internet Explorer menu bar, choose Tools > Pop-up Blocker > Turn Off Pop-up Blocker. • If the Firefox is used: Choose Tools > Options. On the General tab, select Show the Downloads window when downloading a file. On the Privacy tab, select Accept cookies from sites. Then click OK to save the settings.

Network

Table 12-5 lists the troubleshooting methods for problems that may arise on the network.

Table 12-5 Methods for troubleshooting common network problems

Problem	Possible Cause	Solution
When you attempt to use Telnet to access the endpoint, a message is displayed to indicate that the number of connections to the endpoint has reached the limit.	<p>The number of connections to the endpoint has reached the maximum value.</p> <p>NOTE</p> <ul style="list-style-type: none"> • A maximum of seven SSH and Telnet connections to the endpoint is allowed. • A maximum of three SSH connections to the endpoint is allowed. 	Disconnect some Telnet connections.

Video





Table 12-6 lists the troubleshooting methods for video problems.

Table 12-6 Methods for troubleshooting video problems

Problem	Possible Cause	Solution
While the endpoint is powered on and not in a conference, the display device does not display the remote controlled UI or the video of your site.	The display device is powered off.	Power on the display device.
	The video channel of the display device is incorrect.	Use the remote control to select the correct video channel.
	The video settings of the endpoint or display device are incorrect. For example, the brightness is set to 0.	Retain the default values for the video parameters on the endpoint and display device.
	The video cable connection is not secure.	Secure the video cable between the endpoint and display device.
While the endpoint is powered on and not in use during a conference, the display device displays the video of your site but cannot display the remote controlled UI.	No display device is connected to the output port for the remote controlled UI or the connected display device is faulty.	Connect a display device to the output port for the remote controlled UI and verify the video settings on the display device.
	The output port for the remote controlled UI is not set or the output port you set for the remote control UI is not the port connected to the display device.	Choose Advanced > Settings > Video > Common Settings > Video Output . Set GUI to the output port connected to the display device.
	The endpoint does not respond to remote control operations.	Telnet to the endpoint. If you fail to operate the endpoint, it is malfunctioning. In this case, restart the endpoint. If the problem persists, contact the local distributor for maintenance.
While the endpoint is in use during a conference, the display device displays the video of your site but cannot display the video of any remote site.	A local or remote loopback test is being performed.	Stop all local and remote loopback tests.
	Check the call statistics. If the value of Video bandwidth[frame rate] is 0 , no video is sent from remote sites.	Contact the remote site administrator to resolve this problem.
	If the remote video is displayed as a blue screen, the remote site is blocking its video by sending a blue screen.	Contact the remote site administrator to resolve this problem.
	The video output port is set to display the video of your site.	Set the video output port to display the video of a remote site.
The video of your site is in black and white or flickers in	The mode adopted by the video output port is set	<ul style="list-style-type: none"> Ensure that the mode adopted by the video output port and the cable in use match each

Problem	Possible Cause	Solution
black and white.	incorrectly.	other. <ul style="list-style-type: none"> Verify that the cable is connected correctly. Replace the cable if necessary.
While the endpoint is in use during a conference, the video of a remote site is not clear. For example, there are artifacts, frozen images, or discontinuity in the video output.	Faults occur in the local video module.	Perform a local video loopback test. If the video quality is poor, faults occur in the local video module. In this case, send the endpoint to the local distributor for maintenance.
	The remote camera is set to focus on a close or distant scene. When the remote camera is not set to automatic focus and the scene captured by a remote camera changes, the captured video becomes unclear.	Set the remote camera to automatic focus.
	Incorrect audio protocols are specified for conferences whose data transmission rates are lower than or equal to 256 kbit/s. To view the data transmission rate of a conference, access the Status screen. For example, if the conference rate is 256 kbit/s and the audio bandwidth is 64 kbit/s, the video bandwidth is only 196 kbit/s. In this case, the video quality is poor.	If the conference rate is lower than 256 kbit/s, set the audio protocol to G.728 to reduce the bandwidth used for audio transmission.
	Only low video bandwidth is available for your site because the network is busy.	Do not initiate conferences during network busy hours.
	The quality of a network connection device, such as an optical fiber transceiver, is poor. As a result, certain data is lost during transmission.	Replace the related network connection device.
While the endpoint is in use during a conference, the video of a remote site can be displayed continuously but the video quality is not satisfactory.	Ask the remote site administrator to perform a local video loopback test. If the video quality is good, the video frame rate set at the remote site is too high.	Ask the administrator of the remote site to disconnect from the conference, set the video frame rate to a smaller value, and join the conference again.

Problem	Possible Cause	Solution
While the endpoint is not in use during a conference, the video displayed on the display device is too bright or too dark.	The video settings of the endpoint are inappropriate.	Retain the default values for the video parameters on the endpoint and display device.
	The video settings of the display device are inappropriate.	Retain the default values for the video parameters on the endpoint and display device.
	The camera is faulty.	Send the endpoint to the local distributor for maintenance.
While the endpoint is in use during a conference and a remote site is sharing its computer desktop, the local VGA display cannot display the shared computer desktop.	The resolution of the remote computer exceeds the maximum resolution supported by the endpoint.	Ask the remote site administrator to change the resolution and refresh rate of the remote computer to those the endpoint supports.
	The local VGA display is not supported.	Replace the local VGA display with a supported display.
	The presentation sharing function is not enabled at your site.	Choose Advanced > Settings > Conference > Advanced and select Presentation .
A computer is connected to the endpoint, but the local VGA display does not show the computer desktop.	The capability of the VGA display is limited. The resolution or refresh rate of the local SXGA output is too high to be supported by the VGA display.	Set the resolution and refresh rate of the local SXGA output to those the VGA display supports.
	The endpoint supports only certain combinations of resolutions and refresh rates. The combination of the resolution and refresh rate set on the computer, however, is not supported by the endpoint. In this case, the local site cannot display or properly display the computer desktop.	Set the resolution and refresh rate of the computer used for the VGA input to those the endpoint supports.
	The presentation source is not set as the computer desktop.	Choose Advanced > Settings > Video > Common Settings > Video Input . Set Presentation Source to the input port connected to the computer desktop.
	The dual screen function is not enabled.	Choose Advanced > Settings > Video > Common Settings > Video Output and set Presentation display to Enable .
On the camera	The camera you want to control is not selected.	Access the camera control screen and select the camera you want to

Problem	Possible Cause	Solution
control screen,  ,  , and navigation keys on the remote control cannot be used to control the camera.		control.
	Camera settings are incorrect.	Verify the camera settings.
While the endpoint is in use during a conference and the display device displays the video of a remote site, after you press  ,  , or navigation keys on the remote control, the video remains unchanged. That is, you cannot control the remote camera.	The remote control is disabled on the remote camera.	Ask the remote site administrator to enable the remote camera control at the remote site.
	The camera settings are incorrect or the control cable of the camera is not securely connected.	Ask the remote site administrator to verify the camera settings or securely connect the camera control cable.

Audio

Table 12-7 lists the troubleshooting methods for audio problems.

Table 12-7 Methods for troubleshooting audio problems

Problem	Possible Cause	Solution
While the endpoint is in use during a conference, no audio is delivered from the local display device.	Perform an audio test to check whether the problem occurs at your site or a remote site. If no audio is delivered from the display device during the audio test, the problem exists at your site.	<ul style="list-style-type: none"> • If the chair site has muted the speaker of your site, contact the chair site to resolve this problem. • If the display device volume is adjusted to the lowest, restore the volume to its default value. • If the endpoint volume is adjusted to the lowest, restore the volume to its default value. • If the audio cable is connected incorrectly or insecurely, reconnect the audio cable from the endpoint to the display device.
	If audio is properly delivered from the display device during the audio test, the problem	<ul style="list-style-type: none"> • The microphone at the remote site has been muted or the chair site has muted this microphone.

