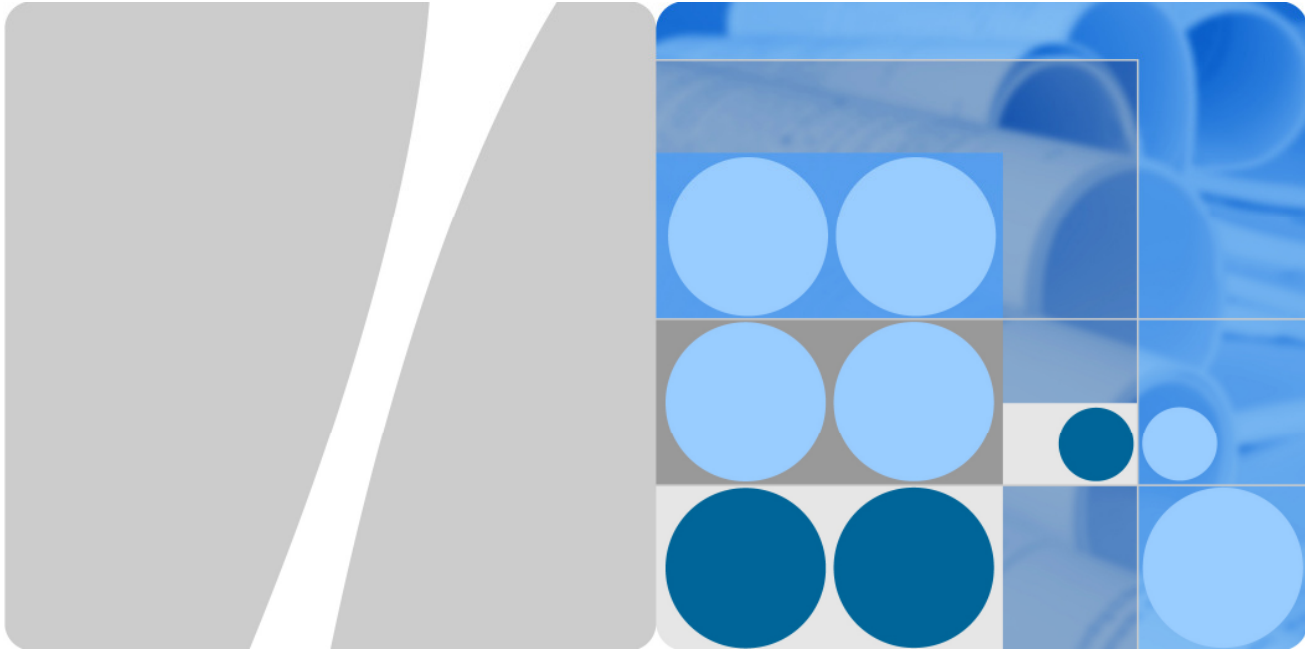




**HUAWEI TE40&TE50&TE60 Videoconferencing
Endpoint
V100R001C10
Administrator Guide**

Issue 01
Date 2014-12-23

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 use the HUAWEI TE40 Videoconferencing Endpoint (TE40 or endpoint for short), HUAWEI TE50 Videoconferencing Endpoint (TE50 or endpoint for short), and HUAWEI TE60 Videoconferencing Endpoint (TE60 or endpoint for short), including conference experience, device control, address book management, system settings, installation, maintenance, and troubleshooting.

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, touch panel (optional), and remote controlled user interface (UI). It is recommended that endpoint administrators set parameters and manage the address book on the endpoint web interface.

When using this document, note the following:

- Unless otherwise specified, the descriptions in this document are applicable to the TE40, TE50, and TE60.
- Except chapters [7.7 Security](#) and [9.4 Customizing the Remote Controlled UI](#) which apply to the endpoint user interface controlled by the remote control (remote controlled UI for short), descriptions and configurations in this document apply to the endpoint web interface.

Symbol Conventions

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

Symbol	Description
 WARNING	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 DANGER	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Symbol	Description
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

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

Issue 01 (2014-12-23)

This issue is the first official release.

Contents

About This Document	ii
1 Overview	1
1.1 Definition of an Endpoint Administrator	1
1.2 Requirements on an Administrator	2
1.3 Related Documentation.....	3
1.4 Safety Precautions	4
1.5 How to Obtain Help.....	10
2 Web-based Login.....	11
3 Menu Structure of the Web Interface	14
4 Conference Experience	16
4.1 Initiating a Point-to-Point Conference	17
4.1.1 Initiating a Conference from the Call Page.....	17
4.1.2 Initiating a Conference from the Address Book.....	18
4.1.3 Holding a Call.....	18
4.2 Initiating a Multipoint Conference.....	19
4.2.1 Understanding the MCU and Built-in MCU.....	19
4.2.2 Initiating a Conference from the Predefined Conference Page.....	22
4.2.3 Initiating a Conference from the Conference History Page	25
4.2.4 Initiating a Conference from the Address Book Page.....	25
4.3 Scheduling a Conference	26
4.4 Joining a Conference Using the Conference Access Number.....	27
4.5 Joining an MSUC Convergent Conference.....	28
4.6 Joining an HD-Video Conference over an IMS Network	30
4.7 Sharing a Presentation	33
4.8 Creating and Sending Captions.....	34
4.9 Using the Do-Not-Disturb Function	35
4.10 Controlling a Conference.....	35
4.11 Recording a Conference.....	43
4.12 Sending and Receiving Instant Messages	44
5 Device Control.....	46
5.1 Viewing the Video.....	47

5.2 Controlling a Camera.....	48
5.3 Setting a Camera Preset	49
5.4 Selecting Video Sources	51
5.5 Controlling Audio	52
5.6 Setting the Combined Picture	55
5.7 Setting Camera Parameters.....	55
5.8 Setting Preferred Video Parameters	57
5.9 Setting Up a PPPoE Dial-Up Connection	58
5.10 Using the Remote Control	59
6 Managing the Local Address Book	60
6.1 Editing the Local Address Book	60
6.2 Using Virtual Conference Rooms	63
6.3 Importing and Exporting Address Book	64
6.4 Customizing a Site Template	64
7 System Settings	66
7.1 Setting Basic Parameters	67
7.1.1 Setting the System time	67
7.1.2 Setting the Ringtone for Incoming Calls	68
7.1.3 Managing Power.....	68
7.1.4 Setting Number Key Functions.....	70
7.2 Specifying Caption Settings.....	70
7.3 Setting Video Parameters.....	72
7.3.1 Understanding Video Input Capabilities	72
7.3.2 Configuring Video Input	75
7.3.3 Setting the Multi-View Mode	77
7.3.4 Understanding Video Output Capabilities	78
7.3.5 Configuring Video Output	81
7.4 Configuring Audio.....	88
7.5 Specifying Conference Settings.....	90
7.5.1 Setting Audio and Video Protocols	90
7.5.2 Setting General Conference Parameters	90
7.5.3 Setting Advanced Conference Parameters	94
7.6 Specifying Network Settings	98
7.6.1 Setting IP Parameters	98
7.6.2 Setting H.323 Parameters	103
7.6.3 Setting SIP Parameters.....	105
7.6.4 Setting Wi-Fi Parameters.....	108
7.6.5 Setting SNMP Parameters.....	111
7.6.6 Setting Network Address Book Parameters	114
7.6.7 Setting Firewall Parameters	117
7.6.8 Setting Network Diagnostics Parameters.....	119

7.6.9 Setting QoS Parameters	120
7.6.10 Connecting to a 4E1 Network.....	122
7.6.11 Connecting to a PSTN Network.....	126
7.7 Security	126
7.7.1 Enabling Encryption	126
7.7.2 Supporting Remote Logins	127
7.7.3 Setting the Password of the Remote Control Administrator	128
7.7.4 Setting the Upgrade Password	129
7.7.5 Setting the Air Content Sharing Password	129
7.7.6 Setting Web Account Security	130
7.7.7 Setting Whitelist	131
7.8 Importing Security Certificates.....	132
7.8.1 Importing a Certificate.....	132
7.8.2 Importing Web Certificates	133
7.8.3 Updating Web Certificates	134
7.9 Managing System Files.....	134
7.9.1 Importing and Exporting Settings	134
7.9.2 Backing Up Settings	135
7.9.3 Importing License Files	135
7.9.4 Importing a Layout Policy File	136
7.9.5 Creating and Downloading a CSR File.....	137
8 Upgrading	138
8.1 Automatic Upgrade	139
8.2 Tool Upgrade	140
8.3 Upgrading the Endpoint Using the Mini System	143
8.4 Upgrading the Endpoint on Its Web Interface.....	144
9 Maintenance.....	145
9.1 Checking the Working Environment Periodically	146
9.2 Managing Common Users and Passwords.....	146
9.3 Customizing the Web Interface.....	147
9.4 Customizing the Remote Controlled UI	149
9.4.1 Customizing Onscreen Status Icons.....	149
9.4.2 Customizing the Home Screen.....	149
9.4.3 Customizing Conference Control Functions to Be Displayed	151
9.4.4 Customizing the Option Bar	151
9.5 Checking the Endpoint Periodically	152
9.6 Viewing System Status	152
9.7 Querying System Information.....	153
9.8 Querying Logs	153
9.9 Restoring Your Endpoint to Default Settings.....	154
10 Troubleshooting	155

10.1 Understanding Diagnosis Methods	155
10.2 Common Faults.....	159
11 Technical Specifications.....	171
11.1 Physical Specifications	171
11.2 Performance and Capacity	172
11.3 Ports and Protocols	173
11.4 Standards Compliance.....	176
A E1 and T1 Grounding Criteria	178
B Menu Structure of the Remote Controlled UI.....	179
C Requirements on Room Layout and Lighting.....	181
D Status Icons.....	182
E Default Settings	185
F Glossary.....	187

1 Overview

About This Chapter

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

[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 on an Administrator](#)

As an 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 on an Administrator

As an 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 and SIP 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 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.

Category	No.	Item	Description
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 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.

You can refer to the documentation listed in [Table 1-2](#).

Table 1-2 Reference documentation

Document	Description	When to Use	How to Obtain
HUAWEI TE40&TE50&TE60 Videoconferencing Endpoint V100R001C10 Quick Installation Guide	Describes the packaged items and provides guidance for quick installation, and common configuration.	When checking whether the carton contains all the required items and when installing the endpoint	Hold Ctrl and click the following hyperlink: Product Support > Unified Communications and Collaboration > Telepresence and Videoconferencing > Telepresence Endpoints > Group Endpoints .
HUAWEI TE40&TE50&TE60 Videoconferencing Endpoint V100R001C10 Quick Installation Guide	Describes the remote controlled UI and provides quick instructions in commonly-used endpoint functions.	When answering questions from standard users who are using the endpoint for the first time or unfamiliar with the endpoint	
HUAWEI TE40&TE50&TE60 Videoconferencing	Describes how to operate the endpoint.	When answering standard users' questions about	

Document	Description	When to Use	How to Obtain
Endpoint V100R001C10 User Guide		daily endpoint operations	
HUAWEI TE40&TE50&TE60 Videoconferencing Endpoint V100R001C10 Administrator Guide (this document)	Describes conference experience, device control, address book management, system settings, upgrade, maintenance, and troubleshooting based on the endpoint web interface.	When setting parameters, managing the address book, controlling conferences, upgrading the endpoint, and performing daily maintenance.	
HUAWEI TE40&TE50&TE60 Videoconferencing Endpoint V100R001C10 Help	Describes the endpoint web interface and method for using this interface.	When answering questions that standard users encounter on the endpoint web interface or explaining the parameters on this interface	Log in to the endpoint web interface and click the Help tab.

1.4 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.

Touch Panel Usage Precautions

- Do not tap the touch panel with excessive force.
- Do not let the touch panel exposed to water or other liquids.
- Place the touch panel on the desktop steadily to prevent it from falling.

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)

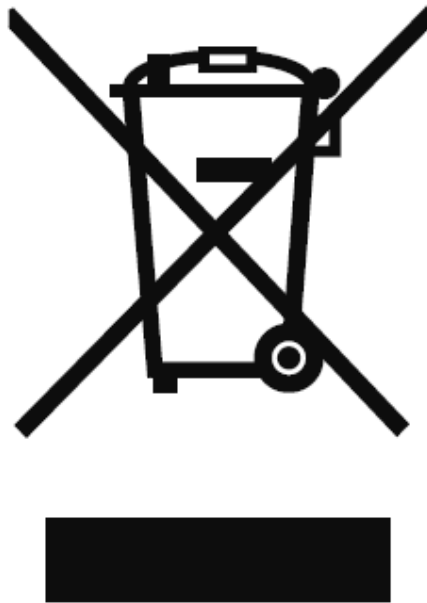
The endpoint complies with Directive 2002/95/EC, 2011/65/EU and other similar regulations from the countries outside the European Union, on the RoHS in electrical and electronic equipment. The endpoint does not contain lead, mercury, cadmium, and hexavalent chromium and brominated flame retardants (Polybrominated 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:



North American Regulatory Information

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.

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class A digital apparatus complies with Canadian ICES-003.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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 radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de classe A est conforme à la norme ICES-003 du Canada.

Cet équipement est conforme aux limites IC d'exposition aux radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à distance minimum de 20cm entre le radiateur et votre corps.

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.

Viewing the Help on the Endpoint Web Interface

The help on the endpoint web interface includes context-sensitive help and operation guide.

Context-sensitive help includes status icons and configuration verification messages. For example, if certain settings on the system settings screen are incorrect, a message will be displayed to indicate the error and how to rectify it.

The operation guide describes how to operate the endpoint web interface. When you are using the endpoint and the documents delivered with the endpoint are unavailable, you can click



in the upper right corner to read the operation guide.

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 (web interface query path: **Help > Version**)
- Software version (web interface query path: **Help > Version**)
- Network information (web interface query path: **Maintenance > System Status > Line Status**)
- Diagnostic and troubleshooting measures you have taken

2 Web-based Login

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

Configuring the Browser

Before running the endpoint web interface on a web browser, configure the browser.

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.

If you want to use Microsoft Internet Explorer 6.0 to access the endpoint web interface in HTTPS mode, enable HTTPS login mode for Microsoft Internet Explorer 6.0 as follows: Log in to the endpoint in Telnet or SSH mode. (The default user name and password are **debug** and **Change_Me**, respectively.) Run the **web ie6httpsmode 1** command to enable the HTTPS login mode.

The following description uses Window7 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.

- 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 **Security Settings** dialog box that is displayed, perform the operations as follows:
 - 1. Set all options under **Downloads** and **Scripting** to **Enable**.
 - 2. (Only Microsoft Internet Explorer 8.0) Select **Display mixed content** under **Miscellaneous**.
- Step 5** Click **OK**.
- Step 6** (Optional) On the **Security** tab, click **Trusted sites** and then **Sites**.
The **Trusted sites** dialog box is displayed.

Step 7 (Optional) In the **Add this website to the zone** text box, enter the IP address of your endpoint. Then click **Add**.

Step 8 (Optional) Click **OK**.

Step 9 Click the **Privacy** tab. Move the slider to display the **Medium** level.

Step 10 Click the **Advanced** tab. Select **Use TLS 1.0** under **Security**.

Step 11 Click **OK**.

The configuration is complete.

----End



NOTE

To ensure that information can be properly displayed, if you choose to skip [Step 6](#) through [Step 8](#), 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**.

Logging In to the Web Interface

Step 1 Open Internet Explorer.

Step 2 In the address box, enter the endpoint IP address, such as **192.168.1.1**.

Step 3 Press **Enter**.

The login page is displayed.

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



NOTE

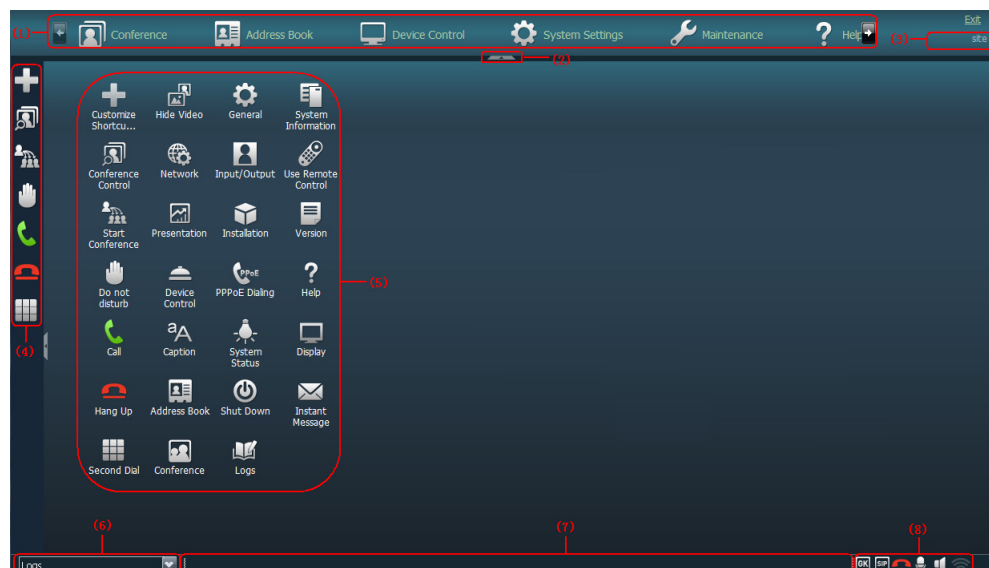
The default user name and password are **admin** and **Change_Me** respectively. You are advised to change the default password the first time you log in to the web interface, and then change your password regularly.

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

Step 6 Click **Log In**.

The home page is displayed, as shown in [Figure 2-1](#).

Figure 2-1 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

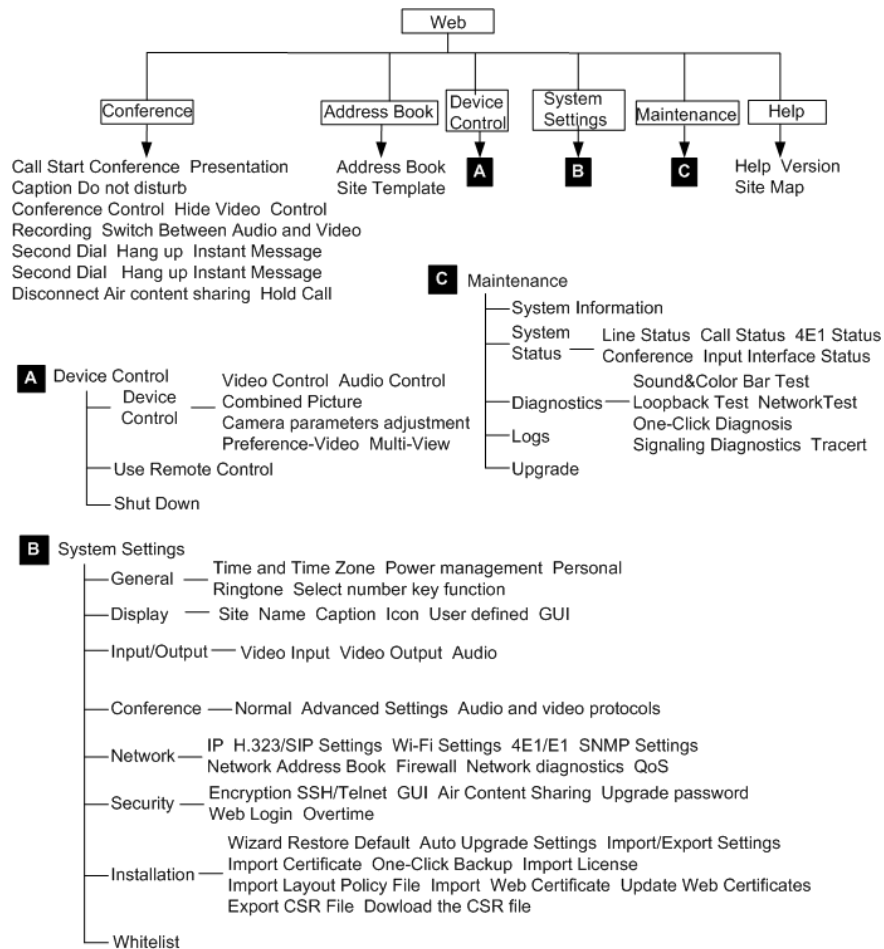
To ensure data security, after accessing the endpoint web interface, close the browser and delete browser caches.

3 Menu Structure of the Web Interface

Knowing the menu structure of the endpoint web interface helps you quickly find each function item.

All function items on the web interface can be accessed from the menu bar on the home page. [Figure 3-1](#) shows the menu structure.

Figure 3-1 Web interface menu structure



NOTE

Only the TE60 supports 4E1 functions.

To quickly access a function item, you can also choose **Help > Site Map** and click the hyperlink for the function item.



NOTE

For details about the menu structure of the remote controlled UI, see [B Menu Structure of the Remote Controlled UI](#).

4 Conference Experience

About This Chapter

You can initiate or join conferences in multiple ways on the endpoint web interface. During a conference, you can control the conference or share presentations.

4.1 Initiating a Point-to-Point Conference

You can initiate a point-to-point conference in multiple ways on the endpoint web interface.

4.2 Initiating a Multipoint Conference

You can initiate a multipoint conference in multiple ways on the endpoint web interface. During a multipoint conference, all the sites can hear and view each other.

4.3 Scheduling a Conference

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

4.4 Joining a Conference Using the Conference Access Number

When initiating a conference for which the participant sites are uncertain, you can set only the number of anonymous sites. With this setting, a site can join the conference by dialing the conference access number and then following the interactive voice response (IVR) instructions.

4.5 Joining an MSUC Convergent 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.

4.6 Joining an HD-Video Conference over an IMS Network

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

4.7 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.

4.8 Creating and Sending Captions

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

4.9 Using the Do-Not-Disturb Function

If you do not want to be disturbed by incoming calls, you can enable the Do-not-disturb function.

4.10 Controlling a Conference

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

4.11 Recording a Conference

Your endpoint can record local and multipoint conferences.

4.12 Sending and Receiving Instant Messages

During a conference, you can send instant messages to remote sites and view or close the instant messages sent from remote sites.

4.1 Initiating a Point-to-Point Conference

You can initiate a point-to-point conference in multiple ways on the endpoint web interface.

4.1.1 Initiating a Conference from the Call Page

On the call page, you can select a site, configure the line type and rate for the site, and place a call to the site to start a conference.

Step 1 Choose **Conference > Call**.

Step 2 Select a remote site you want to call using either of the following methods:

- Click **Call History** and select the remote site.
- Enter the name, number, or IP address of the remote site.

Step 3 Set the site parameters, listed in [Table 4-1](#).

Table 4-1 Site parameters

Parameter	Description	Setting
Site name/IP address/Number	Specifies the name, number, or IP address of the site you want to call.	To call a Cisco TelePresence site, you must set this parameter to the name of the Cisco TelePresence site.
Line type	Specifies the type of the line used to place the call. To call a Microsoft Lync site, set this parameter to Auto or SIP .	By default, the last used line type is displayed.
Rate	Specifies the data transmission rate required. The data transmission rates supported by your endpoint vary depending on the type of site you want to call.	Select the highest available data transmission rate. NOTE If this parameter is set incorrectly, the video quality will be affected or the call might even fail to be set

Parameter	Description	Setting
		up.
Call mode	Specifies the call type. • Video: Place video calls • Voice: Place audio-only calls This parameter is available only when Line type is set to Auto or SIP.	The default value is Video .