Problem	Possible Cause	Solution
	occurs at the remote site.	<p>In this case, contact the chair site to resolve this problem.</p> <ul style="list-style-type: none"> • No sound pickup device, such as a microphone, is connected to the audio input port. In this case, set the audio source again or connect a sound pickup device to the corresponding port. • The related sound pickup device is powered off. In this case, power on the device. • The audio cable is connected insecurely. In this case, reconnect the audio cable to the endpoint.
While the endpoint is in use during a conference, only the sound from your site can be delivered from the display device and you cannot hear other sites.	A loopback test is being performed at your site.	Stop all local and remote loopback tests.

Conference Initiation

Table 12-8 lists the troubleshooting methods for problems you may encounter during conference initiation.

Table 12-8 Methods for troubleshooting common problems with conference initiation

Problem	Possible Cause	Solution
Your site and a remote site cannot call each other using site numbers.	<p>Your site or the remote site has not registered with a GK. A GK is responsible for translating site numbers into IP addresses. If either your site or the remote site does not register with a GK, the translation cannot be implemented, and your site cannot place a call to the remote site using the site number.</p> <p>If a remote site places a call to</p>	Verify GK registration settings and register your site and the remote site with a GK.

Problem	Possible Cause	Solution
	<p>your site by site number, it will receive a message from the GK indicating that your site has not registered with the GK, and the call cannot be set up.</p>	
	<p>The local or remote endpoint is not connected to an IP network.</p>	<ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. From the remote controlled UI, choose Advanced > Diagnostics > Network Test. Enter the IP address of the remote site and start a Ping test. If the Ping test fails, a network error has occurred. In this case, contact the administrator. 3. From the remote controlled UI, choose Advanced > Settings > Network > IP. Verify IP network settings.
<p>Your site cannot place a call to a remote site using the IP address of the remote site.</p>	<p>The local or remote endpoint is not connected to an IP network.</p>	<ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. From the remote controlled UI, choose Advanced > Diagnostics > Network Test. Enter the IP address of the remote site and start a Ping test. If the Ping test fails, a network error has occurred. In this case, contact the administrator. 3. From the remote controlled UI, choose Advanced > Settings > Network > IP. Verify IP network settings.
	<p>NAT settings are incorrect. Specifically, the local endpoint is on a private network while the remote endpoint is on a public or different private network. Check whether your endpoint can communicate with a public network. If the</p>	<p>Choose Advanced > Settings > Network > Firewall and verify NAT settings.</p>

Problem	Possible Cause	Solution
	endpoint cannot, NAT settings are incorrect.	
	The GK with which the local or remote endpoint registers does not support the function for placing calls using IP addresses.	Choose Advanced > Settings > Network > IP > H.323 at your site and the remote site, respectively. Then, disable GK functions.
After the endpoint starts, it fails to register with the GK.	The parameters (GK address, encryption password, and user name) used for GK registration are incorrect.	On the endpoint web interface, choose Advanced > Settings > Network > IP > H.323 and correct the settings.
	Another site with the same number as your site has already registered with the GK.	Contact the videoconferencing system administrator to check whether another site with the same number as your site has already registered with the GK. If such a site exists, change the user name of your site.
	The endpoint is disconnected from an IP network.	<ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. From the remote controlled UI, choose Advanced > Diagnostics > Network Test. Enter the IP address of the remote site and start a Ping test. If the Ping test fails, a network error has occurred. In this case, contact the administrator. 3. From the remote controlled UI, choose Advanced > Settings > Network > IP. Verify IP network settings.
	NAT settings are incorrect. Specifically, the local endpoint is on a private network while the GK is on a public network. Check whether your endpoint can communicate with a public network. If the endpoint cannot, NAT settings are incorrect.	Choose Advanced > Settings > Network > Firewall and verify NAT settings.
	The GK listening port, such as port 1719, is restricted by the network firewall.	Contact the videoconferencing system administrator to resolve this problem.

Problem	Possible Cause	Solution
A predefined conference fails to be initiated on the endpoint.	The endpoint is disconnected from an IP network.	<ol style="list-style-type: none"> 1. Verify that the endpoint is connected to an IP network. Specifically, the LAN indicator on the rear panel of the endpoint is steady green. 2. From the remote controlled UI, choose Advanced > Diagnostics > Network Test. Enter the IP address of the remote site and start a Ping test. If the Ping test fails, a network error has occurred. In this case, contact the administrator. 3. From the remote controlled UI, choose Advanced > Settings > Network > IP. Verify IP network settings.
	<ul style="list-style-type: none"> • Your site is set to pay for the conference but does not have sufficient account balance. • Another site is set to pay for the conference but does not have sufficient account balance, or account number or password entered is incorrect. 	Enter the correct account number and password and top up the related account.
	Multiple conferences are currently being held while port resources on the videoconferencing system are insufficient.	Wait until the resources are available. Alternatively, reduce the number of sites attending the conference and then add sites as required after the conference is held successfully.
	The SiteCall account for using the 4E1 lines is incorrect.	Contact the videoconferencing system administrator to resolve this problem.

Conference Control

Table 12-9 lists the troubleshooting methods for common problems you may encounter during conference control.

Table 12-9 Methods for troubleshooting conference control problems

Problem	Possible Cause	Solution
While the endpoint	A site in the conference is being	Ask the chair site to stop

Problem	Possible Cause	Solution
is in use during a conference, you cannot view the desired site.	broadcast, and all the sites must view that site except the chair site and broadcast site.	site broadcast.
	A site is having the floor, and non-chair sites cannot view other sites.	Ask the chair site to enable the discussion function.
	The chair site has enabled the Voice Activation function.	Ask the chair site to disable the Voice Activation function.
	No video is sent from the site you want to view.	Ask the related site administrator to troubleshoot the site video.
	The View Site function is restricted on the RM or the SMC.	Contact the videoconferencing system administrator to resolve this problem.

12.3 Restoring Default Settings

If customized endpoint settings do not bring expected effects (for example, the display device fails to deliver images because of incorrect input or output port settings), use the **Restore Default** function to restore your endpoint to its default settings.

Restoring your endpoint to its default settings causes the loss of certain stored information, for example, site information in the address book, call records, and logs.

Choose **Advanced > Settings > Installation > Restore Default**. In the displayed dialog box, enter the endpoint serial number and select **OK**.

NOTE

- To view the serial number of your endpoint, choose **Advanced > Diagnostics > System Information > Version**.
- Press and hold the RESET button on the back of the endpoint for about 10 seconds, and the endpoint will be restored to its default settings and restart. After the endpoint is restored to its default settings, its IP address is reset to 192.168.1.1.

13 Feature Configuration

About This Chapter

Feature configuration includes setting the number keys and power key on the remote control, parameters for placing and answering calls, advanced conference parameters, SNMP parameters, quality of service (QoS) parameters, and network diagnostics parameters.

[13.1 Setting the Number Keys and Power Key on the Remote Control](#)

You can set the number keys and power key on the remote control to facilitate your daily use of the endpoint.

[13.2 Setting the Parameters for Placing and Answering Calls](#)

You can set the mode in which the endpoint places and answers calls. For example, you can set the endpoint to automatically answer calls or to enable the do not disturb function.

[13.3 Setting Advanced Conference Parameters](#)

Correctly setting advanced conference parameters brings expected conference effects.

[13.4 Setting SNMP Parameters](#)

To enable the videoconferencing network management system to manage your endpoint, configure the Simple Network Management Protocol (SNMP) settings.

[13.5 Setting QoS Parameters](#)

Quality of service (QoS) settings determine the mode for processing IP data packets during a conference.

[13.6 Setting Network Diagnostics Parameters](#)

Correct settings on the ports used for diagnostics enable you to use a network diagnostics tool to diagnose your endpoint using the ports.

[13.7 Setting Network Diagnostics Parameters](#)



The firewall protects your IP network by preventing harmful data being passed between the internal and external networks. Ensure that the firewall settings are applicable to the H.323 videoconferencing system. Otherwise, the system and the firewall will need to be configured to allow the video conference to pass the firewall.