NOTE

The default settings of advanced conference parameters can meet the requirements of most simple conferences. Alternatively, you can click **Advanced Settings** and set advanced conference parameters. For the description of each advanced conference parameter, see [7.5.3 Setting Advanced Conference Parameters](#).

Step 4 Click **Call**.

----End

4.1.2 Initiating a Conference from the Address Book

You can select a site from the address book and place a call to the site to initiate a conference.

Procedure

Step 1 Choose **Address Book > Address Book**.

Step 2 Select one site you want to call from the local address book or the Lightweight Directory Access Protocol (LDAP) address book.

Step 3 Click **Call**.

----End

To modify the settings of a site you want to call, click the site.

4.1.3 Holding a Call

If you receive a call or want to call another site in a point-to-point conference, you can perform call hold operations.

Prerequisites

The **Multipoint call mode** parameter has been set to **Multipoint converge** on **System Settings > Conference > Normal** on the endpoint web interface.

Procedure

Scenario 1: You are in a point-to-point conference with site B, and site C calls you. You can perform any of the operations described in [Table 4-2](#).

Table 4-2 Call hold operations

Click...	To...
Reject	Reject the incoming call and continue the current point-to-point conference.
Accept & Hold Active	Answer the incoming call and place the current point-to-point conference on hold. NOTE After performing this operation, you can choose Conference > Hold Call and click any of the following: • Resume: Resume the conference call placed on hold and place the active call on hold. • On hold: Place the active call on hold. • Hang up: Disconnect a site.
Accept & End Active	Answer the incoming call and end the current point-to-point conference.
Ignore	Ignore the incoming call and close the call handling dialog box.

Scenario 2: You are in a point-to-point conference with site B and call site C. You can perform any of the following operations described in [Table 4-3](#) in the dialog box that is displayed.

Table 4-3 Call operations

Click...	To...
Hold Active & Call	Place the current point-to-point conference on hold and call site C. NOTE After performing this operation, you can choose Conference > Hold Call and click any of the following: • Resume: Resume the conference call placed on hold and place the active call on hold. • On hold: Place the active call on hold. • Hang up: Disconnect a site.
Cancel	Cancel calling site C.

4.2 Initiating a Multipoint Conference

You can initiate a multipoint conference in multiple ways on the endpoint web interface. During a multipoint conference, all the sites can hear and view each other.

4.2.1 Understanding the MCU and Built-in MCU

The endpoint needs to use the MCU or built-in MCU to initiate a multipoint conference. If the endpoint uses the built-in MCU to initiate a conference, no external MCU is required.

MCU

As an indispensable component in a multipoint conference, the MCU is responsible for multiple functions, such as site access, video exchange, audio mixing, data processing, and signaling interaction.

Built-in MCU

An endpoint with the built-in MCU function can initiate a multipoint conference by implementing functions such as site access, video exchange, audio mixing, data processing, and signaling interaction. The endpoint can work independently, without involving the other components on the videoconferencing network in conference scheduling. In this case, the endpoint functions as a mini MCU.



NOTE

- On the endpoint web interface, choose **Maintenance > System Information**, and check whether the endpoint has a built-in MCU.
- To provide the built-in MCU function, the endpoint requires a specified license. Contact Huawei post-sales engineers to purchase the license.

Conferences held with the built-in MCU function have the following features:

- After a point-to-point call is set up, site-by-site calls can be made to hold a multipoint conference.
- BFCP or H.239 presentation dual-stream conferences are supported. A SIP site supports BFCP dual-stream, an H.323 site supports H.239 dual-stream, and a hybrid conference supports both BFCP and H.239 dual-stream.
- Conferences can be locked from the built-in MCU. After a conference is locked, calls from new sites are restricted.
- Conferences can be attended by both H.323 and SIP sites and support H.323 site control.
- If a conference is held with a built-in MCU, only **Presentation** is available.

Built-in MCU Capabilities of TE40/TE50

The built-in MCU supports the access from six HD video sites and three audio-only sites simultaneously in a conference.

- The six HD video sites include the local site that uses its built-in MCU, that is, the built-in MCU site.
- A maximum of six 720p30 full-adaptive sites are supported.
- G.722 or G.711 full adaptation is supported.

Built-in MCU Capabilities of TE60

The built-in MCU supports the access from nine HD video sites and three audio-only sites simultaneously in a conference.

- The nine HD video sites include the local site that uses its built-in MCU, that is, the built-in MCU site.
- A maximum of nine 720p30 full-adaptive sites are supported.
- G.722 or G.711 full adaptation is supported.

Initiating a Multipoint Conference on the endpoint with a Built-in MCU

Before initiating a multipoint conference, you must enable the built-in MCU function. To do so, choose **System Settings > Conference > Normal** and set **Multipoint call mode** to **AUTO** or **Built-in MCU**.

To initiate a multipoint conference using the built-in MCU, call the first site and then place calls one at a time to several other sites. For details about other methods for initiating a multipoint conference, see [4.2.2 Initiating a Conference from the Predefined Conference Page](#), [4.2.3 Initiating a Conference from the Conference History Page](#), and [4.2.4 Initiating a Conference from the Address Book Page](#).

For example, to use the built-in MCU of endpoint A to initiate a conference that includes endpoints A, B, C, and D, perform the following steps:

From endpoint A, call endpoints B, C, and D until all the calls are set up.



NOTE

If the built-in MCU of an endpoint is used during a conference, **Lock conference** can be selected from the **Conference control** screen on the endpoint whose built-in MCU is being used to prevent unwanted additional sites joining the conference.

Conference Control

Three types of roles exist in a multipoint conference initiated using the built-in MCU: Endpoint to which the built-in MCU belongs, chair site, and non-chair sites. A site can request chair control rights only after chair control is enabled on the Endpoint to which the built-in MCU belongs. The chair control is enabled by default.



NOTE

Only H.323 sites support conference control functions.

Table 4-4 Conference control in a multipoint conference initiated using the built-in MCU

Role	Conference Control
Endpoint to which the built-in MCU belongs	Enable chair control, Disable chair control, Lock conference, Set Continuous Presence, and Recording
Chair site	Release Chair, End conference, Delete Site, Add site, Set Continuous Presence, and Recording NOTE Only H.323 sites where the endpoints in V100R001C10 are used support the Conference Video Layout and Start functions.
Non-chair site	Request chair



NOTE

The recording function is available only when the recording server address is configured on the Endpoint to which the built-in MCU belongs.

Continuous Presence on the Endpoint to Which the Built-in MCU Belongs

The Endpoint to which the built-in MCU belongs adjusts the continuous presence layout based on the number of sites in the conference, and can add the local video and presentation

to continuous presence. A maximum of 7 sites are supported in continuous presence on the TE40/TE50, and a maximum of 10 sites are supported in continuous presence on the TE60.



NOTE

- The maximum number of sites in continuous presence includes the local video and presentation.
- For details about how to add the local video and presentation to continuous presence, see the description of **Add presentation to continuous presence** and **Add local video to continuous presence** in [7.5.2 Setting General Conference Parameters](#). The two parameters are invalid to H.323

sites where the endpoints in V100R001C10 are used. For these sites, you can press  on the remote control to add the local video or presentation to continuous presence.

4.2.2 Initiating a Conference from the Predefined Conference Page

On your endpoint, you can create a conference on the predefined conference page and initiate it from this page.

Prerequisites

You can use SiteCall or the built-in MCU to initiate a multipoint conference.

- **SiteCall:** Before initiating a conference, define the participant sites and register your endpoint with the GK server. Then disable the built-in MCU as follows: Choose **System Settings > Conference > Normal** and set **Multipoint call mode** to **Multipoint converge** or **OFF**.
- **Built-in MCU:** Before initiating a conference, enable the built-in MCU as follows: Choose **System Settings > Conference > Normal** and set **Multipoint call mode** to **Built-in MCU** or **AUTO**. If it is defined on the Service Management Center (SMC) as a manageable participant, its built-in MCU capabilities will be restricted by the SMC. In this case, consult the SMC administrator about the maximum number of calls supported by the endpoint.



NOTE

To provide the built-in MCU function, the endpoint requires a specific license. Contact Huawei post-sales engineers to purchase the license.

Procedure

Step 1 Choose **Conference > Start Conference** and click the **Predefined Conferences** tab.

Step 2 Click **Create Conference** and perform either of the following:

- Click **Address Book**. On the displayed tab, select the desired sites.
- Click **LDAP Address Book**. On the displayed tab, search for and select the desired sites.

Step 3 Click .

The selected sites are added to the site list on the right.

Step 4 Set the conference parameters.

- If you use the built-in MCU to initiate the conference, set **Conference Name**, **Rate**, and **Support recording** only.
- If you use SiteCall to initiate the conference, set all the parameters listed in the table.

Table 4-5 Conference parameters

Parameter	Description	Setting
Conference Name	Specifies the name of the conference.	-
Rate	Specifies the data transmission rate for the conference.	To help ensure conference quality, set this parameter to 1920 kbps or a larger value.
Continuous presence	Specifies the maximum number of site videos that can be viewed simultaneously during the conference. When continuous presence is broadcast, the sites in the conference can view the videos of multiple sites simultaneously. If you select Disable , the conference does not support continuous presence.	The default value is Disable .
Other parameters	Specifies the mode for setting conference parameters. Auto-sensing: Your endpoint sets conference parameters to be the same as the parameter settings described in 7.5 Specifying Conference Settings. User defined: You must manually set Conference control password, Anonymous H.323 sites, Anonymous PSTN sites, H.235 conference, and Paying site.	The default value is Auto-sensing .
Conference control password	Specifies the password to the conference. This password is required for: - The site that wants to chair the conference to obtain the chair control rights. - Anonymous sites to join the conference for authentication. For details about how to use the password to join an authentication conference, see 4.4 Joining a Conference Using the Conference Access Number.	Enter a value that contains 1 to 32 digits.
Anonymous H.323 sites Anonymous PSTN sites	Specify the number of IP or public switched telephone network (PSTN) anonymous sites that are allowed to join the conference. Anonymous sites are the sites whose numbers are not defined. To allow five IP or PSTN anonymous sites to join the conference, set the Anonymous H.323 sites parameter to 5 . To disallow any IP or PSTN anonymous sites to join the conference, set the Anonymous PSTN	The default value is 0 .

Parameter	Description	Setting
	sites parameter to 0 .	
H.235 conference	Specifies the conference security type. • Insecure conference: No data transmitted during the conference is encrypted. • Secure media conference: Media streams are encrypted.	The default value is Insecure conference. To enhance the communication security on your endpoint, select Secure media conference. NOTE If you select Secure media conference, confirm that Encryption is set to Enable or Maximum interconnectivity on your endpoint and the endpoints to call. Otherwise, the calls will fail.
Paying site	Specifies the party that will be charged for the conference. • Local site: The local site pays for the conference. • Another site: Another site pays for the conference. If you select this option, you must fill in Paying account and Paying password.	The default value is Local site .
Support live broadcast	Specifies whether your endpoint supports live broadcasting for multipoint conferences hosted by standalone MCUs.	By default, this parameter is deselected, indicating that the endpoint does not support live broadcasting.
Support recording	Specifies whether your endpoint supports recording for multipoint conferences hosted by standalone MCUs.	By default, this parameter is deselected, indicating that the endpoint does not support recording.
Date	Specifies the conference start time. This parameter is mandatory only when you schedule a conference.	No default value is set for this parameter.
Duration	Specifies the conference duration. This parameter is mandatory only when you schedule a conference.	Unit: minute Do not leave this parameter blank.

Step 5 Click **Hold Conference.**

The conference is initiated according to the parameters you set.

---End

4.2.3 Initiating a Conference from the Conference History Page

The conference history contains the records of conferences your endpoint initiated or attended and sites your endpoint placed calls to or received calls from. You can select a record from the conference history to initiate a new conference.

Prerequisites

You can use SiteCall or the built-in MCU to initiate a multipoint conference.

- SiteCall: Your endpoint has registered with a GK server, and **Multipoint call mode** is set to **Multipoint converge** or **OFF** under **System Settings > Conference > Normal**.
- Built-in MCU: **Multipoint call mode** is set to **Built-in MCU** or **AUTO** under **System Settings > Conference > Normal**.



NOTE

To provide the built-in MCU function, the endpoint requires a specific license. Contact Huawei post-sales engineers to purchase the license.

Background

The conference history stores a maximum of 50 records.

Procedure

Step 1 Choose **Conference > Start Conference** and click the **Conference History** tab.

Step 2 Select a record and click .

The conference starts.

----End

4.2.4 Initiating a Conference from the Address Book Page

From the address book on your endpoint, you can select sites to initiate a conference.

Prerequisites

You can use SiteCall or the built-in MCU to initiate a multipoint conference.

- SiteCall: Your endpoint has registered with a GK server, and **Multipoint call mode** is set to **Multipoint converge** or **OFF** under **System Settings > Conference > Normal**.
- Built-in MCU: **Multipoint call mode** is set to **Built-in MCU** or **AUTO** under **System Settings > Conference > Normal**.



NOTE

To provide the built-in MCU function, the endpoint requires a specific license. Contact Huawei post-sales engineers to purchase the license.

Procedure

Step 1 Choose **Address Book > Address Book**.

- Step 2** Select sites from the local address book. Alternatively, search for sites from the LDAP address book, save the found sites in the local address book, and select the sites from the local address book. Then click **Start Conference**.
- Step 3** Set the conference parameters. Refer to [4.2.2 Initiating a Conference from the Predefined Conference Page](#).
- Step 4** Click **Hold Conference**.
- The conference starts.
- End

4.3 Scheduling a Conference

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

Prerequisites

You have set **Conference line type** in advanced conference settings to **H.323** or **Auto**. For details about the settings, see [7.5.3 Setting Advanced Conference Parameters](#).

Your endpoint has registered with a GK server, and **Multipoint call mode** is set to **Multipoint converge** or **OFF** under **System Settings > Conference > Normal**.

Procedure

Method 1: Create and schedule a conference.

- Step 1** Choose **Conference > Start Conference** and click the **Schedule Conference** tab.
- Step 2** Click **New Schedule**. Select conference sites and set the conference parameters. Refer to [4.2.2 Initiating a Conference from the Predefined Conference Page](#).
- Step 3** Click **Schedule**.
- The conference is scheduled.
- End

Method 2: Create and schedule a predefined conference or schedule a predefined conference that exists in the **Predefined Conferences** list.

- Step 1** Choose **Conference > Start Conference** and click the **Predefined Conferences** tab.
- Step 2** Click **Create Conference** or an entry in the **Conference Name** column.
- The **Hold Conference** page is displayed.
- Step 3** Select conference sites and set the conference parameters. Refer to [4.2.2 Initiating a Conference from the Predefined Conference Page](#).
- Step 4** Click **Schedule**.
- The conference is scheduled.
- End

Method 3: Schedule a conference in the **Conference History** list.

Step 1 Choose **Conference > Start Conference** and click the **Conference History** tab.

Step 2 Click an entry in the **Conference Name** column.

The **Hold Conference** page is displayed.

Step 3 Select conference sites and set the conference parameters. Refer to [4.2.2 Initiating a Conference from the Predefined Conference Page](#).

Step 4 Click **Schedule**.

The conference is scheduled.

----End

Conferences scheduled using any of the preceding methods are displayed in the **Schedule Conference** list.

4.4 Joining a Conference Using the Conference Access Number

When initiating a conference for which the participant sites are uncertain, you can set only the number of anonymous sites. With this setting, a site can join the conference by dialing the conference access number and then following the interactive voice response (IVR) instructions.

Background

A site dials a conference access number and follows the IVR instructions to enter the specified password to join a conference. This process is called two-stage dialing.

Procedure

Step 1 Obtain the access number for the authentication conference.

When a conference starts, endpoints that have joined the conference can view the conference access number by choosing **Maintenance > System Status > Conference**. Anonymous sites can obtain the conference access number and authentication password from the SMC administrator or chair site using other methods.

Step 2 Choose **Conference > Call**.

Step 3 In **Site name/IP address/Number**, enter the access number.

Step 4 Set the call parameters. Refer to [4.1.1 Initiating a Conference from the Call Page](#).



NOTE

Select the highest data transmission rate supported by your endpoint to increase the call success rate.

Step 5 Click **Call**.

Step 6 Choose **Conference > Second Dial**. Follow the IVR instructions to select a language and enter the password (if any) to join a conference.

----End

4.5 Joining an MSUC Convergent 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.

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

Procedure

Step 1 Register the endpoint with the MSUC network.

1. On the endpoint web interface, choose **System Settings > Network** and click the **H.323/SIP Settings** tab.
2. Click the **SIP** tab and set the parameters for interworking with the MSUC to register the endpoint with a Lync server. [Table 4-6](#) describes the related parameters.

Table 4-6 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.	Set this parameter to Enable .
Server	Specifies the IP address or domain name	Example 1: 192.168.1.10

Parameter	Description	Setting
address	of the Lync Server with which you want 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. • 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. • 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	Only TCP and TLS transmission are supported.

Parameter	Description	Setting
	security. Note that selecting this option may affect the call rate. If you select this parameter, you can set SSL version .	
SSL version	Specifies the encryption protocol used for SIP calls, including TLS 1.0 and SSL 3.0 .	The default value is TLS 1.0 .
Video request handling	Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference. • 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. Click **Save**.

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

1. Choose **Conference > Call**.
2. In the text box, enter the Lync client number.
3. Click **Call**.

----End

4.6 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. On the endpoint web interface, choose **System Settings** > **Network** and click the **H.323/SIP Settings** tab.
2. Click the **SIP** tab and set the parameters for interworking with the IMS, as described in [Table 4-7](#).

Table 4-7 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 servers. NOTE If you select this parameter, you must also set Server address, Conference service number, Site number, User name, and Password.	Set this parameter to Enable .
Server address	Specifies the IP address or domain name of the IMS server with which you want the endpoint to register. 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.	IP address example: 192.168.1.10 Domain name example: huawei.com It is recommended that you set Server address to the domain name of the IMS server with which you want the endpoint to register.
Conference service number	Specifies the conference service number for your endpoint to initiate conferences over an IP multimedia subsystem (IMS) network.	Set this parameter to the conference service number obtained from the IMS network administrator.
Proxy server	Specifies whether to enable the proxy server. You must enable the proxy server when	Set this parameter to Enable .

Parameter	Description	Setting
	using the IMS network.	
Proxy server address	Specifies the address of the proxy server. If you set Server address to the IMS server domain name, set this parameter to the IP address bound to that domain name.	Example: 192.168.1.10.
Site number	Specifies the site number for your endpoint. 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.	The parameter value must contain only digits. Example: 12345
User name Password	Specifies the user name for authentication registration.	The value can contain digits, letters, and special characters, such as @ # %. Example: +0867552842007@huawei.com Obtain the value of this parameter from the IMS server administrator.
Server type	Specifies the SIP server type. • 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 Standard .
Transmission type	Specifies the protocol used for SIP signaling transmission. • 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.	Set this parameter to UDP . The IMS network only supports UDP transmission.
Video request	Specifies how your endpoint handles video requests from a remote endpoint	The default value is Manual .

Parameter	Description	Setting
handling	during a point-to-point SIP audio call or multipoint conference. • 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.	

3. Click **Save**.

Step 2 Choose **Conference > Call**.

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

Step 4 Click **Call**.

Step 5 Choose **Conference > Second Dial**.

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.

4.7 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 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 [7.5.3 Setting Advanced Conference Parameters](#).

The presentation video source has been connected.

- **Wired connection**
Use a cable to connect the computer to a video input port on the endpoint.
- **Air content sharing client**
 1. (Optional) In the address box, enter the endpoint IP address and press **Enter**.

2. (Optional) In the upper left corner of the login page, click **Download Air Content Sharing Client** and install the client as prompted.



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

If this is the first time you are installing the air content sharing client, you must restart your computer before you can use it.



3. Double-click .
4. Double-click the endpoint to connect, or enter the endpoint IP address and click **Connect**.
5. In the displayed dialog box, enter the password and click **Connect**.

The default password is **Change_Me**. For details, see [7.7.5 Setting the Air Content Sharing Password](#).



NOTE

Alternatively, ignore the dialog box and watch for the message **An air content sharing source device requests to connect to your endpoint. Accept?** that will be displayed on the endpoint web interface and remote controlled UI. When the message is displayed, select **Accept**. The client then successfully connects to the endpoint without any passwords.

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 [7.5.3 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

Step 1 Choose **Conference > Presentation**.

Step 2 In the displayed dialog box, click **Share**.

The presentation is shared with remote sites.

----End

To stop sharing the presentation, click **Stop**.

4.8 Creating and Sending Captions

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

Procedure

Step 1 Choose **Conference > Caption**.

Step 2 Click **Middle Caption**, **Bottom Caption**, or **Banner**. Then you can:

- Share a caption in the **Caption List** list or a banner in the **Banner Title** list.
- Preview a caption or banner on the display at your site.
- Edit a caption or banner.
- Save a caption or banner.
You can save a maximum of 10 entries to the **Caption List** or **Banner Title** list.
- Create or delete a caption or banner.

----End

4.9 Using the Do-Not-Disturb Function

If you do not want to be disturbed by incoming calls, you can enable the Do-not-disturb function.

Procedure

Step 1 Choose **Conference > Do-not-disturb**.

The **Do-not-disturb** dialog box is displayed.

Step 2 Select **Enable** for **Do-not-disturb** and click **OK**.

----End

4.10 Controlling a Conference

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

Icons on the Conference Control Page

Table 4-8 lists common icons displayed on the conference control page.

Table 4-8 Icons on the conference control page

Icon	Description	Icon	Description
	The site is not in the conference.		Your site is chairing the conference.
	The site is in the conference.		
	The site is being broadcast.		The site is being viewed.
	The speakers of the site have been muted, and the site cannot hear the		The microphones of the site have been muted, and the other sites in the

Icon	Description	Icon	Description
	current conference.		conference cannot hear the site.
	The site is sharing a presentation.		The site is a PSTN, H.323 PHONE, or SIP audio site.

Table 4-9 lists the icons used to adjust the site display mode on the conference control page.

Table 4-9 Icons used to adjust the site display mode

Icon	Description
	Refreshes the conference control page.
	Displays sites in a list.
	Displays sites as icons.

Controlling a Multipoint Conference Hosted by the MCU



NOTICE

- Note that not all the conference control functions listed in Table 4-10 are available on the conference control page during a conference, depending on your role in the conference and the settings of conference control page.

Table 4-10 lists the conference control functions available in a multipoint conference hosted by the MCU.

Table 4-10 Conference control functions

Conference Control Function	Applicable Role	Description
Request Chair	Non-chair site	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. To request chair control rights, click Request Chair and enter the conference control password, that is, the chair password. NOTE Obtain the conference control password from the SMC administrator or the site that initiates the conference.

Conference Control Function	Applicable Role	Description
Request Floor	Non-chair site	If a non-chair site wants to speak during a conference, the site can request the floor from the chair site. This function is especially useful when a remote site is being broadcast. 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. - To give the floor to the requesting site, the chair site clicks Sites Requesting Floor and clicks the site in the list. 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.
View Site	Non-chair site Chair site	- Non-chair site: can use this function when no site or continuous presence is being broadcast during a conference; can view the sites residing on the local MCU or MCUs of the same level only. - Chair site: can view any sites residing on the local MCU and MCUs cascaded to the local MCU; can view a site even when another site is being broadcast in continuous presence. To view a single site, click View Site and select the site or continuous presence to view. To view sites in turn, click View Site, select In Turn on the View Site page, select the sites to view one by one, and click Start Viewing Sites in Turn. To stop viewing sites in turn, click Stop Viewing Sites in Turn.
Revoke Chair	Site that initiates the conference	Click 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.
Call Site Call All	Chair 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 an absent site, click Call Site. To call all absent sites included in the conference site list into the conference, click Call All. The status of a successfully connected site changes from  to .
Add Site	Chair site	You can add sites to an ongoing conference, regardless of whether those sites have been defined in the address book. The MCU hosting the conference then places calls to the added sites. To add sites from the local or LDAP address book or add sites that have not been defined in the address book, click Add Site.

Conference Control Function	Applicable Role	Description
Delete Site	Chair site	To delete an absent site or a site that has joined the conference, click Delete Site, select the site, and confirm the operation. The chair site can disconnect a site from the conference and remove the site from the site list. To enable the site to join the conference again, the chair site must add the site to the conference by performing the Add Site operation.
Hang Up	Chair site	To disconnect a site that has joined the conference, click Hang Up, select the site, and confirm the operation. After a site is disconnected, the site still belongs to the conference but is marked with . To have the site join the conference again, the chair site can perform the Call Site operation.
Broadcast Site	Chair site	The chair site can broadcast any non-audio-only site, including the chair site itself, or broadcast multiple sites in turn. To broadcast a single site, click Broadcast Site and select the site to broadcast. When a site is broadcast, all non-chair sites are forced to view the video of the broadcast site while the chair site can view the video of any site that is present at the conference. To stop broadcasting a site, perform Stop Broadcasting or Discussion operation. To broadcast sites in turn, click In Turn, select In Turn on the Broadcast Site page, select the sites to broadcast one by one, and click Start Broadcasting Sites in Turn. When multiple sites are broadcast in turn, all sites are forced to view the video of the broadcast sites. To stop broadcasting sites in turn, click Stop Broadcasting Sites in Turn.
End Conference	Chair site	If a conference is completed before the scheduled time, the chair site can use the End Conference function to end the conference in advance.
Set Continuous Presence	Chair site	View multiple sites at the same time. The continuous presence function is used to display the video from two or more sites on the same display at the same time. The number of the sites to be displayed and the layout of the site videos vary according to continuous presence modes. This function is available only when continuous presence resources have been reserved for the conference. Click Set Continuous Presence, and choose a layout mode from the Layout drop-down list box on the Set Continuous Presence page. You can click a site to display the site in the highlighted pane as required.
Mute/Unmute Speaker	Chair site	- To disable the speaker of a site, click Mute Speaker and select the site. The site is marked with  and cannot hear other sites in the conference. - To enable the speaker of a site, click Unmute Speaker and select the site. Then the site can hear other sites in the

Conference Control Function	Applicable Role	Description
		conference.
Mute/Unmute MIC	Chair site	- To disable the microphone of a site, click Mute Microphone and select the site. The site is marked with  and cannot be heard by other sites in the conference. - To enable the microphone of a site, click Unmute Microphone and select the site. Then the site can be heard by other sites in the conference.
Voice activation	Chair site	Voice activation is used in discussion mode. When voice activation is enabled, the site with the loudest voice is displayed to other sites in the conference. To enable voice activation, click Voice activation, set Sensitivity on the Voice activation page based on your experience, and click Start. High: Voice activation threshold volume is low. Medium: Voice activation threshold volume is set to a medium level. Low: Voice activation is performed when the voice volume is high. After you enable voice activation and set the sensitivity: - If the sound of one or multiple sites exceeds the voice activation threshold defined on the MCU, the video of the loudest site is broadcast. - If the voice activation threshold is not exceeded, the conference status is not changed. To disable the voice activation function, click Disable.
Lock Presentation	Chair site	Restrict the presentation sharing rights of a site or a conference. - Locking site presentation: When the chair site locks the presentation rights of a site, only that site can share presentations. - Locking conference presentation: When the chair site locks the conference presentation, a site can share its presentation if no other site in the conference is doing so. To cancel locking, click Unlock Presentation. NOTE Before using this function, ensure that the MCU and service software used with your endpoint support this function.
Extend Conference	Chair site	If a conference is not likely to be complete by the scheduled time, click Extend Conference, set Extension time (in min.) on the Extend Conference page, and click OK to extend the conference for the specified time. Before extending a conference, you must ensure that the videoconferencing resources and your account balance are sufficient to cover an extension. To increase the chances of

Conference Control Function	Applicable Role	Description
		success, extend the conference by 30 minutes at most at a time.
Revoke Presentation	Chair site	To stop a site from sharing a presentation, the chair site can revoke the presentation sharing right of the site. This function is available in a dual-stream conference.
Discussion	Chair site	The chair site can enable discussion to cancel certain ongoing site control or conference control operations, such as broadcasting sites. This Discussion function is used to cancel the following operations performed by the chair site: • Broadcasting a site • Muting the speaker • Muting the microphone • Giving the floor In discussion mode: • Audio: All sites have unmuted microphones, and the sound of all the sites together are broadcast to every site. • Video: The video viewed by each site does not change and each site can view any other site.
Give Floor	Chair site	Using this function, the chair site can give the floor to a site and mute all other sites. After the chair site gives the floor to a site, the video and sound of the site are broadcast, and all sites are muted, except the chair site and the site that has the floor. Although the Stop Broadcasting function is available even when a site has the floor, the chair site cannot take back the floor using Stop Broadcasting. After the chair site gives the floor to a site, the video and sound of the site are broadcast, and all sites are muted, except the chair site and the site that has the floor. If the chair site clicks Stop Broadcasting at this time, broadcasting a site stops, but the other non-chair sites are still muted.
Sites Requesting Floor	Chair site	During a conference, after a non-chair requests the floor, the site is added to the floor-requesting sites list. The chair site can select a site from the list to give the floor to that site. The video of that site is then broadcast, and the microphones of all sites are muted, except the chair site and the site that has the floor. Once given the floor, the site is removed from the floor-requesting sites list.
Release Chair	Chair site	Releases chair control rights. When chair control rights are released, any sites in the conference can request to become the chair site.
Monitor Video	All sites	View the video and presentation of a remote site in real time. You can also adjust the sizes of the video and presentation. In this way, you can monitor the status and video quality of the

Conference Control Function	Applicable Role	Description
		remote site. You can also monitor the video from the page described in section 5.1 Viewing the Video . NOTE The video and presentation can be viewed in real time only when the video monitoring function is enabled. This function involves personal privacy. Ensure that its use complies with local laws and regulations.
Recording	Chair site	From the conference control page, click Start to start recording and Stop to stop recording. NOTE To ensure rights of sites, read the instructions and suggestions for using recording products in the latest HUAWEI RSE6500 Security Maintenance before using the products.

Controlling a Multipoint Conference Hosted by a Built-in MCU

[Table 4-11](#) lists the conference control functions available in a multipoint conference hosted by a built-in MCU.

Table 4-11 Conference control functions

Conference Control Function	Applicable Role	Description
Request Chair	Non-chair site	For details, see Table 4-10 . NOTE Obtain the conference control password from the endpoint to which the built-in MCU belongs.
Enable Chair Control	endpoint to which the built-in MCU belongs	The sites in the conference can request chair control rights only after you enable the chair control on the endpoint. After a site becomes the chair site, the following conference control functions are unavailable to the endpoint: • Lock conference • Conference video layout • Recording You can use the preceding conference control functions on the endpoint only after click Disable Chair Control .
Disable Chair Control	endpoint to which the built-in MCU belongs	This function is used to disable chair control in a conference. For example, if a chair site exists in a conference, the site whose built-in MCU is being used can use this function to revoke chair control rights. In addition, the sites in the conference cannot request to become the chair site afterward.
Lock	endpoint to	The Lock conference operation can be performed only from

Conference Control Function	Applicable Role	Description
conference	which the built-in MCU belongs (when no chair site exists in the conference)	the endpoint whose built-in MCU is being used. After the Lock conference operation is performed, the endpoint whose built-in MCU is being used can call the other endpoints to join the conference, but other endpoints cannot call into the conference. To enable other endpoints to call into the conference, perform the Unlock Conference operation.
Conference Video Layout	endpoint to which the built-in MCU belongs (when no chair site exists in the conference) Chair site	This function is used to set the view displayed to all sites. • Voice activated, full screen: The remote sites view, in full screen, the video of the site that generates the loudest volume. • Voice activated, in panes: The remote sites view continuous presence, with the main pane displaying the video of the site that generates the loudest volume. • Bisect: The remote sites view, in bisect mode, the videos of the other sites. The site that generates the louder volume is highlighted. A presentation will not be displayed in this layout. • Fixed site, full screen: The remote sites view, in full screen, the video of a specified site. To view a site in full screen, click it in the site list. • Fixed sites, in panes: The remote sites view continuous presence, with the main pane displaying the video of a specified site. To add a site to the main pane, click it in the site list. NOTE • After you set this parameter, the viewed site views other sites in full screen or continuous presence mode. • This function is available only for H.323 sites where the endpoints in V100R001C10 are used. This function cannot be performed by the following sites at the same time: • Chair site • Site where the built-in MCU is used (in a conference hosted by a built-in MCU and not chaired by any site)
Recording	endpoint to which the built-in MCU belongs (when no chair site exists in the	For details, see Table 4-10. NOTE This function is available only for H.323 sites where the endpoints in V100R001C10 are used. To ensure rights of sites, read the instructions and suggestions for using recording products in the latest HUAWEI RSE6500 Security Maintenance before using the products.

Conference Control Function	Applicable Role	Description
	conference) Chair site	
End Conference	endpoint to which the built-in MCU belongs Chair site	For details, see Table 4-10 .
Release Chair Delete Site Add Site	Chair site	For details, see Table 4-10 .

On the conference control page, you can also perform the following operations:

If the sites in a conference have been classified into groups in a site template, you can select a group from the  drop-down list box. Then, the sites in the selected group are displayed in the preset mode. For details about how to set site groups, see [6.4 Customizing a Site Template](#).

4.11 Recording a Conference

Your endpoint can record local and multipoint conferences.

Prerequisites

To ensure rights of participants, read the instructions and suggestions for using recording products in the latest HUAWEI RSE6500 Security Maintenance before using the products.

Table 4-12 Recording prerequisites

Conference Type	Recording Prerequisites
Local conference	The recording server IP address or URL is set on the endpoint.
Multipoint conference hosted by a Huawei standalone MCU (such as the HUAWEI VP9660 MCU)	- The recording server is online. NOTE Check the recording server's online status from the Service Management Center (SMC). - The endpoint and the recording server have registered with a GK server. Support recording is selected. For details,

Conference Type	Recording Prerequisites
	see 4.2.2 Initiating a Conference from the Predefined Conference Page .
Multipoint conference hosted by a built-in MCU	The recording server IP address or URL is set on the endpoint.

Background

- During recording of local conferences, the endpoint cannot place or answer calls.
- During recording of local conferences, you can perform **Start**, **Pause**, **Resume**, and **Stop** operations. During recording of multipoint conferences, you can perform **Start** and **Stop** operations.
- When a Huawei standalone MCU is used to host a conference, you can enable or disable live broadcast and recording for the conference.
- When a built-in MCU is used to host a conference, you can enable or disable recording for the conference.
- During a multipoint conference, the chair site and the site where the built-in MCU is used can perform recording operations.
- To record a local conference, follow the following steps in this section. To record a multipoint conference, see [4.10 Controlling a Conference](#).

Procedure

Step 1 Choose **Conference > Control Recording**.

Step 2 Click **Start**.

The recording starts.

----End

To stop recording, click **Stop**.

4.12 Sending and Receiving Instant Messages

During a conference, you can send instant messages to remote sites and view or close the instant messages sent from remote sites.

Prerequisites

- Your endpoint is in a conference.
- Your endpoint uses H.323. Only H.323 sites can send and receive instant messages.
- T.140 captions have been enabled on your endpoint, because instant messages are a type of T.140 caption. To enable T.140 captions, choose **System Settings > Display > Caption** and set **Sharing mode** to **T.140**.

Procedure

Step 1 Choose **Conference > Instant Message**.

Step 2 In the displayed **Instant Message** dialog box, enter a message.

Step 3 Select the desired remote sites and click **Send**.

The message is sent to the remote sites. When receiving the message, the remote sites can view and close the message.

----End

5 Device Control

About This Chapter

After a conference starts, you can control the video and audio devices on the endpoint web interface to obtain the expected conference effect.

5.1 Viewing the Video

After the video monitoring function is enabled, you can view the video and presentation of local and remote sites on the endpoint web interface.

5.2 Controlling a Camera

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

5.3 Setting a Camera Preset

Camera presets are camera positions you set and save ahead of time. A camera preset stores the pan, tilt, and zoom settings of the camera. You can easily control the camera by switching between camera presets. You can configure remote camera presets before and during conferences.

5.4 Selecting Video Sources

The endpoint provides multiple video input ports for connecting to video devices. When multiple video devices are connected, you can set one video device as the local video source and another one as the local presentation source. You can also select the video or presentation to be displayed through video output ports.

5.5 Controlling Audio

On your endpoint, you can adjust the audio effects. For example, you can adjust the volume of the microphone and speaker.

5.6 Setting the Combined Picture

With the combined picture function, you can view multiple videos (such as the local and remote videos and presentations) in Picture in Picture (PiP) or split-screen mode on one display.

5.7 Setting Camera Parameters

On your endpoint, you can set the camera parameters, including video mode, noise reduction, and video resolution. You can view the video result of your settings on the display connected to your endpoint.

5.8 Setting Preferred Video Parameters

If you find that the displayed video deviates from its normal position, adjust the picture offset. If a blurring or slight jitter issue occurs in the video, adjust the sampling phase.

5.9 Setting Up a PPPoE Dial-Up Connection

Correct IP parameter settings on your endpoint enable you to set up a PPPoE dial-up connection with a broadband network to communicate with other network devices.

5.10 Using the Remote Control

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

5.1 Viewing the Video

After the video monitoring function is enabled, you can view the video and presentation of local and remote sites on the endpoint web interface.

Prerequisites

The video monitoring function has been enabled. This function can be enabled only on the remote controlled UI. To enable the video monitoring function, choose **Advanced > Settings > Secured > Web Login** and select **Monitor video**.



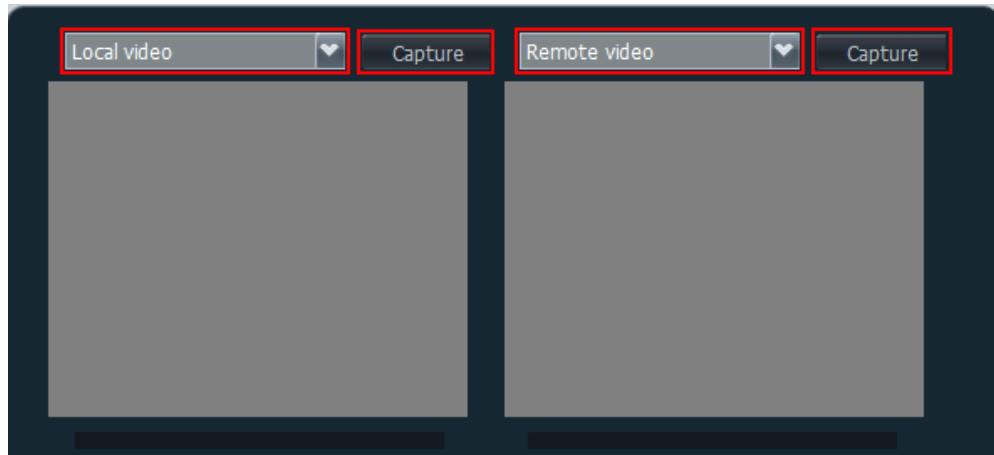
NOTICE

This function involves personal privacy. Ensure that its use complies with local laws and regulations.

Procedure

Log in to the web interface, choose **Device Control > Device Control**, and click the **Video Control** tab to view the video of local and remote sites, as shown in [Figure 5-1](#).

Figure 5-1 Viewing the video



You can click the drop-down list box to select the video source to view, or click **Capture** to capture a picture of the video that is being played.

5.2 Controlling a Camera

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

Prerequisites

You are familiar with the following buttons for camera control:

- : Turns the camera upward, downward, leftward, and rightward.
- : Turns the camera forward.
- : Enlarges the image taken by a camera.
- : Zooms in on a scene.
- : Shrinks the image taken by a camera.
- : Zooms out on a scene.
- : Automatically adjusts the camera focus.

Procedure

Step 1 Choose **Device Control > Device Control**.

- Step 2** In the upper right corner of the **Video Control** page, select the camera you want to control, as shown in [Figure 5-2](#).

Figure 5-2 Camera control



- When your endpoint is not in a conference, you can select only **Local camera**.
- When your endpoint is in a conference, you can select **Local camera** or **Remote camera**. By default, **Local camera** is selected.



NOTE

When **Monitor video** is enabled, the video delivered from the camera under control is displayed in the upper left corner of the **Video Control** page. You can then view the camera output while you control the camera.

- Step 3** Click the controls shown in [Figure 5-2](#) to control cameras.

----End

When the desired video is displayed on the monitor, you can save the camera settings as a preset so you can easily switch to the preset in the future. For details about how to set a camera preset, see [5.3 Setting a Camera Preset](#).

5.3 Setting a Camera Preset

Camera presets are camera positions you set and save ahead of time. A camera preset stores the pan, tilt, and zoom settings of the camera. You can easily control the camera by switching between camera presets. You can configure remote camera presets before and during conferences.

Prerequisites

You are familiar with how to control a camera. For details, see [5.2 Controlling a Camera](#).

Background

Table 5-1 lists the camera preset details.

Table 5-1 Camera preset details

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

Saving a Camera Preset

Step 1 Choose **Device Control > Device Control** and click the **Video Control** tab.

On the displayed **Video Control** page, the camera control area is on the right side.

Step 2 Adjust the camera pan, tilt, and zoom settings until the desired video is displayed on the monitor. Refer to [5.2 Controlling a Camera](#).

Step 3 Click the **Save Preset** tab, as shown in [Figure 5-3](#).

Figure 5-3 Setting a Camera Presets



Step 4 Select a number and click **Confirm**.

- **1**: indicates that the number has not been set for a preset. After you select this number and confirm the selection, the number is used for the current preset.
- **1** (with person icon): indicates that the number has been set for a preset. After you select this number and confirm the selection, the current preset will overwrite the original preset.

----End

Switching Between Camera Presets

Step 1 On the **Video Control** page, click **Switch Preset**.

Step 2 Under **Switch Preset**, select a number corresponding to a preset, and click **Confirm**.

----End

Removing a Camera Preset

Step 1 On the **Video Control** page, click **Save Preset** tab.

Step 2 Under **Save Preset**, select the number corresponding to the preset you want to remove, and click **Clear**.

----End

5.4 Selecting Video Sources

The endpoint provides multiple video input ports for connecting to video devices. When multiple video devices are connected, you can set one video device as the local video source and another one as the local presentation source. You can also select the video or presentation to be displayed through video output ports.

Prerequisites

To set the computer desktop as a video input source, ensure that you have set the computer video to a video resolution and refresh rate that your endpoint supports. For details, see [7.3.5 Configuring Video Output](#).

Background

- Selecting video input sources

A video device can be a document camera, computer, record and playback device, or DVD player. If you have connected multiple video devices to the input ports on your endpoint, select local video and presentation sources from these connected devices.

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.

For details about how to set video input ports, see [7.3.2 Configuring Video Input](#).

- Selecting video output sources

During a conference, you can manually switch between the local video, local presentation, remote video, and remote presentation to be displayed through a video output port.

For details about how to set video output ports, see [7.3.5 Configuring Video Output](#).

Selecting the Video Source and Presentation Source

Step 1 Choose **Device Control > Device Control** and click the **Video Control** tab.

Step 2 In the lower left corner of the **Video Control** page, click the **Video Input Source** tab.

Step 3 Set **Video Source** and **Presentation Source**.

You can set the local video source to multi-view mode. For details about multi-view mode settings, see [7.3.3 Setting the Multi-View Mode](#).

----End

Selecting the Video Output Source

Step 1 Choose **Device Control > Device Control** and click the **Video Control** tab.

Step 2 In the lower right corner of the **Video Control** page, click the **Video Output Source** tab.

Step 3 Select the video or presentation to be displayed through video output ports.

----End

5.5 Controlling Audio

On your endpoint, you can adjust the audio effects. For example, you can adjust the volume of the microphone and speaker.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Audio Control** tab.

Step 2 Set the audio control parameters listed in [Table 5-2](#).

Table 5-2 Audio control parameters

Parameter	Description	Setting
Audio Input		
Audio Input	Turns on or off all audio input sources.	The default value is Unmute .
MIC 1 MIC 2 (only TE60)	Adjusts the microphone volume at your site. When you adjust this microphone volume, the volume heard at remote sites is adjusted accordingly.	The default value is +0dB . Value range: -12 dB to +12 dB
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	The default value is +0dB . Value range: -12 dB to +12 dB

Parameter	Description	Setting
	remote sites is adjusted accordingly.	
HDMI L HDMI R	Adjusts the input volume of the HDML 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 the HDMI port of the endpoint is connected to an input source.	The default value is +0dB . Value range: -12 dB to +12 dB
DP L (only TE60) DP R (only TE60)	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 the DP port of the endpoint is connected to an input source.	The default value is +0dB . Value range: -12 dB to +12 dB
LINE IN L (only TE50) LINE IN R (only 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.	The default value is +0dB . Value range: -12 dB to +12 dB
Microphone array 1 MIC array 1 battery level Microphone array 2 MIC array 2 battery level Microphone array 3(only TE60) MIC array 3 battery level(only TE60)	Displays the microphone array volumes and battery levels in real time.	-
Audio Output		
Speaker	Mutes or unmutes the speaker at your site. To hear other sites, unmute the speaker.	The default value is Unmute .
Volume	Adjusts the output volume heard at your site. If both left and right audio channels are available, the volume of both channels is adjusted at the same time.	The default value is 15 . Value range: 0-21
Alert tone	Increases or decreases the alert tone	The default value is 3 .

Parameter	Description	Setting
volume	volume.	Value range: 0-3
Sound Effect		
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.	The default value is Mute .
AUDIOIN 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.	The default value is Unmute .
SPDIF	Specifies whether you can hear the sound from the local SPDIF digital audio port at your site. To hear the sound, set this parameter to Unmute .	The default value is Mute .
AUDIO IN echo cancellation	If echo cancellation is enabled, the endpoint removes echo in the audio input from the MIC 1 and MIC 2 (only TE60) interfaces.	The default value is Mute .
Music Mode	Specifies whether to enable the MIC 1 and MIC 2 (only TE60) to pick up the music that is playing at the local site to provide a better listening experience.	The default value is Mute .
Bass Middle Treble	Adjusts the gain of bass, middle, and treble tones.	The default value is +0dB . Value range: -6 dB to +6 dB
PSTN		
PSTN	Adjusts the volume of a PSTN call at your site. When you adjust this volume, the volume heard at remote sites is adjusted accordingly.	The default value is +0dB . Value range: -12 dB to +12 dB
Mix PSTN audio	Specifies whether all sites (including PSTN sites such as mobile phones) in a conference can hear each other.	The default value is Enable . If you retain the default value, all sites in a conference can hear each other. Retain the default value when your endpoint joins a multipoint conference as a PSTN site.