13.1 Setting the Number Keys and Power Key on the Remote Control

You can set the number keys and power key on the remote control to facilitate your daily use of the endpoint.

Choose **Advanced** > **Settings** > **General**. Set the number keys and power key, which are described in [Table 13-1](#).

Table 13-1 Number keys and power key on the remote control

Parameter	Description	Setting
Select number key function		
Select number key function	<p>Specifies the functions of the number keys on the remote control.</p> <p>When the endpoint is not in a conference and the display is showing the menus or camera control screen, you can only control camera presets by pressing number keys on the remote control.</p> <p>When the endpoint is in a conference, you can select either of the following options:</p> <ul style="list-style-type: none"> • Second Dial: Follow the instructions to press number keys to perform two-stage dialing. • Control camera preset: On the menus or camera control screen, press a number key to move the camera to the preset bound to that key. 	<p>The default value is Second Dial.</p> <p>To toggle between these two options, press  on the remote control.</p>
Power supply		
Shut Down	<p>Specifies whether the endpoint can be powered off.</p> <p>If you set this parameter to Disable, pressing  on the remote control can only restart the endpoint or place it in sleep mode.</p>	<p>The default value is Enable.</p>

13.2 Setting the Parameters for Placing and Answering Calls

You can set the mode in which the endpoint places and answers calls. For example, you can set the endpoint to automatically answer calls or to enable the do not disturb function.

Choose **Advanced** > **Settings** > **Conference** > **Normal**. Set the parameters described in [Table 13-2](#).

Table 13-2 Parameters for placing and answering calls

Parameter	Description	Setting
Answer Mode	<p>Specifies how your endpoint handles incoming calls.</p> <ul style="list-style-type: none"> • Manual: Your endpoint prompts you to handle a call when the call comes in. • Answer call automatically: Your endpoint automatically answers incoming calls when not being used in a conference. 	The default value is Manual .
Mute local audio for answered calls	<p>This parameter is available only when Answer Mode is set to Answer call automatically.</p> <p>Specifies whether the endpoint turns off all sounds generated at your site when your endpoint joins a conference. If you enable this parameter, no remote site can hear your site.</p>	This parameter is not selected by default.
Open do not disturb right	<p>Specifies whether the do-not-disturb function is available to all users.</p> <p>If you enable this parameter, under Advanced > Utilities, common users can enable or disable the do-not-disturb function. The do-not-disturb function prevents you from being disturbed by incoming calls.</p>	This parameter is selected by default.
Call parameter configuration	<p>Specifies whether you can set the call type and data transmission rate before initiating point-to-point calls. If you select this parameter, you can set the call type and data transmission rate in the displayed dialog box before initiating a point-to-point call. If you do not select this parameter, the endpoint uses the default call type and data transmission rate.</p>	This parameter is not selected by default.
Wi-Fi network preferred	<p>Specifies whether to prioritize a Wi-Fi network when both wireless and wired networks are available.</p> <p>This parameter is available only when Wi-Fi is enabled. For details about how to enable Wi-Fi, see 3.1.5 Setting Wi-Fi Parameters.</p>	This parameter is not selected by default.
Default call bandwidth	<p>Specifies the default data transmission rate for your endpoint.</p> <p>NOTE</p> <p>If this parameter is set incorrectly, the video quality will be affected or the call might even fail to be set up.</p>	The default value is 1920 kbps .

Parameter	Description	Setting
Maximum incoming call bandwidth	Specifies the maximum bandwidth allowed for receiving calls. The bandwidths used for placing and receiving calls cannot exceed than this bandwidth. The settings of this bandwidth and the settings of Default call bandwidth are independent of each other.	The default value is 8 Mbps . The settings cannot exceed the bandwidth supported by the endpoint license.

13.3 Setting Advanced Conference Parameters

Correctly setting advanced conference parameters brings expected conference effects.

Advanced conference parameters apply to the following conferences:

- Point-to-point conferences initiated by your site
- Multipoint conferences initiated by your site
- Conferences that your site joins by answering a call from a remote site

Choose **Advanced** > **Settings** > **Conference** > **Advanced**. Set the advanced conference parameters described in [Table 13-3](#).

Table 13-3 Advanced conference parameters

Parameter	Description	Setting
Audio and video protocols	Using the audio or video protocol you select, your endpoint negotiates the audio or video capability with a remote endpoint to set up a call. If you do not select an audio or video protocol, this protocol is not an option value of the related advanced conference parameters. For example, if you do not select the H.264 HP protocol, it will not be displayed in the option values of the Video protocol parameter.	Retain the default value. NOTE Select at least one audio protocol and one video protocol so that you can use your endpoint to place audio calls or video calls.
Audio protocol	Specifies the audio protocol your endpoint uses to encode audio.	The default value is Auto .
Audio channels	Specifies the audio channels. This parameter is available only when you select AAC-LD or HWA-LD .	The default value is Two .
Video protocol	Specifies the video protocol the endpoint uses to encode video. During a non-multi-stream conference, Video protocol is the video protocol the endpoint uses at your site.	The default value is Auto . To initiate an HD video conference, select an H.264-related video protocol.

Parameter	Description	Setting
Video resolution	<p>Specifies the video format. The available options vary depending on your settings of Video protocol.</p> <p>When Video protocol is set to Auto, set this parameter to either of the following:</p> <ul style="list-style-type: none"> • Sharp: Your endpoint uses a high video resolution to ensure clear video. • Smooth: Your endpoint uses a high frame rate to ensure smooth video. 	The default value is Sharp .
Video frame rate	<p>Specifies the frame rate used during video encoding.</p> <p>Video at a higher frame rate is smoother.</p> <p>When Video protocol is set to Auto, this parameter is not available.</p>	The default value is Auto . Retain the default value.
Prevent little packet loss	<p>Specifies whether to prevent sporadic packet loss to avoid artifacts.</p>	<p>This parameter is not selected by default.</p> <p>Select this parameter if all endpoints are on the same private network and sporadic packet loss occurs.</p>
Presentation	<p>Specifies whether you can share presentations during conferences.</p> <p>NOTE You can set Presentation protocol, Presentation resolution, Presentation mode, Presentation bandwidth setting, Presentation bandwidth (%), Presentation sharing mode, and Presentation plug-and-share only after you set this parameter to Enable.</p>	This parameter is selected by default.
Presentation protocol	<p>Specifies the video protocol your endpoint uses to encode presentations.</p>	The default value is Auto .
Presentation resolution	<p>Specifies the presentation video resolution.</p> <ul style="list-style-type: none"> • Smooth: Your endpoint uses a high frame rate to ensure smooth video. • Sharp: Your endpoint uses a high video resolution to ensure clear video. 	The default value is Sharp .
Presentation bandwidth setting	<p>Specifies the mode for setting the presentation video bandwidth.</p> <ul style="list-style-type: none"> • Auto: Your endpoint automatically sets the presentation video bandwidth based on the bandwidth available. • Manual: You must manually set 	The default value is Auto .