----End

5.6 Setting the Combined Picture

With the combined picture function, you can view multiple videos (such as the local and remote videos and presentations) in Picture in Picture (PiP) or split-screen mode on one display.

Prerequisites

Two or more of the following video sources are available: local video, local presentation, remote video, and remote presentation.

Background

You can view multiple videos on one display at the same time. The positions, sizes, and combination of these images are configurable.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Combined Picture** tab.

Step 2 Click **Switch Video**.

Videos are displayed in the mode you select.

----End

5.7 Setting Camera Parameters

On your endpoint, you can set the camera parameters, including video mode, noise reduction, and video resolution. You can view the video result of your settings on the display connected to your endpoint.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Camera parameters adjustment** tab.

Step 2 Set the camera parameters listed in [Table 5-3](#).

Table 5-3 Camera parameters

Parameter	Description	Setting
Camera input interface	Specifies the endpoint's video input port to which the camera is to be connected.	The default value is 1 MAIN IN .
Exposure mode	Specifies the mode for using natural light. You can select either of the following modes: Auto: The camera automatically selects the optimum configuration based on the surrounding	The default value is Auto .

Parameter	Description	Setting
	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.	
White balance	Specifies the white balance to enable the camera to accurately recognize the color white and deliver more vivid videos. • Auto: The camera automatically calculates and outputs the value using color information from the entire screen. • One-push: This is a fixed white balance mode. Once you select this mode, the value is automatically adjusted. This mode assumes that the camera shoots a white subject occupying more than 1/2 of the image, under correct light conditions. The mode is lost when the endpoint is powered off. You have to reset this mode after the endpoint is powered on. • Manual: This is a manual white balance mode. You automatically control the red gain and blue gain that range from -128 to 127.	The default value is Auto .
Picture mode	Specifies the output video display effect. • Standard: reproduces video more faithfully. • Vivid: delivers brighter video with cooler colors. • Natural: delivers video with warmer colors. • User defined: delivers video with custom settings. After you select this option, you can set the following parameters. – Aperture: sharpens video edges and contours to preserve the impression of clarity and fine	The default value is Standard .

Parameter	Description	Setting
	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 grayscale of each color. The higher the saturation, the brighter a color.	
Noise reduction	Removes noise artifacts from video. A larger value causes the video to have less noise but detail may also be lost.	The default value is Low .
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

5.8 Setting Preferred Video Parameters

If you find that the displayed video deviates from its normal position, adjust the picture offset.
If a blurring or slight jitter issue occurs in the video, adjust the sampling phase.

Background

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

A blurring or slight jitter issue may occur in the video displayed on the display device. In this case, you can set the sampling phase to adjust the color.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Preference–Video** tab.

Step 2 Adjust the video parameters described in [Table 5-4](#).

Table 5-4 Video parameters

Parameter	Setting
Image Offset	Select Horizontal offset or Vertical offset and drag the slider to adjust the image offset on the video input and output ports.
Sampling Phase	Drag the slider to adjust the sampling phase for the video input port.
Small window position offset	Drag the slider to adjust the offset for the Picture in Picture (PiP) window.
Output Adjustment	Drag the slider to adjust the size of the output video. If your monitor specifications are low, and the video output from the endpoint does not display properly, set this parameter to fix the display issue. Before setting this parameter, make sure: • The endpoint is connected to the monitor using a standard cable. • The Extended Display Identification Data (EDID) from the monitor can be correctly read by the endpoint.
Adjust presentation resolution	Drag the slider to adjust the resolution of the presentation. Dragging the slider left blurs the presentation, and dragging the slider right sharpens it.

----End

5.9 Setting Up a PPPoE Dial-Up Connection

Correct IP parameter settings on your endpoint enable you to set up a PPPoE dial-up connection with a broadband network to communicate with other network devices.

Prerequisites

- You have set **PPPoE** to **Enable**.
- You have entered the user name and password that are provided by your broadband access service provider in **User name** and **Password** respectively.
- You have set **Dialing mode** to **Manual**.



NOTE

If **Dialing mode** is set to **Disable**, the endpoint automatically sets up a PPPoE dial-up connection.

Procedure

Step 1 Choose **Device Control > PPPoE Dialing**.

The **PPPoE Dialing** page is displayed.

Step 2 Click **Dial**.



NOTE

To cancel a PPPoE dial-up connection, set **PPPoE** to **Disable**.

----**End**

Follow-up Procedure

When a PPPoE dial-up connection is set up, your endpoint has a new IP address. Use this IP address the next time you want to log in to the endpoint web interface.

To obtain your endpoint IP address, access the home screen of the user interface controlled by the remote control and choose **Advanced > Settings > Network > IP > Local IP address**.

5.10 Using the Remote Control

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

Choose **Device Control > Use Remote Control** and click the desired button on the virtual remote control.

6 Managing the Local Address Book

About This Chapter

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.

6.1 Editing the Local Address Book

From the address book page, you can add a site or group, search for and sort the sites.

6.2 Using Virtual Conference Rooms

From a standalone MCU, the administrator can reserve conference resources, schedule a conference without predefined sites, and assign the conference a number (the virtual conference room number).

6.3 Importing and Exporting Address Book

From the endpoint web interface, you can export the local address book to the local computer or a server. You can also import the modified address book to the endpoint, after which the records in the address book are displayed on the address book page.

6.4 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.

6.1 Editing the Local Address Book

From the address book page, you can add a site or group, search for and sort the sites.

Adding a Site

Step 1 Choose **Address Book > Address Book**.

Step 2 Click **Add Site** and set the site parameters listed in [Table 6-1](#).

Table 6-1 Site parameters

Parameter	Description	Setting
-----------	-------------	---------

Parameter	Description	Setting
Name	Specifies the name of the site. This site name is superimposed on the site video.	The value can contain a maximum of 64 characters, including digits, letters, and special characters.
Category	Specifies the conferencing scenario of the site. • Ordinary site: Select this option for a traditional videoconferencing site. • Telepresence site: Select this option for a Huawei three-screen telepresence site. • CT site: Select this option for a Cisco TelePresence site.	The default value is Ordinary site .
Type	Specifies the type of the line the site uses to access the videoconferencing network. • If you select IP, your endpoint will use the protocol set for Preferred IP protocol to call the site. • If you set Category to CT site, the available value for Type is SIP.	The default value is H.323 .
Rate	Specifies the data transmission rate of the line selected for the remote endpoint. The supported data transmission rates vary depending on the type of the site you want to call.	Select the highest available data transmission rate.
Country/Region code	Specifies the country or area where the site is located. This parameter is available only for integrated services digital network (ISDN) and public switched telephone network (PSTN) sites.	No default value is set for this parameter.
Area code	Specifies the area code for the site. This parameter is available only for ISDN and PSTN sites.	No default value is set for this parameter.
Number	Specifies the site number used to place calls between sites. • IP, E1, 4E1, ISDN, 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 IP address of the site. NOTE This parameter is unavailable if you set	No default value is set for this parameter.

Parameter	Description	Setting
	Category to CT site.	
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.
Line 1 #1 Line 1 #2 Line 2 #1 Line 2 #2 Line 3 #1 Line 3 #2	Specify the numbers your endpoint uses to call the site. These parameters are available only for ISDN sites. - If the ISDN site rate is set to a value ranging from 64 kbit/s to 2048 kbit/s, set Line 1 #1 only, because you only need to dial that number to call the site. - If the ISDN site rate is set to 2, 3, 4, 5, or 6 x 64 kbit/s, set the other required parameters as well, because you need to dial the BRI line numbers one by one to call the site. For example, when the ISDN site rate is set to 2 x 64 kbit/s, set the first two parameters Line 1 #1 and Line 1 #2; when the ISDN site rate is set to 3 x 64 kbit/s, set the first three parameters Line 1 #1, Line 1 #2, and Line 2 #1, and so forth. Line 1 #2 specifies the second number of the first BRI line.	No default value is set for this parameter.
Sort ID	Specifies the sequence number of the site in the address book.	The default value is 0 .

Step 3 Click **Save**.

The settings take effect immediately. The new site is listed in the address book.

----End

Adding a Group

Step 1 Choose **Address Book > Address Book**.

Step 2 Click **Add Group**. In **Name**, enter the group name.

Step 3 Select one or more sites and click .

The selected sites are displayed under **Group Members**.



NOTE

To delete a site listed in **Group Members**, select the site and click  To delete all sites, click



Step 4 Click **Save**.

The new group is listed in the address book.

----End

Managing Address Records

- Searching for Records

In the search box, enter key words for an address and click .

- Modifying Records

Click the name of a site or group in the address book. On the displayed editing page, modify the settings for the site or group.

- Deleting Records

Select the site or group you want to delete and click **Delete**.

- Sorting Records

If there are multiple sites on the address book page, conference-related pages, or other pages, you can sort the sites based on their properties, such as by name, number, line type, online status, and type.

From the site lists on some of these pages, you can click one of five letter ranges,

A-E F-J K-O P-T U-Z

, to display the sites whose names start with letters within that range.

6.2 Using Virtual Conference Rooms

From a standalone MCU, the administrator can reserve conference resources, schedule a conference without predefined sites, and assign the conference a number (the virtual conference room number).

Background

The virtual conference room function simplifies the process of initiating multipoint conferences from the endpoint in the following aspects:

- A virtual conference room can be configured with an easy-to-remember access number for sites to dial to join the conference.
- From the **Virtual Conference Room** page, users can search for virtual conference room entries and call a virtual conference room found or save the record to the endpoint.

Procedure

Step 1 Choose **Address Book > Address Book** and click the **Virtual Conference Room** tab.

Step 2 Perform any of the following operations:

- Select the virtual conference you want to delete and click **Delete**.
- Select the virtual conference you want to call and click **Call**.
- In the search box, enter key words for virtual conferences and click . The virtual conferences that meet the search criteria in the local address book are displayed.
- Click **Search for LDAP Address Book** in the lower right corner to search the LDAP address book for virtual conferences.

----End

6.3 Importing and Exporting Address Book

From the endpoint web interface, you can export the local address book to the local computer or a server. You can also import the 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.

When exporting the address book, you can specify the character encoding format to either of the following:

- China: The character set is GB2312.
- Other countries: The character set is UTF-8.

Procedure

Step 1 Choose **Address Book > Address Book**.

Step 2 Perform either of the following:

- To import new entries to the local address book, click **Import to Local Address Book**.
- To export the local address book, click **Export from Local Address Book**.

----End

6.4 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 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 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 Choose **Address Book > Site Template**.

Step 2 Select the site template you want to delete.

Step 3 Click **Delete**.

----End

7 System Settings

About This Chapter

After the configuration wizard is complete, you can use the endpoint to initiate simple conferences. You can also set advanced parameters for the endpoint on the endpoint web interface based on your video and audio conference requirements.



NOTE

The **System Settings** page is available only to the web interface administrator of the endpoint.

7.1 Setting Basic Parameters

Set basic parameters for the endpoint on the endpoint web interface, such as the system time and functions of number keys on the remote control.

7.2 Specifying Caption Settings

Caption settings include the banner or caption type, position, size, background, and color.

7.3 Setting Video Parameters

You can set video input and output parameters on the endpoint web interface and set the multi-view mode to achieve the desired video effect.

7.4 Configuring Audio

After connecting audio cables, set the audio parameters.

7.5 Specifying Conference Settings

Your endpoint is ready for videoconferencing with its default conference settings, but you can customize the conference settings based on the site requirements.

7.6 Specifying Network Settings

The endpoint can communicate with other devices properly only after network settings are specified on the endpoint web interface based on the network deployment of the endpoint.

7.7 Security

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

7.8 Importing Security Certificates

Import certificates on the endpoint web interface to improve the communication security.

7.9 Managing System Files

Manage system files on the endpoint interface to improve the operation and maintenance (O&M) efficiency of the endpoint.

7.1 Setting Basic Parameters

Set basic parameters for the endpoint on the endpoint web interface, such as the system time and functions of number keys on the remote control.

7.1.1 Setting the System time

You must correctly set the system time of the endpoint for services to run properly.

Step 1 Choose **System Settings > General**.

Step 2 Click the **Time and Time Zone** tab and set the parameters listed in [Table 7-1](#).

Table 7-1 Time and time zone parameters

Parameter	Description	Setting
Location	Specifies the country or area where your endpoint is located. When you set this parameter, your endpoint automatically adjusts the value of the Time zone parameter.	The default value is China .
Time zone	Specifies the time difference between the local time and the Greenwich Mean Time (GMT).	The default value is (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi . Your endpoint automatically sets this parameter based on the value set for Location .
Time format	Specifies the format in which time is displayed.	The default value is 24-hour .
Adjust time automatically based on DST	Specifies whether to automatically adjust the endpoint clock time to daylight saving time (DST). When the DST is enabled, the endpoint clock is adjusted 1 hour forward. NOTE The presence of this parameter is controlled by your settings of Time zone . This parameter is available for countries and regions that support DST.	The default value is Disable .
Date format	Specifies the format in which the date is displayed.	The default value is YYYY/MM/DD .
Enable NTP	Specifies whether to automatically synchronizes system time with a	The default value is Disable .

Parameter	Description	Setting
	Network Time Protocol (NTP) server at an interval of 300 seconds. NOTE If you set this parameter to Enable NTP, you must also set NTP server address .	
NTP address type	Specifies the mode for your endpoint to obtain the NTP server IP address. • Auto: Your endpoint automatically obtains the NTP server IP address. • Manual: You must manually set the NTP server IP address. This parameter is available only when Connection type is set to Dynamic IP . NOTE For details about how to set Connection type , see 7.6.1 Setting IP Parameters .	The default value is Manual .
NTP server address	Specifies the NTP server IP address.	No default value is set for this parameter.
System time	Specifies the time set on the system.	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 Click **Save**.

The settings take effect immediately.

----End

7.1.2 Setting the Ringtone for Incoming Calls

When an incoming call arrives, the endpoint rings. You can set the desired ringtone.

Choose **System Settings > General > Ringtone** and select the desired ringtone.

7.1.3 Managing Power

The endpoint supports the sleep function to reduce power consumption. You can set the sleep time so that the endpoint automatically enters sleep mode when it is idle for the specified period of time. You can also set the scheduled power-on and power-off time.

Step 1 Choose **System Settings > General**.

Step 2 Click the **Power management** tab and set the parameters listed in [Table 7-2](#).

Table 7-2 Basic parameters

Parameter	Description	Setting
Power management		
Shut Down	Specifies whether the endpoint can be powered off. If you set this parameter to Disable , you can only restart the endpoint or place it in sleep mode from Device Control > Shut Down .	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 .
Scheduled power-on	Specifies whether the endpoint automatically powers on at the specified time. NOTE If you enable this function, you must also set Scheduled power-on time (hh:mm) .	The default value is Disable .
Scheduled power-on time (hh:mm)	Specifies the time when the endpoint automatically powers on. The value format depends on the value set for Time format .	The default value is 0:0 , which corresponds to the 24-hour value for Time format .
Scheduled power-off	Specifies whether the endpoint automatically powers off at the specified time. NOTE If you enable this function, you must also set Scheduled power-off time (hh:mm) .	The default value is Disable .
Scheduled power-off time (hh:mm)	Specifies the time when the endpoint automatically powers off. The value format depends on the value set for Time format .	The default value is 0:0 , which corresponds to the 24-hour value for Time format .
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 can be turned off by pressing the power key on the remote control.	The default value is Disable .
Control TV sleep mode	Specifies whether you can turn on or off the display connected to the endpoint. If	The default value is Disable .

Parameter	Description	Setting
	you enable this function and choose Device Control > Shut Down, the display will be turned off. This parameter is available only when Shut Down is set to Disable. NOTE If you enable this function, you must also set Serial port 1-connected TV model and Serial port 2-connected TV model.	
Serial port 1-connected TV model Serial port 2-connected TV model	Specify the types of displays connected to the COM1 and COM2 ports at the back of the endpoint.	The default value is TCL . Set the parameters according to the displays connected to the COM1 and COM2 ports at the back of the endpoint.

Step 3 Click **Save**.

The settings take effect immediately.

----**End**

7.1.4 Setting Number Key Functions

You can set the number keys on the remote control to facilitate your daily use of the endpoint.

To set the number keys choose **System Settings** > **General** > **Select number key function**.

- 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.
- When the endpoint is in a conference, you can select either of the following options:
 - **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.



NOTE

To toggle between these two options, press  on the remote control for 3 seconds or more.

7.2 Specifying Caption Settings

Caption settings include the banner or caption type, position, size, background, and color.

Background

Your endpoint supports T.140 and non-T.140 captions. [Table 7-3](#) describes the differences between these caption types.

Table 7-3 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: • Endpoint used at the chair site • SMC2.0 • Endpoint used by either party during a point-to-point call

Procedure

Step 1 Choose **System Settings > Display** and click the **Caption** tab.

Step 2 Set the caption parameters listed in [Table 7-4](#).

Table 7-4 Caption parameters

Parameter	Description	Setting
Sharing mode	Specifies the type of the caption. For details about caption types, see Table 7-3 .	The default value is T.140 .
Font size	Specifies the font size for the banners and middle and bottom captions.	For middle and bottom captions, the default value is Medium . For banners, the default value is Largest .
Bold	Specifies whether the banners and middle and bottom captions is displayed in bold.	For middle and bottom captions, the default value is No . For banners, the default value is Yes .
Font Type	Specifies the font type of captions. Settings of this parameter take effect only when the language of the remote controlled UI is set to simplified Chinese.	The default value is Boldface .

Parameter	Description	Setting
	NOTE To set the language of the remote controlled UI, choose System Settings > Display > GUI .	
Height	Specifies the percentage of the banner or bottom caption height to the entire display.	The default value is 10% .
Transparency	Specifies the banners and middle and bottom captions transparency.	The default value is Half transparent .
Line spacing	Specifies the vertical spacing between lines of a middle caption.	The default value is Small .
Effect	Specifies the display effect for the banners and middle and bottom captions.	For middle captions, the default value is Scroll upward . For bottom captions, the default value is Scroll leftward . For banners, the default value is Center .
Scrolling speed	Specifies the scroll rate for middle and bottom captions.	The default value is Fast .
Background color	Specifies the background color of the banners and middle and bottom captions.	For middle and bottom captions, the default color is gray. For banners, the default color is red. Up to 64 colors are supported.
Font color	Specifies the foreground color of the banners and middle and bottom captions.	The default color is white. Up to 64 colors are supported.

Step 3 Click **Save**.

The settings take effect immediately.

----**End**

7.3 Setting Video Parameters

You can set video input and output parameters on the endpoint web interface and set the multi-view mode to achieve the desired video effect.

7.3.1 Understanding Video Input Capabilities

You must understand the video input capabilities of the endpoint to correctly set 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 7-5](#), [Table 7-6](#), and [Table 7-7](#) list the capabilities of the video input ports.

Table 7-5 Capabilities of the TE40'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	HD-VI	DVI(HW), HDMI(HW), and YPbPr(HW)	Camera PTZ	None
2 PC IN	2	VGA	VGA and YPbPr	Camera PTZ	The VGA and HDMI Port ports are mutually exclusive and cannot be used at the same time.
		HDMI	DVI and HDMI	Camera PTZ	

Table 7-6 Capabilities of the TE50'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	RCA	CVBS	Camera PTZ	The RCA 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	VGA	VGA and YPbPr	Camera PTZ	The VGA and HDMI Port ports are mutually exclusive and cannot be used at the same time.
		HDMI	DVI and HDMI	Camera PTZ	

Port Name on the UI	Port Number on the Rear Panel	Type	Receivable Input Format	Control	Description
3 3G-SDI IN	3	BNC	SDI	Camera PTZ	None

Table 7-7 Capabilities of the TE60'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 [5.4 Selecting Video Sources](#).

7.3.2 Configuring Video Input

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

Step 1 Choose **System Settings > Input/Output** and click the **Video Input** tab.

Step 2 Set the video input parameters listed in [Table 7-8](#).

Table 7-8 Video input parameters

Parameter	Description	Setting
Remote control	Specifies whether a remote site can control the local camera during a call.	The default value is Allow .
Video Source Management	Specifies whether you can select the video source and presentation source on the remote controlled UI.  Press the 2 3 key on the remote control to select the video source and presentation source only after you enable this parameter.	The default value is Do not allow . Selecting an incorrect video source may result in black screens. To avoid mistakenly selecting an incorrect video source, the default value is recommended here. If you need to change the video source, set this parameter to Allow . After changing the video source, reset this parameter to Do not allow .
Face tracking	Specifies whether the camera automatically adjusts directions and image sizes based on face recognition.	The default value is Allow . Retain the default value so the camera can automatically adjust directions and image sizes based on faces.
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.	Select the serial port that is being used. Otherwise, the camera cannot be controlled.

Parameter	Description	Setting
Moving speed	Specifies the movement and zoom speed for the camera at your site. • Select Slow for accurate positioning. • Select Fast for quick positioning. • Select Medium for medium paced positioning.	The default value is Medium .
Initial position	Specifies the position of the camera after startup. • Auto: The camera moves to its initial position after startup. • Preset 1: The camera moves to the preset after startup. NOTE Each camera preset stores the pan, tilt, and zoom settings of the camera. For how to set presets, see 5.3 Setting a Camera Preset.	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 reversed. • Normal: The input video will not be reversed. • Horizontal mirroring: 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.	The default value is Normal .
Input source	Specifies the input source format.	The default value is Auto .
Stretch mode	Specifies how your endpoint adjusts the input video based on the video encoding format. • 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 part 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 default value is No stretch. It is recommended that you set this parameter to Stretch.

Parameter	Description	Setting
	the screen.	
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 .

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.3.3 Setting the Multi-View Mode

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

Background

Your endpoint is able to combine two or more local inputs and share them over one channel with remote participants. The inputs can be videos captured by the camera or computer desktops. You can set the inputs before or during a conference, and the settings take effect immediately. The multi-view layout can be Picture in Picture (PiP), 2-pane, or 3-pane modes. In PiP mode, the PiP window can be in the upper left, upper right, lower left, or lower right corner. One input can be configured to show in one or more panes, but the input cannot be a remote video source.

Procedure

Step 1 Choose **Device Control > Device Control** and click the **Multi-View** tab.

Step 2 Set **Multi-view mode** for 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 Choose **Device Control > Device Control** and click the **Video Control** tab.

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

The multi-view is displayed as the conference video at the local site. If you are in a conference, the multi-view will be shared to remote sites.

----End

7.3.4 Understanding Video Output Capabilities

You must understand the video output capabilities of the endpoint to correctly set video output parameters.

The video output formats vary according to port types. The capabilities of video output ports and recommended configurations are described in [Table 7-9](#), [Table 7-10](#), and [Table 7-11](#).