Parameter	Description	Setting
	Presentation bandwidth.	
Presentation bandwidth	Specifies the percentage of the call bandwidth presentations can occupy.	The default value is 50 .
Presentation mode	<p>Specifies the mode of the presentation you want to share.</p> <ul style="list-style-type: none"> • Presentation: When the video is switched, the presentation remains unchanged. Only one site in the conference can share a presentation one time. • Live: The presentation viewed by each site is switched along with the video. All sites in a conference can share presentations simultaneously. <p>NOTE When connected to an IMS network, the endpoint cannot share a presentation in Live mode.</p>	The default value is Presentation .
Presentation sharing mode	<ul style="list-style-type: none"> • Auto: The endpoint automatically shares presentations along with videos. This parameter can be set to Auto only when Presentation mode is set to Live. • Manual: You must manually share presentations by using the remote control. 	The default value is Manual .
Presentation plug-and-share	Specifies whether your site automatically shares presentations with remote sites once presentation input is detected.	The default value is Disable .
Conference line type	<p>Specifies the type of line used during a conference.</p> <p>If you select Auto and your endpoint has registered with a network gatekeeper (GK) server, your endpoint preferentially uses H.323 to initiate a conference.</p>	The default value is Auto .
Conference bandwidth	Specifies the transmission bandwidth for a conference.	The default value is Normal .
Dynamic bandwidth	<p>Specifies whether the endpoint implements the following if the packet loss rate increases due to insufficient network bandwidth: automatically decreases the conference bandwidth until packet loss does not occur constantly or the conference bandwidth is decreased to 64 kbit/s. If constant</p>	<p>This parameter is not selected by default.</p> <ul style="list-style-type: none"> • When the network is running within normal parameters, retain the default value. • When the network is not

Parameter	Description	Setting
	packet loss is detected, the endpoint can dynamically adjust bandwidth to recover stable conference quality within 1 minute.	running within normal parameters, select this parameter.
reserved presentation bandwidth	<p>Disable this parameter if your site is not going to send or receive presentations during a conference and the Received value for Presentation bandwidth [frame rate] is not -.</p> <p>If this parameter is disabled, the Received value for Presentation bandwidth [frame rate] restores to - when you rejoin the conference.</p> <p>NOTE To view the Presentation bandwidth [frame rate] value, choose Advanced > Diagnostics > Status > Conference.</p>	The default value is Enable .
Preferred IP protocol	<p>Specifies the protocol that IP sites preferentially use.</p> <p>When Line type is set to Auto for IP sites, your endpoint uses this protocol to call the IP sites.</p>	The default value is H.323 .
Face detection	<p>Specifies whether to perform HD encoding and decoding to improve face recognition video quality.</p> <p>You can increase the video sharpness by enabling this parameter in low bandwidths.</p>	The default value is Disable .
Site called during startup	<p>Specifies the site that your endpoint automatically calls when it starts.</p> <ul style="list-style-type: none"> None: The endpoint does not call any sites. Select site from address book: The endpoint displays the address book screen from which you can specify the site you want your endpoint to call after its startup. <p>You can proceed to set Call times only after you set this parameter.</p>	The default value is None .
Call times	Specifies the maximum number of attempts your endpoint calls a specified site after startup.	<p>The default value is 1.</p> <p>The maximum value is 10.</p> <p>If you set this parameter to 0, your endpoint does not call the specified site after startup.</p>

13.4 Setting SNMP Parameters

To enable the videoconferencing network management system to manage your endpoint, configure the Simple Network Management Protocol (SNMP) settings.

Your endpoint communicates with and is remotely managed by the videoconferencing network management system using SNMP. The videoconferencing network management system implements the following:

- Configures endpoint settings, including the H.323, SIP.
- Checks endpoint alarms.
- Backs up and restores endpoint settings.
- Upgrades the endpoint online.

On the endpoint web interface, choose **System Settings > Network** and click the **SNMP Settings** tab. Set the SNMP parameters described in [Table 13-4](#).

Table 13-4 SNMP parameters

Parameter	Description	Setting
Enable SNMP	Specifies whether the videoconferencing network management system uses SNMP to manage your endpoint. NOTE If you set this parameter to Enable , you must set other SNMP parameters.	The default value is Enable .
Get community name	Specifies the read-only SNMP community name.	The default value is Change_Me . Set this parameter to the value defined on the videoconferencing network management system. The value is a string of 1 to 32 characters.
Set community name	Specifies the read-write SNMP community name.	The default value is Change_Me . Set this parameter to the value defined on the videoconferencing network management system. The value is a string of 1 to 32 characters.
Trap community name	Specifies the trap community name.	The default value is Change_Me . Set this parameter to the value defined on the videoconferencing network management system. The value is a string of 1 to 32

Parameter	Description	Setting
		characters.
Trap server address 1 Trap server address 2 Trap server address 3	Specify the IP address to which your endpoint sends traps, namely, the IP address of the computer where the videoconferencing network management system server is installed. NOTE A trap is an unrequested message that a managed device (for example, an endpoint) sends to a trap server (for example, the SMC) to report urgent and important events.	No default value is set for this parameter. You can leave this parameter blank.
Trap version	Version of the traps that the endpoint sends to the videoconferencing network management system through SNMP.	The default value is v3 trap .
Trap timeout time	Specifies the timeout interval for traps, in seconds. This parameter is available only when Trap version is set to v2 inform or v3 inform .	The default value is 1 .
Trap retry times	Specifies the number of retry attempts for sending a trap. This parameter is available only when Trap version is set to v2 inform or v3 inform .	The default value is 5 .
User name	Specifies the user name for sending traps. This parameter is available only when Trap version is set to v3 trap or v3 inform .	The default value is trapinit .
Authentication protocol Authentication password	Specify the authentication mode and password that your endpoint uses to send traps to the videoconferencing network management system through SNMP. This parameter is available only when Trap version is set to v3 trap or v3 inform .	The default value of Authentication protocol is MD5 . Set Authentication password to the password defined on the videoconferencing network management system. If the two passwords are not the same, authentication fails.
Encryption protocol Encryption password	Specify the encryption protocol and password that your endpoint uses to send traps to the videoconferencing network management system through SNMP. If you select No encryption for Encryption protocol , traps are transmitted using plaintext. This parameter is available only when	The default value of Encryption protocol is DES . Set Encryption password to a string of 1 to 32 characters, which contains letters, digits, and special characters.

Parameter	Description	Setting
	Trap version is set to v3 trap or v3 inform .	
SNMPv3 Authentication Information		
User name	Specifies the user name for connecting your endpoint to the videoconferencing network management system through SNMPv3.	The default value is v3user .
User rights	Specifies the user permissions of your endpoint when it connects to the videoconferencing network management system. <ul style="list-style-type: none"> • Read and write:read and write • Read only: read-only 	The default value is Read and write .
Authentication protocol Current password New password	Specify the authentication mode and password for connecting the videoconferencing network management system to your endpoint.	The default value of Authentication protocol is MD5 . When the videoconferencing network management system attempts to connect to your endpoint, Authentication protocol and New password set on your endpoint are required.
Encryption protocol Encryption password	Specify the encryption protocol and password for connecting the videoconferencing network management system to your endpoint. Available encryption protocols are DES , AES , and No encryption .	The default value of Encryption protocol is DES . Set Encryption password to a string of 32 characters or less, consisting of letters, digits, and special characters.

13.5 Setting QoS Parameters

Quality of service (QoS) settings determine the mode for processing IP data packets during a conference.

Choose **Advanced > Settings > Network > QoS**. Set the QoS parameters described in [Table 13-5](#).

Table 13-5 QoS parameters

Parameter	Description	Setting
QoS type	Specifies the type of the Quality of Service (QoS) network security measure used to deal with the network latency, congestion,	The default value is Priority .

Parameter	Description	Setting
	<p>and other issues.</p> <ul style="list-style-type: none"> • Priority: If you select this option, you must also set IP priority and Service type. • DiffServ: If you select this option, you must also set DSCP. 	
IP priority	<p>Specifies the priority that a network device gives to forwarding the data packets sent by your endpoint.</p> <p>A larger value indicates a higher priority.</p>	<p>The default value is 7.</p> <p>Value range: 0-7</p>
Service type	<p>Specifies how the data packets sent and received by your endpoint are processed on the network.</p> <ul style="list-style-type: none"> • Normal: Network devices transmit the data packets without special processing. • Minimum delay: Data packets are transmitted at the highest rate with the minimum delay. • Maximum throughput: A large number of data packets can be transmitted on the network. • Highest reliability: Data packets can be transmitted to remote sites completely and correctly. • Minimum cost: Network devices transmit data packets of the same traffic at lower costs. 	<p>The default value is Minimum delay.</p>
DSCP audio DSCP video DSCP data DSCP signaling	<p>Specify the service level of data packets sent by your endpoint during transmission.</p> <p>A larger value indicates a higher service level.</p>	<p>The default value is 63.</p> <p>Value range: 0-63</p>
Network jitter	<p>Adjusts network jitter settings to address:</p> <ul style="list-style-type: none"> • Labial synchronization problems during conferences • Choppy audio problems, by increasing the network jitter value. 	<p>The default value is 0ms.</p> <p>Value range: 0 ms to 1000 ms</p>
Lip sync.	<p>Fine-tunes network jitter settings if a slight labial synchronization problem persists after the network jitter settings are adjusted.</p>	<p>The default value is 0ms.</p> <p>Value range: 0 ms to 300 ms</p>

13.6 Setting Network Diagnostics Parameters

Correct settings on the ports used for diagnostics enable you to use a network diagnostics tool to diagnose your endpoint using the ports.

Choose **Advanced > Settings > Network > Network diagnostics**. Set the network diagnostics parameters described in [Table 13-6](#).



NOTE

You can use a network diagnostics tool to diagnose your endpoint only when the endpoint is not used in any conferences.

Table 13-6 Network diagnostics parameters

Parameter	Description	Setting
Network diagnostics	Specifies whether to enable the Registration, Admission and Status (RAS) ports, H.323 call port, and Session Initiation Protocol (SIP) port to be used for network diagnostics.	The default value is Disable .
H.323 call port	Specifies the port the network diagnostics tool uses to receive and send call signaling during communication with your endpoint.	The default value is 1820 .
RAS source port	Specifies the port your endpoint uses to receive and send RAS signaling during communication with the network diagnostics tool.	The default value is 1819 .
RAS destination port	Specifies the port the network diagnostics tool uses to receive and send RAS signaling during communication with your endpoint.	The default value is 1819 .
SIP call port	Specifies the port your endpoint uses to send SIP signaling during communication with the network diagnostics tool.	The default value is 5160 .
Test network after exiting conference	Specifies whether to perform the ping operation after your endpoint exits a conference. Ping results are recorded in a log.	The default value is Enable .



NOTE

Log in to the web interface of the endpoint, choose **System Settings > Network > Network diagnostics** to set **Diagnostics tool user name** and **Diagnostics tool password**. The default value of **Diagnostics tool user name** and **Diagnostics tool password** are **admin** and **Change_Me** respectively.

13.7 Setting Network Diagnostics Parameters

The firewall protects your IP network by preventing harmful data being passed between the internal and external networks. Ensure that the firewall settings are applicable to the H.323 videoconferencing system. Otherwise, the system and the firewall will need to be configured to allow the video conference to pass the firewall.

Choose **Advanced > Settings > Network > Firewall**. Set the firewall parameters described in [Table 13-7](#).

Table 13-7 Firewall parameters

Parameter	Description	Setting
H.460	Specifies whether H.460 is enabled for traversal between public and private networks. If you set this parameter and Use NAT to Enable , your endpoint will use Huawei's proprietary Super Network Passport (SNP). If you set this parameter to Enable and your endpoint is recognized as a private network endpoint, H.460 will be used for traversal between public and private networks.	The default value is Disable .
Use NAT	Specifies whether NAT is enabled for traversal between public and private networks. An endpoint installed on a private network is considered as a public network endpoint after NAT is enabled on the endpoint. Even if you then enable H.460 on the endpoint, it is still considered as a public network endpoint, and H.460 is not used.	The default value is Disable .
NAT address	Specifies the public IP address for your endpoint. This parameter is required after you set Use NAT to Enable .	No default value is set for this parameter.
H.323 call port	Specifies the port a remote site uses to receive and send call signaling during communication with your site.	The default value is 1720 . Value range: 1-65534.
RAS source port	Specifies the port your site uses to receive and send Registration, Admission and Status (RAS) signaling during communication with remote sites.	The default value is 1719 . Value range: 1-65534.
RAS destination port	Specifies the port a remote site uses to receive and send RAS signaling during communication with your site.	The default value is 1719 . Value range: 1-65534.
SIP call port	Specifies the port your site uses to send Session Initiation Protocol (SIP) signaling during communication with	The default value is 5060 . Value range: 1-65534.

Parameter	Description	Setting
	remote sites.	
Local listen port	Specifies the local SIP listening port.	The default value is 5060 . Value range: 1-65534.
Server listen port	Specifies the listening port on the SIP server with which your endpoint registers.	The default value is 5060 . Value range: 1-65534.
Port settings	Specifies the port use. <ul style="list-style-type: none"> • Normal: The number of the port currently in use cannot be changed. • Port convergence: The port numbers used in H.323 converge. Specifically, signals of different formats use the same port number. This saves port resources. • Same port send/receive: Your endpoint sends and receives data streams through the same port. 	The default value is Same port send/receive .
Audio port	Specifies the port your site uses to receive audio packets during communication with remote sites.	The default value is 10002 . Enter an even number ranging from 1 to 65534.
Video port	Specifies the port your site uses to receive video packets during communication with remote sites.	The default value is 10004 . Enter an even number ranging from 1 to 65534.
SIP TLS call port	Specifies the port your site uses to send SIP signaling during communication with remote sites when Transmission type is set to TLS .	The default value is 5061 . Value range: 1-65534.
Local SIP TLS listen port	Specifies the local SIP listening port when Transmission type is set to TLS .	NOTE For details about how to set Transmission type , see 3.1.4 Setting SIP Parameters .
SIP server TLS listen port	Specifies the listening port on the SIP server with which your endpoint registers when Transmission type is set to TLS .	
Use TCP to transmit streams	Specifies whether to use the Transmission Control Protocol (TCP) to transmit video and data streams. NOTE If you set this parameter to Enable , you must also set TCP listen port and TCP connection port .	
TCP listen port	Specifies the local listening port for TCP streams.	The default value is 20002 . Value range: 1-65534.

Parameter	Description	Setting
TCP connection port	Specifies the local connection port for TCP streams.	The default value is 20004 . Value range: 1-65534.

14 Ports on the Rear Panel

This section describes the ports on the rear panel and their functions, helping you correctly connect the required devices to the endpoint.

[Figure 14-1](#) to [Figure 14-3](#) show the ports on the rear panels of the different models covered by this document and illustrate the differences between them.

Figure 14-1 TE80



A E1 and T1 Grounding Criteria

Read the following grounding criteria carefully and comply with the relevant requirements during the installation of the endpoint.

The grounding design of the telecom office (station) follows the principle of equalized voltage. That is, the work grounding and the protection grounding (including the shielded grounding and the surge protection grounding of the distribution frame) share a set of grounding conductors.

When the E1 cable of the cabinet is over 7.5 m and the T1 cable of the cabinet is over 10 m, a shielded cable and a shielded connector should be used and grounded.

When the E1 interface is connected to other devices using coaxial cables, the external shield layers at the transmitting endpoint and receiving endpoint should be connected to the protection ground at the same time. The dual in-line package (DIP) switch offers the possible disconnection function at the receiving end.

Copper-core materials instead of aluminum materials should be used for the ground cable. The plastic insulated copper wires with yellow and green insulation color should be used for the protective ground cable. The protective ground cable should not exceed 30 m, and the shorter the better. When the protective ground cable exceeds 30 m, the ground bar should be rearranged.

In a balanced circuit, the joint of the E1 (T1) cable and the connector should be grounded using the external shield layer (the grounding conductor) or an additional wire to ensure normal reception and transmission in each E1 (T1) channel. In an unbalanced circuit, the metal braid shield layer of the cable should be seamlessly connected to the coaxial connector.

When the E1 cable exceeds 30 m and the T1 cable exceeds 40 m, use the multi-point grounding mode. In addition, connect the E1 cable to the ground at every 15 m and the T1 cable to the ground at every 20 m.

When the E1 or T1 cable is extended out of the office (station), the E1 or T1 cable should go through the main distribution frame (MDF) attached with the security unit. The shield layer of the E1 or T1 cable should be firmly connected to the protection ground of the MDF. The security unit on the MDF should have the overvoltage protection, overcurrent protection, and failure alarm functions. The maintenance personnel should check the equipment periodically and replace the ineffective protection unit in time.