Table 7-9 Specifications of video output ports on the TE40

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After the 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 the combined picture.
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 Dual-screen function is enabled, this port displays the local or remote presentation if a presentation source is connected to this port and displays Huawei logo or local video if no presentation source is connected to this port.
3 VGA OUT	3	VGA	VGA and YPbPr	By default, this port displays the local video.

Table 7-10 Specifications of video output ports on the TE50

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After the 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 the combined picture.
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 Dual-screen function is enabled, this port displays the local or remote presentation if a presentation source is connected to this port and displays Huawei logo or local video if no presentation source is connected to this port.
3 VGA OUT	3	VGA	VGA and YPbPr	By default, this port displays the local video.
4 3G-SDI OUT	4	BNC	SDI	By default, this port displays the local video.
5 SD OUT	5	RCA	CVBS	By default, this port displays the local video.

Table 7-11 Specifications of video output ports on the TE60

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After the Startup

Port Name on the UI	Port Number on the Rear Panel	Type	Output Format	Default Settings After the 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 the combined picture.
2 PC OUT	2	DVI-I	DVI, VGA, YPbPr, and HDMI	By default, this port functions as the auxiliary output port and is used to display the local video. When the Dual-screen function is enabled, this port displays the local or remote presentation if a presentation source is connected to this port and displays Huawei logo or local video 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 displays the local video. Connect a display to this port using a DVI-S-Video/VGA/CVBS cable.
3 DVR OUT	3	HDMI	DVI and HDMI	By default, this port displays the local video.
4 3G-SDI OUT	4	BNC	SDI	By default, this port displays the local video.

7.3.5 Configuring Video Output

After connecting video cables, set the video output parameters, such as output mode, resolution, refresh rate, and stretch mode. This will enable your endpoint to deliver a superior video experience.

Background

Video is clearer at a higher resolution. Select a video resolution that is supported by the display connected to your endpoint.

[Table 7-12](#), [Table 7-13](#), and [Table 7-14](#) lists the resolutions supported by the video output ports in each output mode.

Table 7-12 Available video resolutions in each output mode of TE40

Output Mode	Video Resolution
1 MAIN 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
2 HDMI 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
3 VGA 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

Table 7-13 Available video resolutions in each output mode of TE50

Output Mode	Video Resolution
1 MAIN 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
2 HDMI 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

Output Mode	Video Resolution
HDMI	720p, 1080i, and 1080p
3 VGA 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
4 3G-SDI OUT	
SDI	720p, 1080i, and 1080p
5 SD OUT	
CVBS	NTSC and PAL

Table 7-14 Available video resolutions in each output mode of TE60

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	
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

Output Mode	Video Resolution
4 3G-SDI OUT	
SDI	720p, 1080i, and 1080p

Video is smoother at a higher refresh rate. Select a video resolution that is supported by the display connected to your endpoint. [Table 7-15](#) lists the refresh rates available for each video resolution.

Table 7-15 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
720p	60, if the output mode is VGA 50 or 60, if the output mode is DVI, YPbPr, or HDMI
1080i	50 or 60
1080p	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 **System Settings > Input/Output** and click the **Video Output** tab.

Step 2 Set the video output parameters listed in [Table 7-16](#).

Table 7-16 Video output parameters

Parameter	Description	Setting
GUI	Specifies the video output port for the remote controlled UI. 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	The default value is 1 MAIN OUT .

Parameter	Description	Setting
	to a value different from the value of Main output interface .	
Caption output	Specifies the video output port for captions. NOTE This parameter takes effect only when the caption type is set to T.140.	The default value is 1 MAIN OUT .
Main output interface	Specifies the main output port. - When Dual-screen is set to Enable, this port is used to display the local or remote video. - When Dual-screen is set to Disable, this port is used to display the local or remote video, or local or remote presentation.	The default value is 1 MAIN OUT .
Auxiliary output port	Specifies the auxiliary output port for preferentially displaying presentation. - When Dual-screen is set to Enable, this port is used to display the local or remote presentation if a presentation source is plugged in and is used to display the local video or Huawei logo if no presentation source is plugged in. - When Dual-screen is set to Disable, this port is used to display the local video or presentation when the endpoint is not used in a conference, and is used to display the remote video or presentation when the endpoint is used in a conference.	The default value of TE60 is 2 PC OUT . The default value of TE40 or TE50 is 2 HDMI OUT . Do not set Main output interface and Auxiliary output port to the same output port.
Dual-screen	Specifies whether the endpoint displays the video and presentation on separate displays. If you set this parameter to Enable , you can set Show Huawei logo .	The default value is Disable . You can enable this function only when your endpoint is connected to two displays.
Show Huawei logo	Specifies whether to show the Huawei logo on the display connected to an auxiliary port when the endpoint is not used in a conference and does not have any presentation source plugged in.	The default value is Enable .
Name	Specifies the output port name to help you identify ports during a conference.	- The default value for the 1 MAIN OUT port is 1 MAIN OUT. - The default value for the 2 PC OUT port (only TE60) is

Parameter	Description	Setting
		2 PC OUT. - The default value for the 2 HDMI OUT port (only TE40 and TE50) is 2 HDMI OUT. - The default value for the 3 VGA OUT port (only TE40 and TE50) is 3 VGA OUT. - The default value for the 3 DVR OUT port (only TE60) is 3 DVR OUT. - The default value for the 4 3G-SDI OUT port (only TE50 and TE60) is 4 3G-SDI OUT. - The default value for the 5 SD OUT port (only TE50) is 5 SD OUT. - The default value for the 2 SD OUT port (only TE60) is 2 SD OUT.
Output mode	Specifies the format for the video received by the display. Output modes vary according to video output ports. For details, refer to Table 7-12, Table 7-13 and Table 7-14.	- The default value for the 1 MAIN OUT port is: DVI if the TE60 is used. HDMI if the TE40 or TE50 is used. - The default value for the 2 PC OUT port (only TE60) is DVI. - The default value for the 2 HDMI OUT port (only TE40 and TE50) is DVI. - The default value for the 2 SD OUT port (only TE60) is CVBS. - The default value for the 3 VGA OUT port (only TE40 and TE50) is VGA. - The default value for the 3 DVR OUT port (only TE60) is DVI. - The default value for the 4 3G-SDI OUT port (only TE50 and TE60) is SDI. - The default value for the 5 SD OUT port (only TE50) is CVBS.

Parameter	Description	Setting
		The default value for the 2 SD OUT port (only TE60) is CVBS.
Video resolution	Specifies the resolution for each video output port. The available options vary depending on your settings of Output mode . Table 7-12 , Table 7-13 and Table 7-14 lists the resolutions supported by the video output ports in each output mode.	- The default value for the 5 SD OUT port (only TE50) is NTSC. - The default value for the 2 SD OUT port (only TE60) 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 7-15 lists the refresh rates available for each video resolution.	The default value is 60Hz. NOTE After setting Video resolution and Refresh rate, adjust the sampling phase if the image is blurry or has a little jitter. For details, see 5.8 Setting Preferred Video Parameters.
Stretch mode	Specifies how to adjust the aspect ratio to fit the video into the screen. 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 the main output port of your endpoint displays the video and presentation during a conference. Full screen: When a presentation is not being shared, your endpoint displays the remote video in full screen. When a presentation is being shared, your endpoint displays the presentation in full screen. PiP: When a presentation is not being shared, your endpoint displays the local video and remote video in Picture in Picture (PiP) mode. When a presentation is being shared, your	The default value is Full screen .

Parameter	Description	Setting
	endpoint displays the presentation and video in PiP mode. • PoP: When a presentation is not being shared, your endpoint displays the local video and remote video in Picture out Picture (PoP) mode. When a presentation is being shared, your endpoint displays the presentation, remote video, and local video in PoP mode. • User defined: Users define the content to be displayed by the main output port based on the imported layout policy file.	
Small window position	Specifies the position of the PiP window on the screen. This parameter is available only when Automatic layout mode is set to PiP.	The default value is Lower right corner .
Display local video Display remote video Display presentation	Specifies the content to be display through a port. You can select these three parameters for all video output ports, except Main output interface and Auxiliary output port.	Select or deselect these three parameters based on your needs.
Automatic layout mode	Specifies how the auxiliary output port displays the video and presentation after the endpoint joins a conference. This parameter is available only when you have imported the layout policy file through the web interface and selected Dual-screen. • Default: The content displayed by the auxiliary output port depends on the setting of Dual-screen. – When Dual-screen is set to Enable, this port is used to display the local or remote presentation if a presentation source is plugged in and is used to display the local video or Huawei logo if no presentation source is plugged in. – When Dual-screen is set to Disable, this port is used to display the local video or presentation when the endpoint is not used in a conference, and is used to display the remote video	The default value is Default .

Parameter	Description	Setting
	or presentation when the endpoint is used in a conference. In this case, Automatic layout mode is unavailable on the web interface. • User defined: Users define the content to be displayed by the auxiliary output port based on the imported layout policy file.	

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.4 Configuring Audio

After connecting audio cables, set the audio parameters.

Procedure

Step 1 Choose **System Settings > Input/Output** and click the **Audio** tab.

Step 2 Set the audio parameters listed in [Table 7-17](#).

Table 7-17 Audio parameters

Parameter	Description	Setting
Switch controls	Controls whether audio signals collected by audio input devices, excluding the microphone array, are transmitted to your endpoint when you turn off the microphone array. • MIC array only: Your endpoint can receive audio signals collected by audio input devices, excluding the microphone array, when you turn off the microphone array. • All audio inputs: Your endpoint cannot receive audio signals collected by any audio input devices when you turn off the microphone array. To enable your endpoint to receive audio signals again, do any of the following: • Press the button on the microphone array to turn it on. • Press the microphone button on the remote control to turn on the	The default value is All audio inputs .

Parameter	Description	Setting
	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 > Settings > Audio > Audio Input and select the audio input ports you want to enable.	
Wireless MIC power saving mode	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. 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.	The default value is Enable .
LINE OUT mode	Specifies the LINE OUT mode. Main output interface: The LINE OUT port is used as the main audio output port and delivers the audio of remote sites. Auxiliary output port: The LINE OUT port is used as the auxiliary audio output port and delivers the audio at your site as well as the audio at remote sites.	The default value is Main output interface .
Secondary dial tone	Enables or disables tone prompts for secondary dials.	The default value is Disable .
Echo delay	Adjusts the echo delay to eliminate echos caused by delay in audio output during conferences.	The default value is 0 .

Step 3 Click **Save**.

The settings take effect immediately.

----**End**

7.5 Specifying Conference Settings

Your endpoint is ready for videoconferencing with its default conference settings, but you can customize the conference settings based on the site requirements.

7.5.1 Setting Audio and Video Protocols

Your endpoint supports multiple audio and video protocols. Select the protocols required for call purposes.

Background

Using the audio or video protocol that you select, your endpoint negotiates the audio or video capability with a remote endpoint to set up a call.

If you do not select any audio or video protocols on the **Audio and video protocols** tab, you cannot set audio or video protocols while you are [7.5.3 Setting Advanced Conference Parameters](#).

Procedure

Step 1 Choose **System Settings > Conference** and click the **Audio and video protocols** tab.

Step 2 Select audio and video protocols.



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.
- Select **RTV** and **H.264 UC** when your endpoint interoperates with a Lync device.

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.5.2 Setting General Conference Parameters

You can set the modes in which the endpoint places and answers calls. For example, you can set the endpoint to automatically answer calls, enable the do not disturb function, or set the multipoint call mode.

Background

General 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 the call from a remote site

Procedure

Step 1 Choose **System Settings > Conference** and click the **Normal** tab.

Step 2 Set the general conference parameters listed in [Table 7-18](#).

Table 7-18 General conference parameters

Parameter	Description	Setting
Answer Mode	Specifies how your endpoint handles incoming calls. 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	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. This parameter is available only when Answer Mode is set to Answer call automatically.	The default value is Disable .
Open do not disturb right	Specifies whether the do-not-disturb function is configurable on the remote controlled UI. The do-not-disturb function blocks all incoming calls.	The default value is Yes .
Site called during startup	Specifies the site that your endpoint automatically calls when it starts. You can proceed to set Call times only after you set this parameter.	The default value is None. The available options are entries in the contacts list.
Call times	Specifies the maximum number of attempts your endpoint calls a specified site after startup. If you set this parameter to 0, your endpoint does not call the specified site after startup.	The default value is 1. The maximum value is 10.
Default call bandwidth	Specifies the default data transmission rate for your endpoint. NOTE If this parameter is set incorrectly, the video quality will be affected or the call might even fail to be set up.	The default value is 1920 kbps .
Maximum incoming call bandwidth	Specifies the maximum bandwidth allowed for receiving calls. The bandwidths used for placing and receiving calls cannot exceed this bandwidth. The settings of this bandwidth and the settings of Default call bandwidth are	The default value is 8 Mbps. The settings cannot exceed the bandwidth supported by the endpoint license.

Parameter	Description	Setting
	independent of each other.	
HELPDESK number	Specifies the help desk number, which is used during emergencies.	Obtain this number from the videoconferencing system administrator.
PSTN call	Specifies whether to support calls from PSTN sites. After you enable this parameter and the endpoint connects to a PSTN network, the endpoint can receive calls from PSTN sites.	The default value is Enable .
Call parameter configuration	Specifies whether you can set the call type and data transmission rate before initiating point-to-point calls.	The default value is Disable .
Wi-Fi network preferred	Specifies whether to prioritize a Wi-Fi network when both wireless and wired networks are available.	The default value is Disable .
Multipoint call mode	Specifies how your endpoint initiates a multipoint conference. AUTO: The endpoint auto-selects the initiation mode based on its system settings and capabilities. The built-in MCU is prioritized. Multipoint converge: The endpoint initiates a multipoint conference using SiteCall with a standalone MCU. Built-in MCU: The endpoint initiates a multipoint conference using its built-in MCU. This function requires the endpoint to have a built-in MCU. In addition, you need to set Default remote layout, Add presentation to continuous presence, and Add local video to continuous presence. OFF: The endpoint allows for two concurrent calls, which can be one audio call and one video call, or two audio-only calls. Selecting this option does not affect the use of the SiteCall function.	The default value is AUTO .
Default remote layout	Specifies the default view displayed to remote sites in a multipoint conference initiated by the endpoint's built-in MCU. If the view is in continuous presence, the number of panes is determined by the built-in MCU's capabilities and the	The default value is Voice activated, in panes .

Parameter	Description	Setting
	number of participant sites. The video feeds for the continuous presence panes are determined by the joining sequence of participant sites and your settings of this parameter. • Voice activated, full screen: The remote sites view, in full screen, the video of the site that generates the loudest volume. • Voice activated, in panes: The remote sites view continuous presence, with the main pane displaying the video of the site that generates the loudest volume. • Bisect: The remote sites view, in bisect mode, the videos of the other participant sites. The site that generates the louder volume is highlighted. A presentation will not be displayed in this layout. • Fixed site, full screen: The remote sites view, in full screen, the video of a specified site. To view a site in full screen, click it in the site list. • Fixed sites, in panes: The remote sites view continuous presence, with the main pane displaying the video of a specified site. To add a participant site to the main pane, click it in the site list. NOTE After you set this parameter, the local site views other sites in full screen or continuous presence mode, but cannot view itself.	
Add presentation to continuous presence	Specifies whether the shared presentation is displayed in continuous presence during a multipoint conference initiated by the endpoint's built-in MCU. If the continuous presence layout is Bisect, the presentation will not be displayed in continuous presence. NOTE The settings of this parameter do not take effect at H.323 sites where the endpoints in V100R001C10 are used.	The default value is Disable .
Add local video to continuous presence	Specifies whether a site's local video is displayed in the site's continuous presence view during a multipoint conference initiated by the endpoint's	The default value is Disable .

Parameter	Description	Setting
	built-in MCU. NOTE The settings of this parameter do not take effect at H.323 sites where the endpoints in V100R001C10 are used.	
Continuous presence pane display mode	Specifies the display mode for the panes in continuous presence. • Stretch: The video in a pane has its aspect ratio automatically adjusted so it can fill the entire pane. • Tile: The video in a pane is repeated until it can fill the entire pane.	The default value is Stretch .
Voice Switching Sensitivity	Specifies the sensitivity for the voice activation function used in multipoint conferences. • High: Voice activation is performed when the voice volume is low. • Medium: Voice activation is performed when the voice volume is moderate. • Low: Voice activation is performed when the voice volume is high.	The default value is High .
Recording server address	Specifies the IP address or URL of the Recording & Streaming Engine (RSE). If the endpoint has been registered with an H.323 gatekeeper (GK), you can enter the H.323 number or unified recording number that the endpoint uses to register with the GK.	No default value is set for this parameter.

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.5.3 Setting Advanced Conference Parameters

Your endpoint allows you to configure advanced conference parameters before you initiate single-stream or dual-stream conferences.

Procedure

Step 1 Choose **System Settings > Conference** and click the **Advanced Settings** tab.

Step 2 Set the advanced conference parameters listed in [Table 7-19](#).

Table 7-19 Advanced conference parameters

Parameter	Description	Setting
Audio protocol	Specifies the audio protocol the 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, the 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 HP-related video protocol.
Video resolution	Specifies the video format. The available options vary depending on your settings of Video protocol . When Video protocol is set to Auto , set this parameter to either of the following: 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	Specifies the frame rate used during video encoding. When Video protocol is set to Auto , this parameter is not available. Video at a higher frame rate is smoother. Video at a lower frame rate is clearer.	It is recommended that you set this parameter to Auto .
Prevent little packet loss	Specifies whether to prevent sporadic packet loss to avoid artifacts.	The default value is Disable . Select this parameter if all endpoints are on the same private network and sporadic packet loss occurs.
Presentation	Specifies whether you can share presentations during conferences. NOTE You can set Presentation protocol , Presentation resolution , Presentation mode , Presentation bandwidth setting , Presentation bandwidth (%) ,	The default value is Enable .

Parameter	Description	Setting
	Presentation sharing mode , and Presentation plug-and-share only after you set this parameter to Enable .	
Presentation protocol	Specifies the video protocol your endpoint uses to encode presentations.	The default value is Auto .
Presentation resolution	Specifies the presentation format. The available options vary depending on your settings of Presentation protocol . When Presentation protocol is set to Auto , set this parameter to either of the following: • 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 mode	Specifies the mode of the presentation you want to share. • 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. NOTE When connected to an IMS network, the endpoint cannot share a presentation in Live mode.	The default value is Presentation .
Presentation bandwidth setting	Specifies the mode for setting the presentation video bandwidth. • Auto: Your endpoint automatically sets the presentation video bandwidth based on the bandwidth available. • Manual: You must manually set Presentation bandwidth (%).	The default value is Auto .
Presentation bandwidth	Specifies the percentage of the call bandwidth presentations can occupy. NOTE	The default value is 50 .

Parameter	Description	Setting
	This parameter is available only when Presentation is set to Enable and Presentation bandwidth setting is set to Manual .	
Presentation sharing mode	Specifies the mode for sharing presentations. 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  button or through the web interface. For details about how to share presentations through the web interface, see 4.7 Sharing a Presentation.	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 .
Dynamic bandwidth	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 packet loss is detected, the endpoint can dynamically adjust bandwidth to recover stable conference quality within 1 minute.	The default value is Disable. - When the network is running within normal parameters, select Disable. - When the network is not running within normal parameters, select Enable.
Conference bandwidth	Specifies the transmission bandwidth for a conference. If your endpoint accesses an E1 network through an IP line, set this parameter to Limited for better video conference quality.	The default value is Normal .
Conference line type	Specifies the type of line used during a conference. If you select Auto and your endpoint has registered with a network gatekeeper (GK), your endpoint	The default value is Auto .

Parameter	Description	Setting
	preferentially uses H.323 to initiate a conference.	
Preferred IP protocol	Specifies the protocol that IP sites preferentially use. When Line type is set to Auto for IP sites, your endpoint uses this protocol to call the IP sites.	The default value is H.323 .
reserved presentation bandwidth	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 -. If this parameter is disabled, the Received value for Presentation bandwidth [frame rate] restores to - when you rejoin the conference. NOTE To view the Presentation bandwidth [frame rate] value, choose Maintenance > System Status > Conference .	The default value is Enable .
Face detection	Specifies whether to perform HD encoding and decoding to improve face recognition video quality. You can increase the video sharpness by enabling this parameter in low bandwidths.	The default value is Disable .

Step 3 Click **Save**.

The settings take effect immediately.

---End

7.6 Specifying Network Settings

The endpoint can communicate with other devices properly only after network settings are specified on the endpoint web interface based on the network deployment of the endpoint.

7.6.1 Setting IP Parameters

To use the endpoint on an IP network to implement video communication, correctly set IP parameters, which include DNS server address, network interface mode, and gateway address.

Procedure

Step 1 Choose **System Settings > Network** and click the **IP** tab.

Step 2 Set the IP parameters listed in [Table 7-20](#).

Table 7-20 IP parameters

Parameter	Description	Setting
Common Settings		
Network interface mode	Specifies the working mode for the network ports on the endpoint. • 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 same time. • 1000Mbps and full duplex: The data transmission rate is 1000 Mbit/s, and data can be sent and received at the same time.	The default value is Auto detection. It is recommended that the parameter value be set to the same as the network port working mode of the remote network device. NOTE 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.
Hub network port mode	Specifies whether the endpoint can function as a hub in this mode, enabling the devices connected to its two network ports to communicate with each other. When the endpoint is connected to the Internet, devices connected to the network ports on the endpoint can also access the Internet.	The default value is Disable .
MTU	Specifies the maximum transmission unit (MTU) in bytes. If the MTU is too large, the network transmission rate may be slowed, resulting in packet transmission failures. If the MTU is too small, the	The default value is 1500 .

Parameter	Description	Setting
	network transmission efficiency may suffer.	
Local IP address		
PPPoE	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 User name Password	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. • 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 the network. For details about how to use PPPoE for dial-up connections, see 5.9 Setting Up a PPPoE Dial-Up Connection.	The default value of Dialing mode is Auto .
Connection type	Specifies the mode in which the endpoint obtains an IP address. • 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.	The default value is 192.168.1.1 Examples: • IPv4: 192.168.1.10 • IPv6:

Parameter	Description	Setting
		fc00:0:0:0:200:55:26:1
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.	The default value is 255.255.255.0
Gateway address	Specifies the gateway address that corresponds to the endpoint IP address.	Examples: - IPv4: 192.168.1.1 - IPv6: fc00:0:0:0:200:55:0:1
IPv6	Specifies whether IPv6 is used. If you use IPv6, you must also set Connection type , Local IP address , Subnet prefix length , and Gateway address .	The default value is Disable .
Subnet prefix length	Specifies the prefix length for the IPv6 address of the endpoint.	The default value is 0 . You need to set this parameter only when the IPv6 is enabled.
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.
DNS		
DNS address type	Specifies the mode for setting the DNS server address. Auto: The endpoint automatically obtains the DNS server address. If you select this option, a DNS server must be available on the network. Manual: You must set DNS server address 1, DNS server address 2, or DNS server address 3.	The default value is Auto .
DNS server address 1 DNS server address 2 DNS server address 3	Specifies the IP address of the active Domain Name System (DNS) server. After you set this parameter, domain names can be used as the addresses of network gatekeeper (GK) and Session Initiation Protocol (SIP) servers. The DNS server will translate the domain names into the IP addresses of the GK and SIP servers.	No default value is set for this parameter.
802.1x		
802.1x	Specifies whether to enable 802.1x authentication. If the network where your	The default value is Disable .