 **NOTE**

For questions about grounding the device, contact the device provider for technical support.

B Technical Specifications

Knowing technical specifications of the endpoint helps you better use it.

[Table B-1](#) lists the technical specifications of the endpoint.

Table B-1 Technical specifications

Category	Item	Specifications
Standards compliance	Multimedia frame protocol	ITU-T H.323 and IETF SIP
	Video standard	H.261, H264 SVC, H264 HP, H264 BP, H263, and H263+
	Audio standard	AAC-LD, G.711A, G.711U, G.719, G.722, G.728, G.729A, HWA-LD, G.722.1 and G.722.1C
	Dual-stream standard	ITU-T H.239 and BFCP
	Communication standard	H.221, H.225, H.231, H.233, H.234, H.235, H.241, H.242, H.243, H.245, H.281, H.283, H.350, H.460, and T.140
	Network standard	TCP/IP, FTP, DHCP, SNMP, Telnet, HTTP, SSH, HTTPS, PPPoE, RTP, RTCP, and SNTP
	Protocol for signaling and media stream encryption	H.281 and H.224
	Media stream encryption protocol	AES and DES
	Protocol for signaling and media stream encryption	H.235, SRTP, and TLS
Call	IP	64 kbit/s-8 Mbit/s

Category	Item	Specifications
bandwidth	4E1(only for the TE80)	64 kbit/s-8 Mbit/s
Video	Input	2 x HD-VI/DVI, 2 x DVI-I (HDMI, VGA, and YPbPr supported with conversion cables), 1 x CVBS/S-VIDEO (converted from a DVI-I port), 1 x HDMI/DVI (audio input supported), 1 x DisplayPort (audio input supported), and 1x3G-SDI
	Output	2 x HDMI/DVI (audio output supported), 2 x DVI-I (HDMI, VGA, and YPbPr supported with conversion cables), 1 x CVBS/S-VIDEO (converted from a DVI-I port), and 1 x 3G-SDI
	Video resolution	1080p60 with a minimum bandwidth of 1 Mbit/s (optional) 1080p30 with a minimum bandwidth of 512 kbit/s (optional) 720p60 with a minimum bandwidth of 512 kbit/s 720p30 with a minimum bandwidth of 384 kbit/s 4SIF/4CIF with a minimum bandwidth of 128 kbit/s SIF/CIF with a minimum bandwidth of 64 kbit/s SQSIF/SQCIF/QSIF/QCIF with a minimum bandwidth of 64 kbit/s
	Presentation resolution	Input: 1920 x 1200 60fps, 1080p 60fps, 1680 x 1050 60fps, 1600 x 1200 60fps, 1600 x 900 60fps, 1400 x 1050 60fps, 1440 x 900 60fps, 1366 x 768 60fps, 1360 x 768 60fps, 1280 x 1024 60/75/85fps, 1280 x 960 60/75/85fps, 1280 x 800 60/75/85fps, 1280 x 768 60/75/85fps, 1280 x 600 60fps, 1152 x 864 60/75/85fps, 720p 60/75/85fps, 1024 x 768 60/70/75/85fps, 800 x 600 56/60/72/75/85fps, 640 x 480 60/72/75/85fps Output: 1600 x 1200, 1920 x 1200, 1920 x 1080, 1280 x 1024, 1280 x 720, 1024 x 768, 800 x 600 Coding/Decoding resolution: 1600 x 1200, 1920 x 1200, 1920 x 1080, 1280 x 1024, 1280 x 720, 1024 x 768, 800 x 600, 4CIF, CIF
	Other video features	Video Motion Enhancement VideoIntensifier ViewProcessing Facial Recognition The TE40 and TE50 support the following: <ul style="list-style-type: none"> • dual 1080p60 (presentation mode: presentation) • 1080p60+1080p30 (presentation mode: live) The TE80 supports the following: dual 1080p60 (presentation modes: presentation or live)

Category	Item	Specifications
Audio	Input	2 x XLR, 2 x RCA, 1 x microphone array HD-AI port, 1 x HDMI port (supporting audio input), and 1 x DisplayPort (supporting audio input)
	Output	4 x RCA port, 2 x HDMI port (supporting audio output), and 2 x DVI-I (output using DVI-HDMI conversion cables)
	Audio processing	AEC, ANS, and AGC
Network port	Network port	2 x 10/100/1000 M LAN, 1 x Wi-Fi, 1 x 4 E1 connector (optional, only for the TE80), and 1 x PSTN (Only available in China)
USB port	USB	2 × USB 2.0
COM port	COM	2 × COM
Peripherals	VPC600 and VPC620 HD cameras	
	Endpoint control by using the camera to forward infrared signals	
	The endpoint supports up to 30 and 16 camera presets for the local site and remote site respectively.	
	VPM220 and VPM220W microphone arrays The TE40 and TE50 can be connected to only one VPM220 or VPM220W microphone array. The TE80 can be connected to up to two VPM220 or VPM220W microphone arrays.	
Electricity supply requirements	Operating voltage and frequency	100 V AC–240 V AC; 50 Hz–60 Hz;
	Maximum power consumption	150 W
Environmental requirements	Operating state	
	Ambient temperature	0 °C to 40 °C (32 °F to 104 °F)
	Relative humidity	10% to 80%
	Ambient noise	< 46 dBA SPL
	Minimum illuminance	7lux
	Recommended illuminance	> 300 lux
	Non-operating state	
	Ambient	–40 °C to +85 °C

Category	Item	Specifications
	temperature	
	Relative humidity	0% to 95%
Physical specifications	Codec dimensions (H x W x D)	435mm x 354mm x 106.5mm
	Package dimensions (H x W x D)	570mm x 600mm x 210mm
	Weight	11.5kg (net weight) and 12.5 kg (gross weight)
Infrared remote control port	Infrared signal reception	NEC

C Status Icons

The icons provided on the user interface indicate the status and settings of the system.















The icons help show the system status and perform operations as required. [Table C-1](#) lists the icons that will appear on the lower-right corner of the call screen and indicate the current network status. Before initiating a conference, check the status of these icons.







Table C-1 Network status icons

Icon	Name	Indicates ...
	SIP registration failure	The endpoint fails to be registered with the SIP server.
	GK registration failure	The endpoint fails to register with the gatekeeper after the gatekeeper is enabled.
	Network disconnection	The endpoint is disconnected from an IP network. The network cable may be disconnected.
	DNS resolution failure	After the DNS server is enabled and domain names are adopted as SIP server or GK server addresses, the DNS server fails to resolve the domain names.
	Wi-Fi connection status	The first icon indicates that the Wi-Fi network has disconnected after the Wi-Fi client is enabled. The other icon indicates the signal status of a connected Wi-Fi network.

When you view a video, the icons listed in [Table C-2](#) are used to indicate the status of certain operations. During a conference, pay attention to the status of these icons to ensure that the relevant operations are performed correctly.

Table C-2 Operating status icons

Icon	Name	Indicates ...
	Microphone status	The status of the microphone of the local site when displayed on the lower right corner of the screen. In this case, the microphone is a physical device used at the local site. When one of these icons is displayed in other positions of the screen, it indicates the microphone status of a remote site in a conference.
	Speaker status	The status of the speaker of the local site when displayed on the lower right corner of the screen. When one of these icons is displayed in other positions of the screen, it indicates the speaker status of a remote site in a conference.
	Encrypted conference	The current conference is an encrypted conference (with media streams encrypted).
	Chair	The local site is the chair site.
	Remote site	A remote site is currently being viewed.
	Local site	The local site is currently being viewed.
	Presentation sharing	A presentation is currently being shared.
	Local site broadcast	The local site is being broadcast in the current conference.
	Do Not Disturb	The Do Not Disturb function is enabled at the local site.
	Hide Video	The local video is hidden during a conference. You can use this function to prevent the local video from being seen by remote sites. After this function is enabled, the local site is displayed as a blue screen at remote sites.
	Camera control (up and down)	The camera lens is turned upward or downward.
	Camera control (left and right)	The camera lens is turned leftward or rightward.
	Camera control (zooming)	The video input from the camera is shrank or enlarged.
	Poor network condition	Network impairments or packet loss occurs in the network where the endpoint is located. see 8.2 Customizing Onscreen Status Icons .