Parameter	Description	Setting
	endpoint is deployed requires authentication, set this parameter to Enable. NOTE If you set this parameter to Enable, you must also set Authentication mode.	
Authentication mode	Specifies the authentication mode, which can be certificate authentication or password authentication. Certificate: Use an imported certificate and the set Certificate account to initiate authentication to the authentication server. Password: Use the set user name and password to initiate authentication to the authentication server.	The default value is Password. NOTE If you select Certificate, obtain the certificate from the certificate server administrator first. For details about how to import a certificate, see 7.8.1 Importing a Certificate.
Certificate account	Specifies the ID that matches the certificate imported for certificate authentication.	The default value is administrator. Obtain the values from the authentication server administrator.
User name Password	Specify the user name and password for network authentication.	The default value of User name is admin. Obtain the values from the authentication server administrator.
802.1p/q		
802.1p/q	Specifies whether to enable 802.1p/q. If the switch has a virtual LAN (VLAN) set, enable 802.1p/q and set related parameters so the endpoint can access the switch and network interconnection can be implemented. NOTE If you set this parameter to Enable, you must also set VLAN ID and Priority.	The default value is Disable. NOTE The settings must be consistent with those on the switch. Otherwise, network interconnection may fail.
VLAN ID	Specifies the ID of the VLAN to which the endpoint needs to connect.	The default value is 1. Value range: 1-4094 Obtain the ID from the network administrator.
Priority	Specifies the priority of packets forwarded by the switch. The priority increases with the value.	The default value is 0. Value range: 0-7

Step 3 Click **Save**.

Log in to the endpoint web interface using the new IP address.

----End

7.6.2 Setting H.323 Parameters

To prepare your endpoint for video communication using the H.323, set H.323 parameters such as whether to use the network gatekeeper (GK).

Procedure

Step 1 Choose **System Settings > Network** and click the **H.323/SIP Settings** tab.

Step 2 Set the H.323 parameters listed in [Table 7-21](#).

Table 7-21 H.323 parameters

Parameter	Description	Setting
Enable GK	Specifies whether your endpoint uses a GK. • Enable: 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 site numbers if the remote sites also register with GKs. • Disable: 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. NOTE If you select Enable, you must also set GK registration mode, Site number, H.323 ID, and Password.	The default value is Disable. It is recommended that you set this parameter to Enable.
GK registration mode	Specifies the mode for registering your endpoint with a GK. • Auto: Your endpoint automatically registers with an available GK on the network and obtains the GK address. • Manual: You must set GK address, which specifies the GK with which you want your endpoint to register.	The default value is Auto. It is recommended that you set this parameter to Manual.
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	No default value is set for this parameter.

Parameter	Description	Setting
	the server.	
E.164	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.
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 @ # %. 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 System Settings > Security > Encryption , and set Encryption to Enable .	The name can consist of digits, letters, and special characters, such as @ # %. 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. For successful GK authentication, the password defined on your endpoint must be consistent with the password predefined on the GK.	No default value is set for this parameter.
Use VoIP gateway VoIP gateway address	Specifies whether your endpoint can place calls to the endpoints connected to the specified voice over IP (VoIP) gateway. If you set this parameter to Enable , you must also set VoIP gateway address .	The default value is Disable .
Huawei GK	Specifies whether your endpoint uses a Huawei GK. If the Huawei GK is disabled, some functions, such as Conference Control , are unavailable on your endpoint.	The default value is Enable . Disable this parameter if your endpoint needs to interwork with other manufacturers' devices.
HTTPS mode	Specifies whether to upload SiteCall conference information using HTTPS encryption. If this parameter is set to disabled, your endpoint will use the Transfer Control	The default value is Enable .

Parameter	Description	Setting
	Protocol (TCP) to upload SiteCall conference information, which may be insecure.	
Multipoint conference authentication	Specifies whether to authenticate the server during SiteCall.	The default value is Disable .

Step 3 Click **Save**.

----End

7.6.3 Setting SIP Parameters

To prepare your endpoint for video communication using Session Initiation Protocol (SIP), set and SIP parameters, such as whether to register the endpoint with a SIP server.

Procedure

Step 1 Choose **System Settings > Network** and click the **H.323/SIP Settings** tab.

Step 2 Set the SIP parameters listed in [Table 7-22](#).

Table 7-22 SIP parameters

Parameter	Description	Setting
Register with server	Specifies whether your endpoint registers with a SIP server. • Enable: An endpoint that registers with a SIP server can place calls to remote sites using their IP addresses or site numbers if the remote sites also register with SIP servers. • Disable: 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. NOTE If you set this parameter to Enable, you must also set Server address, Conference service number, Site number, User name, and Password.	The default value is Disable .
Server address	Specifies the IP address or domain name of the SIP server with which you want your endpoint to register. If you set this parameter to the SIP server domain name, enable the domain name	No default value is set for this parameter.

Parameter	Description	Setting
	server (DNS). If the DNS is not enabled, enable Proxy server .	
Conference service number	Specifies the conference service number for your endpoint to initiate conferences over an IP multimedia subsystem (IMS) network. Set this parameter to the conference service number obtained from the administrator of the IMS network.	No default value is set for this parameter.
Proxy server	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. NOTE If you set this parameter to Enable , you must also set Proxy server address , Site number , User name , and Password .	The default value is Disable . Set this parameter based on the actual SIP network environment.
Proxy server address	Specifies the address of the proxy server. If you set Server address to the SIP server domain name, set this parameter to the IP address bound to that domain name.	No default value is set for this parameter.
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.	No default value is set for this parameter. Enter a value containing any of the following: letters, digits, special characters such as @ # %.
User name	Specifies the user name for authentication registration.	No default value is set for this parameter. 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.	No default value is set for this parameter. Obtain the value of this parameter from the SIP server administrator.
Server type	Specifies the SIP server type. OCS: Select this option if your endpoint registers with the Microsoft	The default value is Standard .

Parameter	Description	Setting
	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.	
Transmission type	Specifies the protocol used for SIP signaling transmission. • 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 when your endpoint registers with a SIP server. For details, see 7.8.1 Importing a Certificate. Note that selecting this option may affect the call rate. If you select this parameter, you can set SSL version.	The default value is TLS . To improve communication security, select TLS .
SSL version	Specifies the encryption protocol used for SIP calls, including TLS 1.0 and SSL 3.0 .	The default value is TLS 1.0 .
Video request handling	Specifies how your endpoint handles video requests from a remote endpoint during a point-to-point SIP audio call or multipoint conference. • 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 3 Click **Save**.

----End

7.6.4 Setting Wi-Fi Parameters

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

Setting Wi-Fi Client Parameters

The endpoint can join a Wi-Fi network and hold video and audio conferences over the Wi-Fi network only after **Wi-Fi Client** is enabled.

Step 1 Choose **System Settings > Network** and click the **Wi-Fi Settings** tab.

Step 2 Set **Wi-Fi Client** to **Enable**.

Your endpoint automatically scans for available wireless routers and lists them in the **Select WLAN** list box.

If you need to set a static IP address for your endpoint, go to [Step 3](#). Otherwise, go to [Step 5](#).

Step 3 Set **Connection type**, network mode parameters listed in [Table 7-23](#).

Table 7-23 Network mode parameters

Parameter	Description	Setting
Connection type	Specifies the mode in which the endpoint obtains an IP address. - Static IP: The network administrator assigns an IP address to the endpoint. If you select this option, you must also set IP address, Subnet mask, and Gateway address. - 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.	The default value is Dynamic IP. Select Dynamic IP unless special network requirements are imposed.
IP address	Specifies the IP address for the endpoint to connect to a WLAN access point to implement communication.	No default value is set for this parameter. This IP address and the IP address of the WLAN access point must be on the same network segment. For example: if the IP address of the WLAN access point is 192.168.1.100 and its subnet mask is 255.255.255.0, you

Parameter	Description	Setting
		must set Local IP address to 192.168.1.X. X can be any integer ranging from 0 to 255 except 100.
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.	No default value is set for this parameter.
Gateway address	Specifies the gateway address that corresponds to the endpoint IP address.	No default value is set for this parameter.

Step 4 Click **Save**.

Step 5 Under **Select WLAN**, select the wireless router to connect to and click **Connect**.



NOTE

If the wireless router you want to connect to is not listed, select **Others**, click **Connect**, and manually add the router.

Step 6 When prompted, set the authentication parameters listed in [Table 7-24](#).

Table 7-24 Authentication parameters

Parameter	Setting
Common authentication mode	
Security Key or Password	Set this parameter if the authentication mode of the connected wireless router is set to WPA-PSK , WPA2-PSK , or WEP . Obtain the value from the wireless router administrator.
802.1x authentication mode	
EAP method	Consult the wireless router administrator about the detailed settings. The authentication mode can be certificate authentication or password authentication. If certificate authentication is used, import a wireless certificate (with the prefix of 802.1x) that matches the settings of Identity . For details about how to import a certificate, see 7.8.1 Importing a Certificate . If password authentication is used, set Identity and Password .
Phase 2 authentication	
CA certificate	
User certificate	
Identity	
Password	

Step 7 Click **OK**.

When your endpoint is connected to the wireless router, the status of the router is **connected**.

----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 **System Settings > Network** and click the **Wi-Fi Settings** tab.

Step 2 Set **Wi-Fi Hotspot** to **Enable**.

Step 3 Set **Settings**, network hotspot parameters listed in [Table 7-25](#).

Table 7-25 Wi-Fi hotspot parameters

Parameter	Description	Setting
SSID Number	Specifies the name of the Wi-Fi network to which your endpoint connects.	The default values for the TE40, TE50, and TE60 are TE40_wifi_ap , TE50_wifi_ap , and TE60_wifi_ap respectively. The value is a string of 1 to 32 characters, containing digits, letters, and special characters, such as @ # %.
Channel	Specifies the channel to transmit 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	Specifies the identity authentication mode used on the Wi-Fi network. Wi-Fi Protected Access (WPA) provides greater security than Wired Equivalent Privacy (WEP). OPEN: When you select this option, the values available for Encryption mode are NONE and WEP. SHARE: When you select this option, the value available for Encryption mode is WEP. WPA-PSK: When you select this option, the value available for Encryption mode are TKIP and AES. WPA2-PSK: When you select this option, the value available for Encryption mode are TKIP and AES.	The default value is WPA2-PSK . To ensure security, set this parameter 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	Specifies the encryption method used on	The default value is AES .

Parameter	Description	Setting
mode	the Wi-Fi network. The required key types vary depending on your settings for this parameter. If you set Encryption mode to NONE , the Wi-Fi network provided by your endpoint is open to everyone.	NOTE When the endpoint is connected to a VPM220W, you must set Encryption mode to AES .
Password	Specifies the password required when other devices connect to your endpoint.	Specifies the encryption method used on the Wi-Fi network. The required key types vary depending on your settings for this parameter. If you set Encryption mode to NONE , the Wi-Fi network provided by your endpoint is open to everyone.
IP address Subnet mask	Specify the IP address and subnet mask of your endpoint.	Examples: • IP address: 192.168.2.1 • Subnet mask: 255.255.255.0
Enable DHCP server.	Specifies whether your endpoint assigns IP addresses to devices connected to it. NOTE If you select this parameter, you must also set Start IP address and End IP address .	This parameter is selected by default.
Start IP address End IP address	Specify the IP address segment for devices connected to your endpoint.	Examples: • Start IP address: 192.168.2.10 • End IP address: 192.168.2.100
Enable VPM220W	Specifies whether the endpoint can connect to the the VPM220W. Enable this option when the endpoint connects to the VPM220W.	This parameter is selected by default.

Step 4 Click **Save**.

The settings take effect immediately. You can then check the MAC address, and IP address of the device connected to your endpoint.

----End

7.6.5 Setting SNMP Parameters

To enable the videoconferencing network management system to manage your endpoint, configure the Simple Network Management Protocol (SNMP) settings.

Background

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 and SIP.
- Queries endpoint status.
- Checks endpoint alarms.
- Backs up and restores endpoint settings.
- Upgrades the endpoint online.

Procedure

Step 1 Choose **System Settings > Network** and click the **SNMP Settings** tab.

Step 2 Set the SNMP parameters listed in [Table 7-26](#).

Table 7-26 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 .
SNMPv2	Specifies whether to use SNMPv2. If you set this parameter to Enable , you must set Get community name , Set community name , and Trap community name .	The default value is Disable . Using SNMPv2 may impose security risks. Please set this parameter with caution.
Get community name	Specifies the credential that the videoconferencing network management server uses to obtain endpoint settings.	The default value is Change_Public . This parameter contains 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.
Set community name	Specifies the credential that the videoconferencing network management server uses to specify endpoint settings.	The default value is Change_Private . This parameter contains 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.
Trap community	Specifies the credential that the endpoint uses to report alarms to the	The default value is

Parameter	Description	Setting
name	videoconferencing network management server.	Change_Me. This parameter contains 6 to 32 characters. In addition, it must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.
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 SHA . 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	Specify the encryption protocol and password that your endpoint uses to send	The default value of Encryption protocol is AES .

Parameter	Description	Setting
Encryption password	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 Trap version is set to v3 trap or v3 inform .	Set Encryption password to a string of 1 to 32 characters, which contains letters, digits, and special characters.
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. • Read and write: read and write • Read only: read-only	The default value is Read and write .
Authentication protocol Authentication password	Specify the authentication mode and password for connecting the videoconferencing network management system to your endpoint.	The default value of Authentication protocol is SHA . 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.	The default value of Encryption protocol is AES . Set Encryption password to a string of 48 characters or less, consisting of letters, digits, and special characters.

Step 3 Click **Save**.

The settings take effect immediately.

---End

7.6.6 Setting Network Address Book Parameters

With correct network address book settings on your endpoint, you can download site information from the network address book to your endpoint.

Background

The network address book stores address information of the sites in a videoconferencing system. You can use any of the following methods to find the site you want to call:

- Download the network address book from a File Transfer Protocol over SSL (FTPS) server to the local address book. Then search the local address book for the site.
- Search for the site on the directory server.



NOTE

The directory server stores site information. The endpoint can access the directory server using the Lightweight Directory Access Protocol (LDAP).

Procedure

Step 1 Choose **System Settings > Network** and click the **Network Address Book** tab.

Step 2 Set the network address book parameters listed in [Table 7-27](#).

Table 7-27 Network address book parameters

Parameter	Description	Setting
Network Address Book		
Enable network address book	Specifies whether to enable the network address book. If you set this parameter to Enable , you must also set the rest of the parameters described in this table.	The default value is Disable .
Mode	Specifies the mode for network address book download.	The default value is Passive .
Synchronize automatically	Specifies whether your endpoint automatically downloads records from the network address book to the local address book.	The default value is Disable .
FTPS	Specifies whether to use File Transfer Protocol over SSL (FTPS) to encrypt data through the Secure Sockets Layer (SSL) and ensure data integrity.	The default value is Enable .
Local records prevail if duplicates exist	Specifies whether records that already exist in the local address book remain unchanged during an address update from the network address book.	The default value is Disable .
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.	The default value is Enable .
Clear local	Specifies whether your endpoint	The default value is Disable .

Parameter	Description	Setting
records during update	automatically clears the local address book when the local address book is updated.	
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 of 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 get access to the network address book.	No default value is set for this parameter.
LDAP Server		
Server address	Specifies the IP address of the LDAP directory server.	No default value is set for this parameter.
Port	Specifies the port for connecting 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. Example: dc=zdtest,dc=com
Authentication type	Specifies the LDAP server authentication mode. 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 option, you must also set Domain name. Anonymous: 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.	The default value is Enable .
User name Password	Specifies the user name and password used for LDAP server authentication.	The default value of User name is admin . The value can consist of digits, letters, and special characters, such as @ # %.
Domain name	Specifies the domain name used for LDAP server authentication. This parameter is mandatory when Authentication type is set to Secured .	No default value is set for this parameter.

Parameter	Description	Setting
Synchronize automatically	Specifies whether your endpoint regularly updates the LDAP Address Book entries in the local address book. NOTE If you set this parameter to Enable , you must also set Automatic update interval and Local records prevail if duplicates exist .	The default value is Enable .
Automatic update interval	Specifies the interval for updating the LDAP Address Book entries in the local address book.	The default value is 24 h .
Local records prevail if duplicates exist	Specifies whether records that already exist in the local address book remain unchanged during an address update from the address book on the LDAP server.	The default value is Disable .

Step 3 Click **Save**.

----End

7.6.7 Setting Firewall Parameters

Correct firewall settings ensure the security of the video conferences held using your endpoint.

Background

With Network Address Translation (NAT) technology, a device on a local area network (LAN) is allocated a dedicated internal IP address and uses an external IP address to communicate with external devices. If your LAN uses NAT technology, set the IP address of the NAT wide area network (WAN) on your endpoint.

Procedure

Step 1 Choose **System Settings > Network** and click the **Firewall** tab.

Step 2 Set the firewall parameters listed in [Table 7-28](#).

Table 7-28 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	The default value is Enable .

Parameter	Description	Setting
	recognized as a private network endpoint, H.460 will be used for traversal between public and private networks.	
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.
SIP across public and private networks	Specifies whether the endpoint supports traversal between public and private networks when deployed on a Simple Internet Protocol (SIP) network.	The default value is Enable .
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 remote sites.	The default value is 5060 . Value range: 1-65534.
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.
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	Specifies the local SIP listening port when Transmission type is set to TLS .	NOTE For details about how to set Transmission type , see 7.6.3 Setting SIP Parameters .

Parameter	Description	Setting
port		
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 .	
Port settings	Specifies the port use. • 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.

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.6.8 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.

Background

You can use a network diagnostics tool to diagnose your endpoint only when the endpoint is not used in any conferences.

Procedure

Step 1 Choose **System Settings > Network** and click the **Network diagnostics** tab.

Step 2 Set the network diagnostics parameters listed in [Table 7-29](#).

Table 7-29 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 .
Diagnostics tool user name Diagnostics tool password	Specify the user name and password the network diagnostics tool uses for authentication when attempting to communicate with your endpoint.	The default value of Diagnostics tool user name is admin .
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 .

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.6.9 Setting QoS Parameters

Quality of service (QoS) settings determine the mode for processing IP data packets during a conference.

Procedure

Step 1 Choose **System Settings > Network** and click the **QoS** tab.

Step 2 Set the QoS parameters listed in [Table 7-30](#).

Table 7-30 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, and other issues. • 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.	The default value is Priority .
IP priority	Specifies the priority that a network device gives to forwarding the data packets sent by your endpoint. A larger value indicates a higher priority.	The default value is 5 . Value range: 0-7
Service type	Specifies how the data packets sent and received by your endpoint are processed on the network. • 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 amount 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.	The default value is Minimum delay .
DSCP audio DSCP video DSCP data DSCP signaling	Specify the service level of data packets sent by your endpoint during transmission. A larger value indicates a higher service level.	The default value is 32 . Value range: 0-63
Network jitter	Adjusts network jitter settings to address: • Labial synchronization problems during conferences • Choppy audio problems, by increasing	The default value is 0ms . Value range: 0 ms to 1000 ms

Parameter	Description	Setting
	the network jitter value.	
Lip sync.	Fine-tunes network jitter settings if a slight labial synchronization problem persists after the network jitter settings are adjusted.	The default value is 0ms . Value range: 0 ms to 300 ms

Step 3 Click **Save**.

The settings take effect immediately.

----End

7.6.10 Connecting to a 4E1 Network

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



NOTICE

- Do not connect outdoor cables directly to the endpoint. 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 TE60 has a 4E1 interface card installed, connect the endpoint 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.

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 TE60.

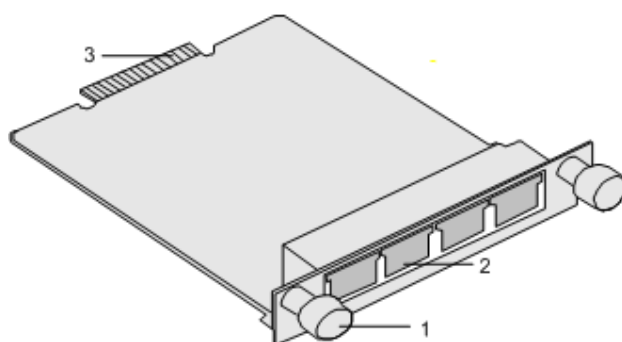


NOTICE

For safety reasons, insert the interface card only when the TE60 is powered off.

[Figure 7-1](#) shows the appearance of a 4E1 interface card, for your reference only.

Figure 7-1 4E1 interface card



1 Captive screw

2 4E1 port (RJ45)

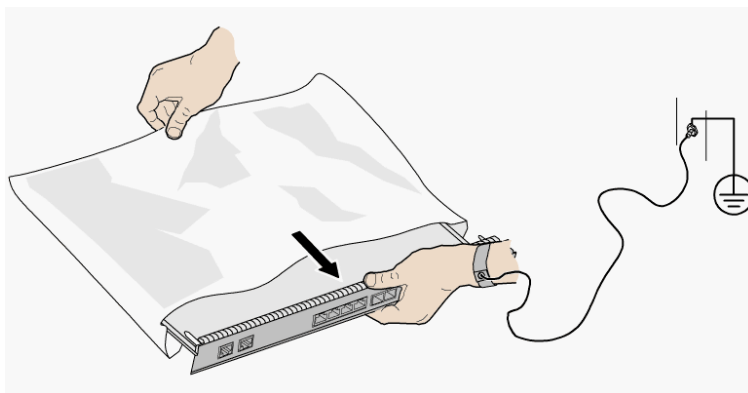
3 Edge connector



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 7-2](#).

Figure 7-2 Wearing an ESD wrist strap



Insert the interface card, as shown in [Figure 7-3](#).

Figure 7-3 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.

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 7-31](#).

Table 7-31 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.

Setting 4E1 Parameters

Only the TE60 supports 4E1 functions. If 4E1 lines are used for video communication, 4E1 parameters, such as the account, password, clock mode, signaling mode, and sensitivity, must be set. You are allowed to set 4E1 parameters only after a 4E1 interface card is inserted into the rear port on the TE60.

Procedure

- Step 1** Choose **System Settings** > **Network** and click the **4E1/E1** tab.

Step 2 Set the 4E1 parameters listed in [Table 7-32](#).

Table 7-32 4E1 parameters

Parameter	Description	Setting
Account Password	These are the account and password used by the endpoint when the endpoint initiates an H.323 conference.	For detailed information of the conference account and password, contact the administrator of the videoconferencing system.
Clock mode	The following clock modes are available: • Preferred clock: If this option is selected, the endpoint uses the internal clock and provides the clock to the remote device that is connected to the E1 interface of the endpoint. In a point-to-point call, Clock mode for either endpoint must be set to Preferred clock. • Alternate clock 1, Alternate clock 2, Alternate clock 3 and Alternate clock 4: If one of these options is selected, the endpoint obtains the clock from a line.	• If the endpoint is connected to an MCU, set the MCU clock as the master clock and the endpoint clock as the slave clock. • If the endpoint is connected to another endpoint, set the clock mode of one endpoint to the master clock and the clock mode of the other endpoint to the slave clock.
Signaling mode	Specifies the transmission mode for 4E1 signaling. Cyclic redundancy checking (CRC) is used to test the network condition. The CRC result indicates the frame error rate. When an option that contains CRC4 is selected, the endpoint tests the network for bit errors.	• To use channel associated signaling, you can select CAS. • To use common channel signaling, you can select CCS.
Sensitivity	Set this parameter based on the length of the 4E1 line used between the endpoint and the nearest network node, such as a switch.	• If the distance between the endpoint and the nearest network node is longer than 100 m, select Long line. • If the distance between the endpoint and the nearest network node is shorter than 100 m, select either Long line or Short line. Long line is recommended.

Step 3 Click **Save**.

----End

7.6.11 Connecting to a PSTN Network

To implement voice communication over a public switched telephone network (PSTN), you must connect the endpoint to the PSTN.

After being connected to the PSTN, the endpoint can place calls to PSTN phones.

To connect the endpoint to the PSTN, connect the PSTN port on the endpoint to the PSTN port installed by the carrier through a phone cable. After that, the endpoint can be used as a fixed-line phone while providing video conference functions.

The PSTN number of the endpoint is the fixed-line phone number assigned to the PSTN port installed by the carrier.

The application scenarios of connecting the endpoint to the PSTN are as follows:

- Use the endpoint as a fixed-line phone to place calls to mobile phones or other fixed-line phones.
- Invite a mobile phone or fixed-line phone user to a multipoint conference when the endpoint is in the conference.

PSTN phones can place calls to the endpoint connected to the PSTN directly by dialing the PSTN number of the endpoint.

By default, the endpoint allows for incoming PSTN calls. To view the related parameter settings, log in to the endpoint web interface, and choose **System Settings > Conference > Normal**.

By default, the endpoint has the PSTN audio input enabled. To view the setting of the **PSTN** parameter, log in to the endpoint web interface, and choose **Device Control > Device Control > Audio Control > PSTN**.

- Gain adjustment: You can move the slider to adjust the volume of PSTN calls.
- Sound mixing for PSTN sites: specifies whether all the sites (including PSTN sites, such as mobile phones) in a multipoint conference can hear each other. Enable this option when the endpoint joins a multipoint conference as a PSTN site.



NOTE

The endpoint comes with a PSTN port, which can be used in China only.

7.7 Security

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

7.7.1 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.
- Step 2** Set **Encryption** parameters.
- **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 3** Choose **Save**.
- End

7.7.2 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



NOTICE

This operation can be performed only on the remote controlled UI.

- Step 1** Choose **Advanced > Settings > Secured**.
- Step 2** Click the **Web Login** tab and select **Web Login**.
- After **Web Login** is selected, remote users can log in to the endpoint web interface to set parameters, start conferences, and view the endpoint status.
- Step 3** Select **Save**.
- End

SSH and Telnet Login

Telnet is an insecure protocol. You are advised to use SSH login.

- Step 1** Choose **Advanced > Settings > Secured > SSH/Telnet**. Set the SSH and Telnet login parameters described in [Table 7-33](#).

Table 7-33 SSH and Telnet login parameters

Parameter	Description	Setting
-----------	-------------	---------

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 deselected 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 and regularly change the password afterward.
SSH	Specifies whether to enable SSH, which improves transmission security and prevents information disclosure.	This parameter is deselected by default. 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 and regularly change the password afterward.



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

7.7.3 Setting the Password of the Remote Control Administrator

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 password if the password is not set to blank.

Procedure

By default, the password of the remote control administrator is **12345678**. To improve device security, set a password at your first login and regularly change the password afterward.

Step 1 Choose **System Settings > Secured**.

Step 2 Click **GUI** tab. Set the password parameters described in [Table 7-34](#).

Table 7-34 Setting the password of the remote control administrator

Parameter	Description	Setting
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 not selected, the administrator password is required only when you select Settings on the Advanced screen.	This parameter is not selected by default.
Current password	Specifies the current password of the remote control administrator.	-
New password Confirm password	Specifies the new password of the remote control administrator.	The password contains a maximum of 32 characters. If you set this password to blank, no password is required when you access the Settings screen and use the customized tool bar on the menu screen. NOTE You are advised to set a complex password. A simple or empty password results in high security risks.

Step 3 Select **Save**.

----End

7.7.4 Setting the Upgrade Password

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

The default upgrade password is **Change_Me**. To improve device security, set a password at your first login and regularly change the password afterward. To change the password, choose **System Settings > Secured > Upgrade password** and set **Upgrade password**.

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.

7.7.5 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 [4.7 Sharing a Presentation](#).

Procedure

The default air content sharing password is **Change_Me**. To improve device security, set a password at your first login and regularly change the password afterward. To change the password, choose **System Settings > Secured > Air Content Sharing** and set **Password**.

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.

7.7.6 Setting Web Account Security

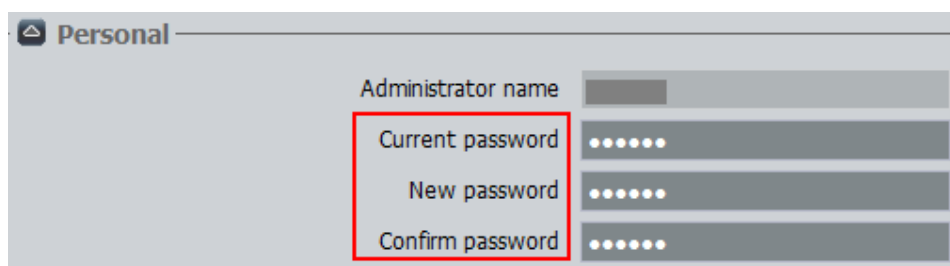
Properly keep the web interface administrator account to ensure the security of web-based login.

Setting the Web Administrator Account

The default account name of the web interface administrator is **admin**, which can be modified only on the remote controlled UI. To change the account name, choose **Advanced Settings > Settings > Secured > Web Login** on the remote controlled UI of the endpoint and set **Administrator name**.

The default password of the web interface administrator is **Change_Me**. To improve device security, set a password at your first login and regularly change the password afterward. On the web page of the endpoint, choose **System Settings > General > Personal** and set the administrator password, as shown in [Figure 7-4](#).

Figure 7-4 Setting the administrator password

The image shows a screenshot of a web interface titled 'Personal'. It contains four input fields: 'Administrator name', 'Current password', 'New password', and 'Confirm password'. The 'Current password', 'New password', and 'Confirm password' fields are masked with dots. A red rectangular box highlights the 'Current password', 'New password', and 'Confirm password' fields.

Setting Web Login Security

Step 1 Choose **System Settings > Secured**.

Step 2 Click **Web Login** tab, set the Web login parameters listed in [Table 7-35](#).

Table 7-35 Web login parameters

Parameter	Description	Setting
Maximum login	Specifies the maximum number of attempts	The value can be 3 , 5 , or

Parameter	Description	Setting
attempts	that you can enter incorrect passwords for any endpoint account or incorrect authentication passwords for connecting to the endpoint. When this number is reached, the endpoint automatically locks the account.	10. The default value is 5 .
Lock time	Specifies the duration an endpoint account will be locked. You can attempt to log in again only when this duration ends. .	The duration can be 5, 10, 15, 20, 30, or 60 minutes. The default value is 5 min.
HTTP	To ensure data transmission security, the endpoint uses HTTPS to access its web pages by default. If a third-party interface uses HTTP to access the endpoint, set this parameter to Enable ; otherwise, the interface cannot access the endpoint.	The default value is Disable .
Wake Up the Endpoint	Specifies whether an endpoint can be waked up on its web interface. If you select this parameter, you can access the web interface of an endpoint to wake up the endpoint when it is in sleep mode.	The default value is Enable .

Step 3 Click the **Overtime** tab and set **Enable overtime**.

Specifies the allowed idle time, exceeding which the current user will be automatically logged out. The default value is **1 h**. If you set this parameter to **Disable**, the endpoint will not log out users automatically.

Step 4 Click **Save**.

The settings take effect immediately.

----End

7.7.7 Setting Whitelist

After you configure a whitelist, only devices with the IP addresses specified in the whitelist can connect to the endpoint. If the whitelist is empty, all IP addresses are allowed to connect to the endpoint. The whitelist helps enhance videoconferencing security.

Background



NOTICE

Set the whitelist under the guidance of technical support engineers.

The endpoint whitelist is empty by default. That is, all IP addresses are allowed to connect to the endpoint. If an endpoint is deployed in a public network, it is recommended that you add commonly used IP addresses and IP address segments to the whitelist to decrease network attack risks. You must add the IP addresses of the following devices to the whitelist:

- PC that is used to access the endpoint web interface
- Videoconferencing MCU
- SMC
- Recording server

Procedure

Step 1 Choose **System Settings > Whitelist**.

Step 2 Select **Enable**.

If **Enable** is deselected, the whitelist is invalid. That is, all IP addresses are allowed to connect to the endpoint. You can modify the whitelist only after selecting **Enable** here.

Step 3 Click **Add** and set **IP address** and **Mask length**.

Step 4 Click **OK**. The settings take effect immediately.

To delete a record from the whitelist, select the record and click **Delete**.

----End

7.8 Importing Security Certificates

Import certificates on the endpoint web interface to improve the communication security.

7.8.1 Importing a Certificate

You can import client, server, and SiteCall and 802.1x authentication certificates into your endpoint. These certificates can be used to identify users, certificate authorities, and servers to improve communication security. For example, a client certificate is required when your endpoint registers with the SIP server using the Transport Layer Security (TLS) protocol.

Prerequisites



NOTICE

Before importing a certificate, make sure it is issued by a security authority to prevent security risks.

- **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.
- **802.1x authentication certificate:** You have obtained the required certificates from the network administrator.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import Certificate**.

The **Import Certificate** dialog box is displayed.

Step 3 Click **Select File** to select the certificate you want to import.

Step 4 Select the desired certificate type.



NOTE

- To import a certificate for authentication calls and when the endpoint functions as the server, select **Server certificate**.
- To import a certificate for authentication registration or calls and when the endpoint functions as a client (for example, TLS-based registration), select **Client certificate**.
- To import a certificate used for SiteCall security, select **Multipoint conference certificate**.
- To import certificates used for 802.1x wired or wireless network authentication, select the desired certificates. When selecting the certificate type, choose the network type, which is **Wireless and wired** by default.

Step 5 Click **Import**.

Step 6 Click **Return** when **OK** is displayed.

----End

7.8.2 Importing Web Certificates

To help ensure communication security, import web certificates, including the trusted Certificate Authority (CA) file, local certificate file, local private key file, and local private key password file, to the endpoint through the endpoint web interface.

Background



NOTICE

Professional guidance is required for importing certificates. Make sure the certificate to be imported matches the certificate type selected; otherwise, the endpoint may malfunction.

Procedure

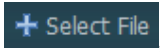
Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import Web Certificate**.

The **Import Web Certificate** dialog box is displayed.

Step 3 Click  and select a certificate type.

Step 4 Click , select the certificate you want to import, and click **Import**.

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

----End

7.8.3 Updating Web Certificates

After you import web certificates to the endpoint, update them to enable them to take effect.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Update Web Certificates**.

Step 3 Click **OK**.

The endpoint restarts.

----End

7.9 Managing System Files

Manage system files on the endpoint interface to improve the operation and maintenance (O&M) efficiency of the endpoint.

7.9.1 Importing and Exporting Settings

You can import or export settings on the endpoint web interface. After your endpoint is restored to its default settings, you can import previously exported settings.

Background

After your endpoint is restored to its default settings upon a fault, you can import previously exported settings.

For example, when your endpoint is faulty and needs to be restored to its default settings, export the existing settings before the restoration. After you restore your endpoint, directly import the exported settings instead of manually setting the parameters. This saves your time.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

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

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

Step 3 Perform either of the following:

- To import system settings, click **Import Settings**.
- To export system settings, click **Export Settings**.

The web administrator password is required when you import the configuration file. After the configuration file is imported successfully, the endpoint automatically restarts for the configuration file to take effect.

----End

7.9.2 Backing Up Settings

The administrator can use the **One-Click Backup** function to create a configuration backup file for your endpoint. If some parameter settings under **System Settings** are inadvertently deleted or changed, you can use this backup file to restore all settings under **System Settings** to the pre-backup settings.

Background

If a configuration backup file is already stored on your endpoint, a new configuration backup file will replace the original one.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **One-Click Backup**.

Step 3 On the **One-Click Backup** page, click **Back Up Settings**.

Your endpoint then starts to create a configuration backup file. When the backup is complete, a notification message is displayed.

----End

Follow-up Procedure

To restore all settings under **System Settings** to the pre-backup settings, click **Restore Backup Settings**. Your endpoint will then restart and restore the settings.

7.9.3 Importing License Files

Some functions on your endpoint, such as Wi-Fi and built-in MCU, 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 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import License**.

The **Import License** dialog box is displayed.

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

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

----End

7.9.4 Importing a Layout Policy File

After a layout policy file is imported to the endpoint, you can set the layout configured in that file during a multipoint conference hosted by the endpoint's built-in MCU or chaired by your site.

Prerequisites

A layout policy file has been exported using the layout customization tool.



NOTE

You can obtain the layout customization tool from the software package for the endpoint.

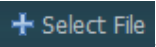
Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Import Layout Policy File**.

The **Import Layout Policy File** dialog box is displayed.

Step 3 Click , select the layout policy file you want to import, and click **Import**.

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

----End

7.9.5 Creating and Downloading a CSR File

You can create and export a CSR file from the endpoint web interface.

Prerequisites

The local private key password file has been imported.

Background

You can send the CSR file to a certification organization to generate an authentication certificate for your endpoint.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Export CSR File**.

Step 3 Enter the CSR file information and click **OK**.

The created CSR file will be stored on the endpoint.

Step 4 Click **Download the CSR file** to save the CSR file to the local computer.

----End

8 Upgrading

About This Chapter

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



NOTICE

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

The differences between the four upgrade methods as follows:

- 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 [8.1 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 [8.2 Tool Upgrade](#).
- Upgrade using the mini system
If upgrading the endpoint using its normal system fails due to a power failure or other causes, you can use the mini system to complete the upgrade. For details, see [8.3 Upgrading the Endpoint Using the Mini 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 [8.4 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.

[8.1 Automatic Upgrade](#)

You can update your endpoint's software from the web interface. 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.

8.2 Tool Upgrade

You can use a computer to locally upgrade the endpoint.

8.3 Upgrading the Endpoint Using the Mini System

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

8.4 Upgrading the Endpoint on Its Web Interface

You can update the endpoint software from the web interface.

8.1 Automatic Upgrade

You can update your endpoint's software from the web interface. 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 **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Auto Upgrade Settings**.

The **Auto Upgrade Settings** page is displayed.

Step 3 Set the upgrade parameters listed in [Table 8-1](#).

Table 8-1 Upgrade parameters

Parameter	Description	Setting
Auto upgrade	Specifies whether the automatic upgrade function is enabled. If you set this parameter to Enable , you must also set Upgrade interval , Server address , User name , and Password . Your endpoint will obtain upgrade files from the specified server and install the files when the specified upgrade interval is reached.	This parameter is deselected 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.
Upgrade	Specifies the upgrade interval. This	The default value is 0.5 h .

Parameter	Description	Setting
interval	parameter is available only when Auto upgrade is selected.	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.
User name Password	Specify the user name and password your endpoint uses to access the server.	No default value is set for these parameters.

Step 4 Perform either of the following:

- If you selected **Auto upgrade**, click **Save**.
- Click **Manual upgrade**.

----End

8.2 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 [7.7.4 Setting the Upgrade Password](#).

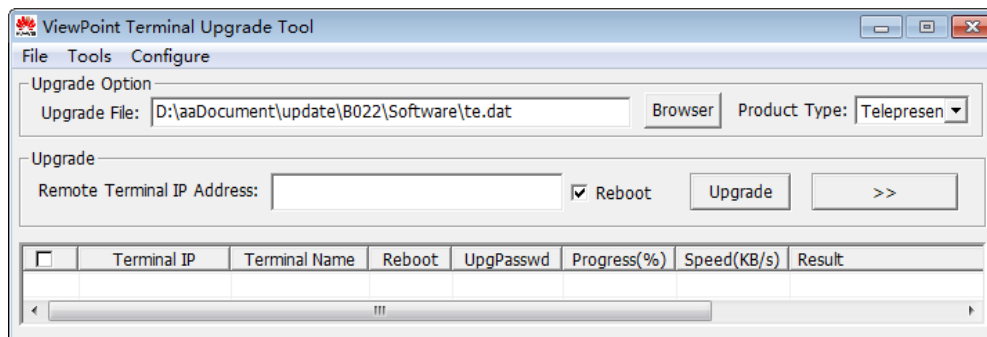
Upgrading a Single endpoint

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 8-1](#).

Figure 8-1 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 8-1](#).

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

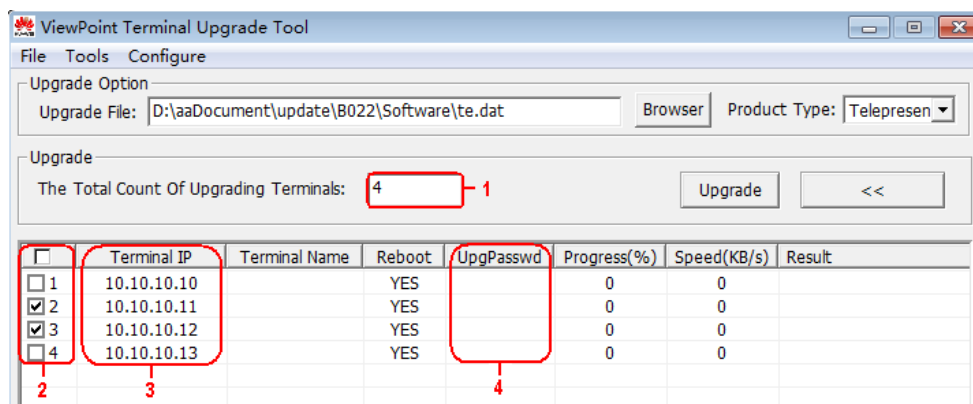


NOTE

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

Step 5 Click >>' button shown in [Figure 8-1](#) to display the window as shown in [Figure 8-2](#).

Figure 8-2 Upgrading multiple endpoints in batches



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

8.3 Upgrading the Endpoint Using the Mini System

If upgrading the endpoint using its normal system fails, you can use the mini 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 [7.7.4 Setting the Upgrade Password](#).

Background

The mini 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 mini 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 mini system upgrade function.



NOTE

- The mini 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

8.4 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 **Upgrade** 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.

9 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.

[9.1 Checking the Working Environment Periodically](#)

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

[9.2 Managing Common Users and Passwords](#)

Properly keep the accounts of common web interface users. After logging in to the web interface, a common user can configure only personal settings.

[9.3 Customizing the Web Interface](#)

On the endpoint, you can customize the shortcut bar and desktop icons to be displayed on the web interface.

[9.4 Customizing the Remote Controlled UI](#)

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

[9.5 Checking the Endpoint Periodically](#)

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

[9.6 Viewing System Status](#)

System status information helps you maintain your endpoint.

[9.7 Querying System Information](#)

System information helps you maintain your endpoint.

[9.8 Querying Logs](#)

Logs record, in real time, all important events that occur when your endpoint runs. These records assist you in maintaining your endpoint and locating system faults.

[9.9 Restoring Your Endpoint to Default Settings](#)

You can use the **Restore Default** function to restore your endpoint to its default settings.

9.1 Checking the Working Environment Periodically

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

Table 9-1 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 9-1 Checking the working environment

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

9.2 Managing Common Users and Passwords

Properly keep the accounts of common web interface users. After logging in to the web interface, a common user can configure only personal settings.

Step 1 Choose **System Settings** > **General** on the endpoint web interface.

The **General** page is displayed.

Step 2 Click the **Personal** tab and set the parameters described in Table 9-2.

Table 9-2 Setting the accounts of common web interface users

Parameter	Description	Setting
Name of user 1 Name of user 2 Password of user 1 Password of user 2 Confirm password	Specify common users' user name and password. This type of user can configure personal but not system settings.	The user name can contain a maximum of 64 characters, and the password can contain 6 to 32 characters. The password must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.

Parameter	Description	Setting
Name of API user Password of API user Confirm password	Specify the user name and password for authenticating the touch panel when it attempts to connect to your endpoint or authenticating the Service Management Center (SMC) when it attempts to add your endpoint as manageable participant.	- The default value of User name is api. - The default value of User password is Change_Me. The user name can contain a maximum of 64 characters, and the password can contain 6 to 32 characters. The password must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.

Step 3 Click **Save**.

The settings take effect immediately.

----End

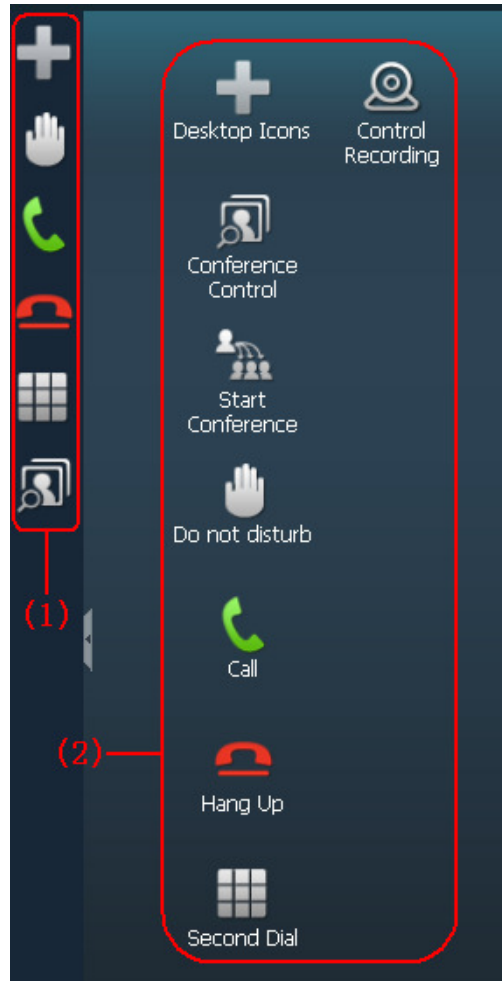
9.3 Customizing the Web Interface

On the endpoint, you can customize the shortcut bar and desktop icons to be displayed on the web interface.

Background

Figure 9-1 shows the shortcut bar and desktop icons.

Figure 9-1 Shortcut bar and desktop icons



(1) Shortcut bar

(2) Desktop icons

Procedure

Step 1 On the endpoint web interface, choose **System Settings > Display** and click the **User defined** tab.

Step 2 Perform any of the following operations:

- To customize desktop icons, click **Desktop Icons** and select the icons you want to display on the desktop.
- To customize the shortcut bar, click **Shortcut Bar Icons** and select the icons you want to display in the shortcut bar. A maximum of 10 icons can be displayed on the shortcut bar.
- To restore the web interface to its default style, click **Restore Initial Style**.

Step 3 Follow the onscreen instructions to complete your settings.