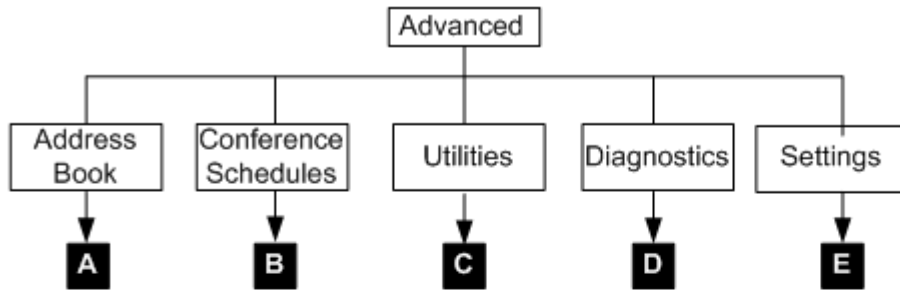
Icon	Name	Indicates ...
	Video monitoring	A remote site is recording or taking photos of the conference from the endpoint web interface.
	Recording	The current conference is being recorded.
	Connected to a VPM220W	The endpoint is connected to a VPM220W. The first icon indicates that the VPM220W has insufficient battery while the other icon indicates a sufficient battery.
	Remote site muted	The remote site is muted, and the local site cannot hear the remote site.
	Local site's speaker muted by the chair site	The chair site mutes the local site's speaker so the local site cannot hear other sites.
	Local site's microphone muted by the chair site	The chair site mutes the local site's microphone so other sites cannot hear the local site.

D Menus

This section describes the structure of the menus, which helps users to quickly identify each function item.

The **Advanced** tab on the menu screen is the interface to all the function configuration items of the endpoint. [Figure D-1](#) shows the menu structure.

Figure D-1 Menu structure



C Utilities

- Middle Caption
- Banner
- Bottom Caption
- Hide Video
- Do not disturb
- Help

D Diagnostics

- Status — Line Status 4E1 Status Call Status
— Conference Input Interface Status
- Sound & Color Bar Test
- System Information — Version Specifications
- Loopback Test
- Logs
- Remote Control Test
- Network Test

E Settings

- Installation — Wizard Restore Default Auto Upgrade Settings
- General — Date and time Power supply Select number key function
- Display — Personalize Caption Icon Packet Loss Threshold
 - └ Banner Middle Caption Bottom Caption
- Conference — Normal Advanced Common Settings
- Video — Video Input Video Output Common Settings Video Parameters
Image Offset Sampling Phase
- Audio — Audio Input Volume Sound Effect
- Network — IP 4E1 Network Address Book Wi-Fi Network diagnostics Firewall QoS
 - └ LAN1 LAN2 H.323 SIP
 - └ Wi-Fi Client Wi-Fi Hotspot
- Security — Password Web Login Encryption SSH/Telnet Upgrade password
Air Content Sharing



NOTE

Only the TE80 supports 4E1 functions.

E Terminology

This appendix provides the terms you will encounter in this administrator guide.

Numerics

1080i	1080i is the shorthand name for a format of high-definition video modes. 1080 denotes the number of horizontal scan lines - also known as vertical resolution - and the letter i stands for interlaced. In the alternate format of high-definition video mode, known as 1080p, the p would stand for progressive scan. 1080i is generally used in place of 1440x1080, at a frame rate of 29.97 (30000/1001), while 1080p is usually used in place of 1920x1080 (full HD), at a frame rate of 23.976 fps (24000/1001).
1080p	1080p is the shorthand name for a category of HDTV video modes. The number 1080 represents 1,080 lines of vertical resolution (1,080 horizontal scan lines), while the letter p stands for progressive scan (meaning the image is not interlaced). 1080p can be referred to as full HD or full high definition although 1080i is also "Full HD" (1920x1080 pixels). The term usually assumes a wide-screen aspect ratio of 16:9, implying a horizontal resolution of 1920 pixels. This creates a frame resolution of 1920x1080, or 2,073,600 pixels in total. The frame rate in hertz can be either implied by the context or specified after the letter p (or i), such as 1080p30, meaning 30 Hz.
2 panes	Users see two sites on one display device in two panes. The two panes are of the same size. Each pane is about 1/4 of the screen. Use 2-pane as an adjective.
2CIF	2CIF defines a video with a resolution of 352 × 576 pixels and using progressive scanning.
2SIF	2SIF defines a video with a resolution of 352 × 480 pixels and using progressive scanning.
3 panes	Users see three sites on one display device in three panes. Use 3-pane as an adjective.
4CIF	4CIF defines a video resolution of 704 × 576 pixels.
4SIF	4SIF defines a video with a resolution of 704 × 480 pixels and using progressive scanning.

720p 720p is the shorthand name for a category of HDTV video modes. The number 720 stands for the 720 horizontal scan lines of display resolution (also known as 720 pixels of vertical resolution), while the letter p stands for progressive scan or non-interlaced. When broadcast at 60 frames per second, 720p features the highest temporal (motion) resolution possible under the ATSC standard. Progressive scanning reduces the need to prevent flicker by filtering out fine details, so sharpness is much closer to 1080i than the number of scan lines would suggest.

B

broadcast (site) All sites, except for the site being broadcast, view the site that is broadcast. On the Broadcast Site screen, users can choose between Broadcast Single and Broadcast in Turn.

broadcast single (site) Broadcast one specified site.

C

call absent (sites) Place calls to all the sites that are on the site list but are absent from the conference.

call site Place a call to a site to add the site to the conference.

cascading Multiple MCUs are connected in series at different layers to allow the number of participants to expand beyond what a single MCU can support. In cascading mode, an MCU in an upper layer can control an MCU in a lower layer.

camera preset Users can control a camera by zooming, panning, and tilting the camera or changing the focus. Then, users can store this camera position and assign a number to this position. This preset position is a camera preset. During a conference, users can move the camera to a camera preset by selecting the relevant number.

CIF CIF (Common Intermediate Format), also known as FCIF (Full Common Intermediate Format), is a format used to standardize the horizontal and vertical resolutions in pixels of YCbCr sequences in video signals, commonly used in video teleconferencing systems. It was first proposed in the H.261 standard.

continuous presence A feature in multi-point conferencing that allows the video endpoint to see images from multiple video endpoints at the same time. All parties remain continuously visible or 'present' for the duration of the call and the user can have control over the screen layout. Continuous presence is better suited for team collaboration since it allows participants to see the reactions (body language) of all participants, not just the speaker.

D

delete site Remove a site from the site list.

dual stream During a conference, two channels of video streams can be sent or received simultaneously. For example, one channel is used for transmitting video (such as video captured by a camera) and the other channel is used for transmitting presentation (such as a computer desktop). The two channels of videos can be displayed on two displays.

E

end conference End a conference. In this case, all sites leave the conference.

F

full-duplex A full-duplex, or sometimes double-duplex system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time. A good analogy for a full-duplex system would be a two-lane road with one lane for each direction.

G

G.711 G.711, also known as Pulse Code Modulation (PCM), is a very commonly used waveform codec. G.711 uses a sampling rate of 8,000 samples per second, with the tolerance on that rate 50 parts per million (ppm). Non-uniform quantization (logarithmic) with 8 bits is used to represent each sample, resulting in a 64 kbit/s bit rate. There are two slightly different versions; μ -law, which is used primarily in North America, and A-law, which is in use in most other countries outside North America.

G.722 G.722 is an ITU-T standard 7 kHz wideband speech codec operating at 48, 56 and 64 kbit/s. It was approved by ITU-T in November 1988. Technology of the codec is based on sub-band ADPCM (SB-ADPCM).

G.728 G.728 is an ITU-T standard for speech coding operating at 16 kbit/s. It is officially described as Coding of speech at 16 kbit/s using low-delay code excited linear prediction.

give floor After the chair site gives floor to a site, the other sites view and hear the site. All the sites, except the chair site and the site that is given the floor, are muted.

H

H.239 H.239 is an ITU-T recommendation from the H.32x Multimedia Communications' macrofamily of standards for multimedia communications over various networks. The H.239 recommendation is titled "Role management and additional media channels for H.3xx-series endpoints". Practical importance of this recommendation is its setting forth a way to have multiple video channels (for example, one for conferencing, another for

presentation) within a single session (call).

- H.263** H.263 is a video codec standard originally designed as a low-bitrate compressed format for videoconferencing. It was developed by the ITU-T Video Coding Experts Group (VCEG) in a project ending in 1995/1996 as one member of the H.26x family of video coding standards in the domain of the ITU-T. H.263v2 (H.263+) added support for flexible customized picture formats and custom picture clock frequencies. Previously the only picture formats supported in H.263 had been Sub-QCIF, QCIF, CIF, 4CIF, and 16CIF, and the only picture clock frequency had been 30000/1001 (approximately 29.97) clock ticks per second.
- H.264** H.264/AVC/MPEG-4 Part 10 (Advanced Video Coding) is a standard for video compression. The final drafting work on the first version of the standard was completed in May 2003. H.264/AVC is the latest block-oriented motion-compensation-based codec standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC Moving Picture Experts Group (MPEG), and it was the product of a partnership effort known as the Joint Video Team (JVT). The ITU-T H.264 standard and the ISO/IEC MPEG-4 AVC standard (formally, ISO/IEC 14496-10 - MPEG-4 Part 10, Advanced Video Coding) are jointly maintained so that they have identical technical content. H.264 is used in such applications as Blu-ray Disc, videos from YouTube and the iTunes Store, DVB broadcast, direct-broadcast satellite television service, cable television services, and real-time videoconferencing.
- 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.
- half-duplex** A transmitting mode in which a half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.
- hang up (site)** Hang up a remote site and remove the site from the conference.
- HD** Refers to a video system of higher resolution than standard-definition (SD) video, most commonly at display resolutions of 1280×720 (720p) or 1920×1080 (1080i or 1080p, full HD). High definition (HD) refers to an increase in display or visual resolution of television formats (HDTV), high definition video (used in HDTV broadcasting, digital film and computer HD video film formats), high definition multimedia interface (HDMI), an all-digital audio and video interface capable of transmitting uncompressed streams and other formats for recording and transmitting visual and audio communications.
- hide video** During a conference, a site can hide its video to prevent other sites from viewing the video of the site.

I

intelligent mode A video transforming mode, in this mode, cut the video first and then stretch the video. Ensure that the aspect ratio of the video remains unchanged. For example, to change a wide-screen video to a narrow-screen video, crop the left and right edges of the wide-screen video, and then stretch the video to full screen.

L

lock conference (presentation) After the chair site locks a conference and if site A is sharing presentation, the other sites in the conference cannot share presentation until site A stops sharing presentation.

lock site (presentation) After the chair site locks the presentation, only the site that is currently sharing the presentation can continue sharing presentation. Other sites cannot share presentation.

P

presentation During a conference, the local site can share the content input by a computer with remote sites, such as an excel file, a diagram, or a presentation.

R

release chair Pass the chair control to another site.

request chair Request chair rights and become the chair site.

request floor Request to speak. During a conference, users can request the floor from the chair site.

revoke chair When chair control rights are revoked, no chair site exists in the conference. If the site that revokes the chair rights wants to become the chair site, the site needs to request chair rights.

revoke presentation After the chair site revokes the presentation token, the relevant site stop sharing the presentation.

S

S-Video Separate Video[1], more commonly known as S-Video, also called Y/C, and sometimes incorrectly [2] referred to as Super Video[3], is an analog video signal that carries video data as two separate signals: luma (luminance) and chroma (color). This differs from composite video, which carries picture information as a single lower-quality signal, and component video, which carries picture information as three separate higher-quality signals. S-Video carries standard definition video (typically at 480i or 576i resolution), but does not carry audio on the same cable.

SIF Source Input Format (SIF) defined in MPEG-1, is a video format that was developed to allow the storage and transmission of digital video. 625/50 SIF format (PAL/SECAM) has a resolution of (360 or) 352 x

288 active pixels and a refresh rate of 25 frames per second.
525/59.94 SIF Format (NTSC) has a resolution of (360 or) 352 x 240 active pixels and a refresh rate of 29.97 frames per second.

site group	A group of conference sites. If certain sites attend a conference frequently, users can define these sites as a group to facilitate site management.
start presentation	Start sharing local-site presentation with remote sites.
stop broadcasting (site)	Stop broadcasting a site. The other sites stop viewing the site.
stop presentation	Stop sharing local-site presentation with remote sites.
SVGA	Super Video Graphics Array or Ultra Video Graphics Array, almost always abbreviated to Super VGA, Ultra VGA or just SVGA or UVGA is a broad term that covers a wide range of computer display standards. Originally, it was an extension to the VGA standard first released by IBM in 1987. Unlike VGA—a purely IBM-defined standard—Super VGA was defined by the Video Electronics Standards Association (VESA), an open consortium set up to promote interoperability and define standards. When used as a resolution specification, in contrast to VGA or XGA for example, the term SVGA normally refers to a resolution of 800 × 600 pixels.

U

UXGA	Ultra extended graphics array, supporting a maximum resolution of 1600 x 1200 pixels.
-------------	---

V

video	The video is generally output from the HD OUT 1 interface of an HD video endpoint and is captured by a camera.
view single (site)	View any site.
view site	View any site. On the View Site screen, users can choose between View Single and View in Turn.
voice activation	This function is used for discussion or arguing scenarios. The site with the loudest voice is broadcast.

X

XGA	XGA, the Extended Graphics Array, is an IBM display standard introduced in 1990. Today, it is the most common appellation of the 1024×768 pixels display resolution, but the official definition is broader than that.
------------	--

F Acronyms and Abbreviations

Numerics

4CIF 4 x Common Intermediate Format

A

AAC-LD Advanced Audio Coding-Low Delay

ADSL Asymmetric Digital Subscriber Line

B

BFCP Binary Floor Control Protocol

BNC Bayonet Neill-Concelman connector

BRI Basic Rate Interface

C

CAS Channel Associated Signaling

CCS Common Channel Signaling

CRC Cyclic Redundancy Check

CVBS Composite Video Base Signal

D

DHCP Dynamic Host Configuration Protocol

DNS Domain Name Server

DP DisplayPort

DSCP Differentiated Services Code Point

DVI Digital Visual Interface

DVR Digital Video Recorder

F

FTP File Transfer Protocol

G

GK Gatekeeper

H

HD High Definition

HDMI High Definition Multimedia Interface

I

ISDN Integrated Services Digital Network

IMS IP multimedia subsystem

M

MCU Multipoint Control Unit

N

NAT Network Address Translation

NTP Network Time Protocol

NTSC National Television Standards Committee

P

PAL Phase Alternating Line

PPPoE Point-to-Point Protocol over Ethernet

PSF Progressive Segmented Frame

PSTN Public Switched Telephone Network

PTZ Pan/Tilt/Zoom

Q

QoS Quality of Service

S

SD	standard definition
SDI	Serial Digital Interface
SIP	Session Initiation Protocol
SMB	SubMiniature version B connector
SSH	Secure Shell
SVC	Scalable Video Coding
SXGA	Super Extended Graphics Array

V

VGA	Video Graphics Array
------------	----------------------

W

Wi-Fi	Wireless Fidelity
WOL	Wake on LAN

Y

YPbPr	
--------------	--