----End

9.4 Customizing the Remote Controlled UI

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

9.4.1 Customizing Onscreen Status Icons

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

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

Choose **System Settings > Display**, click the **Icon** tab, and customize status icons.

Packet Loss Rate Icon

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.

When **Serious packet loss notice** is enabled, the remote controlled UI displays a text alert if the packet loss rate is greater than threshold B for 5 seconds or more.

Other Icons

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

- The status icon to be displayed on screens is selected.
- The function or the condition that corresponds to the status icon has been enabled.

9.4.2 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.



NOTE

The following operations are based on the remote controlled UI. Some parameters can also be set on the web interface. To set the parameters on the web interface, log in to the web interface and choose **System Settings > Display > Site Name**.

Step 1 On the remote controlled UI, choose **Advanced > Settings > Display > Personalize**.

Step 2 Set the custom parameters described in [Table 9-3](#).

Table 9-3 Custom parameters

Parameter	Description	Setting
Transparency	Transparency of the remote controlled UI against the background image. If you set this parameter to Opaque , the background image is not displayed on operation screens except the call and menu screens. If you set this parameter to other values, the background image is visible on the remote controlled UI.	The default value is 15% .
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 .
Bold	Specifies whether a site name is displayed in bold.	This parameter is not selected by default.
Background color	Specifies the background color for the site name display.	The default color is gray.
Transparency	Specifies the transparency for the site name display.	The default value is Fully transparent .

Parameter	Description	Setting
Set the horizontal offset	Fine-tunes the site name's position left or right on the local video.	The default value is 48 . Value range: 0-96.
Set the vertical offset	Fine-tunes the site name's position up or down on the local video.	The default value is 48 . Value range: 0-96.

Step 3 Select **Save**.

----End

9.4.3 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: **Add Site**, **Disconnect Site**, **Mute/Unmute MIC**, **Extend Conference**, **End Conference**, **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

9.4.4 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  or  on the remote control.

Procedure

Step 1 Press  or  on the remote control to access the menu screen.

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, press **OK** on the remote control to select or deselect the icon.

Step 4 Select **OK**.

----End

9.5 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.

9.6 Viewing System Status

System status information helps you maintain your endpoint.

On the endpoint web interface, choose **Maintenance > System Status**. On the **System Status** page that is displayed, you can check:

- Line status: includes the local IP address, alternate IP address, network interface mode, WLAN IP address, information about whether GK is enabled, H.323 site number, information about whether SIP is enabled, SIP site number, PSTN status, PSTN number of a remote site, running duration, and camera status.
- Call status: includes the conference number (or the IP address, number, or name of the remote site), 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. The call status is displayed only when your endpoint is in 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 number, signaling encryption, media stream encryption, conference number for video access, conference number for audio access, and password for conference authentication. The conference parameters are displayed only when your endpoint is in a conference.

- Input port status: includes the video information, USB1 and USB2 ports and air content sharing information.
- 4E1 connection status (only for the TE60).

9.7 Querying System Information

System information helps you maintain your endpoint.

Choose **Maintenance > System Information**. On the displayed **System Information** page, you can check:

- 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)
- Support for and capabilities of the built-in MCU
- Whether your endpoint supports dual stream, namely, the video and presentation
- Whether your endpoint supports H.235 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
- Valid term of the license
- ESN
- MAC address

9.8 Querying Logs

Logs record, in real time, all important events that occur when your endpoint runs. These records assist you in maintaining your endpoint and locating system faults.

Background

Your endpoint can store a maximum of 10000 log records. When the memory for recording logs is full, new logs can still be recorded by replacing the oldest one.

Procedure

Step 1 Choose **Maintenance > Logs**. On the **Logs** page, specify one or more of the following criteria to query logs:

- Time when the log is created
- Log level: **Information**, **Warning**, **Error**, or **All levels**
- Log type: **4E1**(only TE60), **Main control**, **WEB**, **UI**, **BSP**, **Audio**, **Video**, **Protocol**, or **All**

Step 2 Click **Query**.

----End

9.9 Restoring Your Endpoint to Default Settings

You can use the **Restore Default** function to restore your endpoint to its default settings.

Prerequisites

You have obtained the serial number of your endpoint.

To obtain the serial number of your endpoint, choose **Help > Version**.

Background

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.

Procedure

Step 1 Choose **System Settings > Installation**.

The **Installation** page is displayed.

Step 2 Click **Restore Default**.

Step 3 Enter the serial number of your endpoint.

Step 4 Click **Restore Default** and confirm your operation.

----End

10 Troubleshooting

About This Chapter

This chapter describes how to diagnose and troubleshoot endpoint faults.

10.1 Understanding Diagnosis Methods

The endpoint supports the following diagnosis methods: sound and color bar tests, loopback tests, network tests, one-click diagnosis, signaling diagnostics, tracert, and remote control tests.

10.2 Common Faults

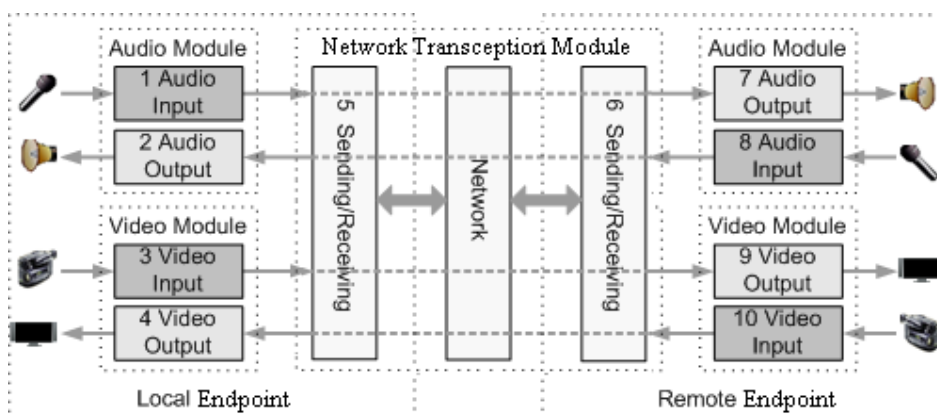
This section describes the problems you might encounter when using your endpoint and provides solutions.

10.1 Understanding Diagnosis Methods

The endpoint supports the following diagnosis methods: sound and color bar tests, loopback tests, network tests, one-click diagnosis, signaling diagnostics, tracert, and remote control tests.

[Figure 10-1](#) shows the diagnosis model for your endpoint.

Figure 10-1 Diagnosis model



According to [Figure 10-1](#), diagnosis functions diagnoses the audio module, video module, and network module.

Audio signals are transmitted in the following paths:

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

Video signals are transmitted in the following paths:

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

Sound and Color Bar Tests

[Table 10-1](#) lists the sound and color bar tests.

Table 10-1 Sound and color bar tests

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

- Sound test: Choose **Maintenance > Diagnostics**. On the **Diagnostics** page, click **Sound Test**. While the test audio stored on your endpoint plays, check the sound quality.
- Color bar test: Choose **Maintenance > Diagnostics**. On the **Diagnostics** page, click **Color Bar Test**. Seven color bars are shown on the display for you to check the color quality.

Loopback Test

Your endpoint can transmit audio or video data on a channel to simulate an actual application and test whether the output is satisfactory. You can perform a local loopback test to check the local network connection or a remote loopback test to check the remote network connection.

When you perform a remote loopback test, data is transmitted from your site to a remote site, and then back to your site. [Table 10-2](#) lists the types of loopback tests available on your endpoint.



CAUTION

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

Table 10-2 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 → Monitor
Digital loopback	Local audio and video modules	The endpoint performs local audio and video loopback tests simultaneously.
Remote audio loopback	• Remote audio module • Network transmission	Microphone → 1 → 5 → 6 → 7 → 8 → 6 → 5 → 2 → Speaker
Remote video loopback	• Remote video module • Network transmission	Camera → 3 → 5 → 6 → 9 → 10 → 6 → 5 → 4 → Monitor
Remote digital loopback	• Remote audiovisual modules • Network transmission	The endpoint performs remote audio and video loopback tests simultaneously.

Network Test

Table 10-3 Network test

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

Before a test, verify that the LAN network port indicator is green, which indicates that your endpoint is correctly connected to an IP network.

- In **IP address**, enter an IP address that is in a different network segment from your endpoint IP address. Then click **Start**. If the test succeeds, 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 click **Start**. If the test succeeds, the gateway settings, NAT address, and IP address of your endpoint are correct.

One-Click Diagnosis

Web administrators and API users can perform one-click diagnosis on the endpoint. The diagnosis file helps with fault identification.

Step 1 Choose **Maintenance > One-Click Diagnosis**.

The **One-Click Diagnosis** dialog box is displayed.

Step 2 Click **Start** to start diagnosis.

The diagnosis takes about 5 minutes.

Step 3 Click **Download** to save the diagnosis file to the local computer.

----End

Signaling Diagnostics

Web administrators and API users can perform signaling diagnostics and export the diagnostics file from the endpoint web interface. The diagnostics file helps with fault identification.

- Only one user can perform signaling diagnostics.
- If not manually stopped, signaling diagnostics automatically stops after 10 minutes or when the diagnostics file size reaches 10 MB.

Step 1 Choose **Maintenance > Signaling Diagnostics**.

The **Signaling Diagnostics** dialog box is displayed.

Step 2 Click **Start** to start signaling diagnostics.

When prompted, click **OK**.



NOTE

Signaling diagnostics does not monitor media stream data, but will obtain site information, such as site numbers. Perform this operation with caution.

Step 3 Click **Stop** to stop signaling diagnostics.

Step 4 Click **Download** to save the diagnostics file to the local computer.

----End

Route Test

A route test helps determine the path that a data packet at the network layer uses to access a destination address.

Before you perform route test, choose **System Settings > Network > Network diagnostics** and set **Network diagnostics** to **Enable**.

Table 10-4 lists the parameters that you need to set before performing a route test.

Table 10-4 Route parameters

Parameter	Description	Setting
-----------	-------------	---------

Parameter	Description	Setting
IP address	Specifies the IP address of the destination device.	Example: 10.10.10.1
Maximum hops	Specifies the maximum allowed hops.	Example: 5
Timeout time(s)	Specifies the timeout duration for the call waiting time, in seconds.	Example: 1

Remote Control Test

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.

When using the remote control to operate the endpoint, you can use the camera to forward infrared signals to the endpoint. To enable the camera to forward infrared signals, choose **Advanced > Settings > Video > Common Settings > Video Input** and set **Infrared camera is used to control the endpoint** to **Yes**.

10.2 Common Faults

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

Web Interface

[Table 10-5](#) lists the troubleshooting methods for problems that may arise on the endpoint web interface.

Table 10-5 methods for troubleshooting endpoint web interface problems

Problem	Possible Cause	Solution
A message is displayed to	The latest patches for the operating system or Internet	Install the latest patches for the operating system and Internet

Problem	Possible Cause	Solution
indicate that your endpoint failed to connect to the Internet or download images.	Explorer are not installed.	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.	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.	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, 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.	• 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.	• 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 10-6 lists the troubleshooting methods for problems that may arise on the network.

Table 10-6 Methods for troubleshooting common network problems

Problem	Possible Cause	Solution
---------	----------------	----------

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.	The number of connections to the endpoint has reached the maximum value. NOTE - 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 10-7 lists the troubleshooting methods for video problems.

Table 10-7 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

Problem	Possible Cause	Solution
		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 black and white.	The mode adopted by the video output port is set incorrectly.	- Ensure that the mode adopted by the video output port and the cable in use match each other. - 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	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.

Problem	Possible Cause	Solution
	only 196 kbit/s. In this case, the video quality is poor.	
	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.
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	Set the resolution and refresh rate of the computer used for the VGA

Problem	Possible Cause	Solution
	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.	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 control screen,  ,  , and navigation keys on the remote control cannot be used to control the camera.	The camera you want to control is not selected.	Access the camera control screen and select the camera you want to 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 10-8 lists the troubleshooting methods for audio problems.

Table 10-8 Methods for troubleshooting audio problems

Problem	Possible Cause	Solution
---------	----------------	----------

Problem	Possible Cause	Solution
Current noise is generated when the endpoint's audio output ports are connected to audio devices, such as speakers, tuning consoles, and audio matrices.	Disconnect the endpoint's audio output ports from the audio devices. Check whether the problem is rectified. If the problem persists, the current noise is caused by audio device or cable issues.	Replace the cables or repair the audio devices.
	If the problem is rectified, check the grounding status of the audio devices and endpoint.	• If the audio devices' shells are grounded, the endpoint's shell must be grounded nearby. • If the audio devices' shells are not grounded, the endpoint's shell does not need to be grounded either. Specifically, change the endpoint's AC three-core power supply to two-core power supply.
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.	• 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 occurs at the remote site.	• The microphone at the remote site has been muted or the chair site has muted this microphone. In this case, contact the chair site to resolve this problem. • 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

Problem	Possible Cause	Solution
		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 10-9 lists the troubleshooting methods for problems you may encounter during conference initiation.

Table 10-9 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.	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. If a remote site places a call to 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.	Verify GK registration settings and register your site and the remote site with a GK.
	The local or remote endpoint is not connected to an IP network.	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.

Problem	Possible Cause	Solution
		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.
Your site cannot place a call to a remote site using the IP address of the remote site.	The local or remote endpoint is not connected to an IP network.	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 remote endpoint is on a public or different private 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 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	Contact the videoconferencing system administrator to check

Problem	Possible Cause	Solution
	already registered with the GK.	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.	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.
A predefined conference fails to be initiated on the endpoint.	The endpoint is disconnected from an IP network.	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.

Problem	Possible Cause	Solution
		3. From the remote controlled UI, choose Advanced > Settings > Network > IP . Verify IP network settings.
	- 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 10-10](#) lists the troubleshooting methods for common problems you may encounter during conference control.

Table 10-10 Methods for troubleshooting conference control problems

Problem	Possible Cause	Solution
While the endpoint is in use during a conference, you cannot view the desired site.	A site in the conference is being broadcast, and all the sites must view that site except the chair site and broadcast site.	Ask the chair site to stop 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.

Problem	Possible Cause	Solution
	The View Site function is restricted on the RM or the SMC.	Contact the videoconferencing system administrator to resolve this problem.

11 Technical Specifications

About This Chapter

This chapter describes the product specifications, external ports, system performance and capacity, and standards compliance.

- [11.1 Physical Specifications](#)
- [11.2 Performance and Capacity](#)
- [11.3 Ports and Protocols](#)
- [11.4 Standards Compliance](#)

11.1 Physical Specifications

Table 11-1 Physical specifications

Item	Specifications
Electricity supply requirements	
Operating voltage and frequency	100 V AC–240 V AC; 50 Hz–60 Hz;
Maximum power consumption	- TE60: 150W - TE50: 60W - TE40: 60W
Working state environment requirements	
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

Item	Specifications
Recommended illuminance	> 300 lux
Non-working state environment requirements	
Ambient temperature	–40°C to +85°C
Relative humidity	0% to 95%
Physical specifications	
Codec dimensions (H x W x D)	72.5 mm x 435 mm x 265.5 mm (2.85 in. x 17.13 in. x 10.45 in)
Weight	- TE60: 4.6 kg (net weight) - TE50: 4.1 kg (net weight) - TE40: 3.9 kg (net weight)

11.2 Performance and Capacity

Table 11-2 lists the endpoint performance and capacity specifications.

Table 11-2 Performance and capacity

Item	Specifications
Call bandwidth (IP)	64 kbit/s-8 Mbit/s
Call bandwidth (4E1, only TE60)	64 kbit/s-8 Mbit/s
Video resolution	1080p60 with a minimum bandwidth of 1 Mbit/s (optional) 1080p30 with a minimum bandwidth of 512 kbit/s (only TE40 is optional) 720p60 with a minimum bandwidth of 512 kbit/s (only TE40 is optional) 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,

Item	Specifications
	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	- dual 1080p60 - Video Motion Enhancement - VideoIntensifier - ViewProcessing - Super Error Concealment
Audio features	AEC, ANS, AGC, VoiceClear, AudioEnhancer, and lip synchronization
Built-in MCU capability	- TE40: six 720p30 video sites and three audio-only sites - TE50: six 720p30 video sites and three audio-only sites - TE60: nine 720p30 video sites and three audio-only sites

11.3 Ports and Protocols

Table 11-3 Ports on the TE60

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
Video input	1 x HDMI/DVI (audio input supported) 2 x DVI-I (HDMI, VGA, and YPbPr supported with conversion cables) 2 x HD-VI/DVI 1 x CVBS/S-VIDEO (converted from a DVI-I port) 1 x DisplayPort 1 x 3G-SDI	DVI1.0 VESA	HD-VI port for VPC600/VPC620
Video	2 x HDMI/DVI (audio output)	DVI1.0 VESA	-

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
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) • 1 x 3G-SDI		
Audio input	• 1 x XLR • 2 x RCA • 1 x HDMI • 1 x HD-AI • 1 x DisplayPort	-	-
Audio output	• 4 x RCA • 2 x HDMI • 2 x DVI-I (with the use of a DVI-HDMI cable)	-	-
USB port	2 x USB 2.0	USB 2.0	-
Network port	• 2 x 10/100/1000M LAN • 1 x Wi-Fi (built-in) • 1 x 4E1 (optional) • 1 x PSTN	-	Currently, the PSTN port can be used in China only.
Serial port	2 x RS232	-	-
Infrared remote control port	Infrared signal reception	NEC	-

Table 11-4 Ports on the TE50

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
Video input	• 1 x HD-VI/DVI • 1 x HDMI/DVI (audio input)	• DVI1.0 VESA • HDMI 1.3	HD-VI port for VPC600/VPC620

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
	supported) • 1 x VGA/YPbPr • 1 x 3G-SDI • 1 x CVBS		
Video output	• 2 x HDMI/DVI (audio output supported) • 1 x VGA/YPbPr • 1 x 3G-SDI • 1 x CVBS	DVI1.0 VESA	-
Audio input	• 1 x XLR • 2 x RCA • 1 x HDMI • 1 x HD-AI • 1 x 3.5mm	-	-
Audio output	• 4 x RCA • 2 x HDMI	-	-
USB port	2 x USB 2.0	USB 2.0	-
Network port	• 2 x 10/100/1000M LAN • 1 x Wi-Fi (built-in) • 1 x PSTN	-	Currently, the PSTN port can be used in China only.
Serial port	2 x RS232	-	-
Infrared remote control port	Infrared signal reception	NEC	-

Table 11-5 Ports on the TE40

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
Video input	• 1 x HD-VI/DVI • 1 x HDMI/DVI (audio input supported) • 1 x VGA/YPbPr	• DVI1.0 VESA • HDMI 1.3	HD-VI port for VPC600/VPC620

Port	Description and Quantity	Standards and Protocols Compliance	Remarks
Video output	2 x HDMI/DVI (audio output supported) 1 x VGA/YPbPr	DVI1.0 VESA	-
Audio input	1 x XLR 2 x RCA 1 x HDMI 1 x HD-AI	-	-
Audio output	4 x RCA 2 x HDMI	-	-
USB port	2 x USB 2.0	USB 2.0	-
Network port	2 x 10/100/1000M LAN 1 x Wi-Fi (built-in) 1 x PSTN	-	Currently, the PSTN port can be used in China only.
Serial port	2 x RS232 COM	-	-
Infrared remote control port	Infrared signal reception	NEC	-

11.4 Standards Compliance

Table 11-6 lists the standards that the endpoint complies with.

Table 11-6 Standards compliance

Item	Specifications
Video encoding and decoding protocols	H.264 SVC, H.264 HP, H.264 BP, H.263, and H.263+
Video encoding and decoding protocols	AAC-LD, G.711A, G.711U, G.719, G.722, G.728, G.729A, HWA-LD, G.722.1, and G.722.1C
Multimedia frame protocols	ITU-T H.323 and IETF SIP
Dual-stream standard	ITU-T H.239 and BFCP
Network transmission	TCP/IP, RTP, RTCPFTP, DHCP, SNMP, Telnet, HTTP, SSH, HTTPS, PPPoE, and SNTP

Item	Specifications
protocols	
Other communications protocols	H.225, H.235, H.241, H.245, H.281, H.350, H.460, T.140
IP protocol	IPv4/IPv6 dual stack
Protocol for signaling and media stream encryption	H.235; TLS, SRTP
H.323 remote camera control	H.281 and H.224

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

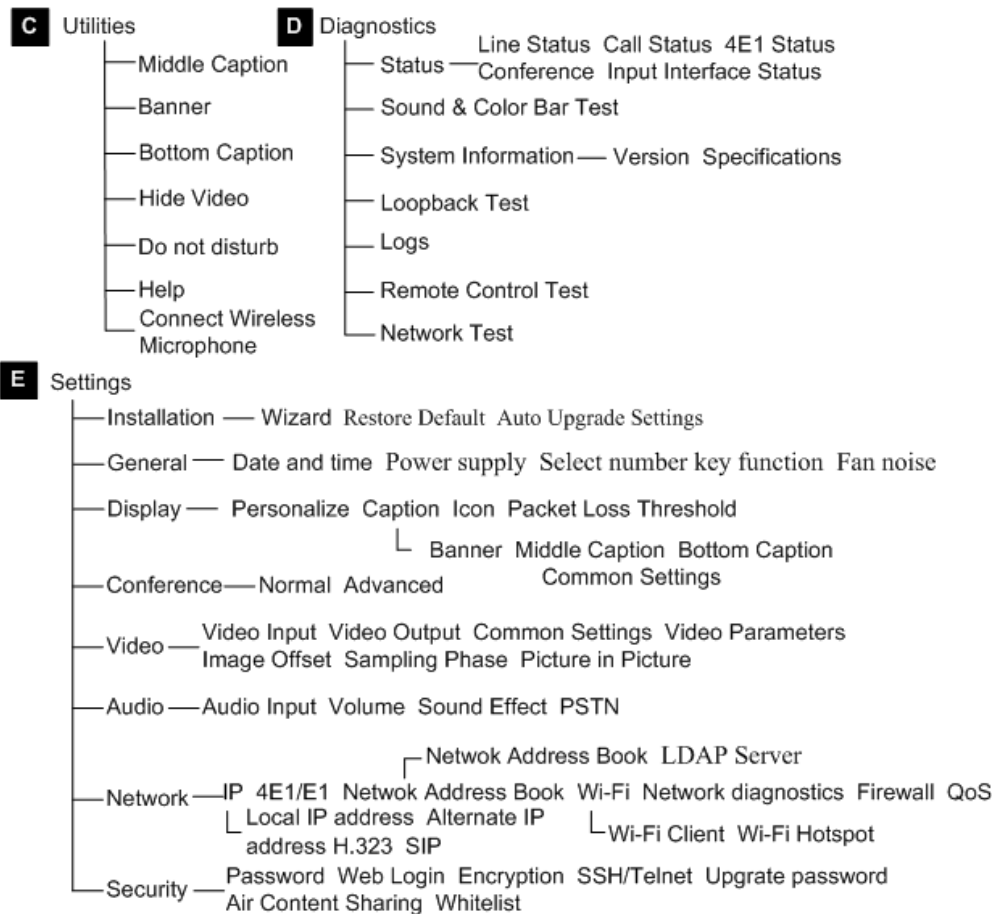
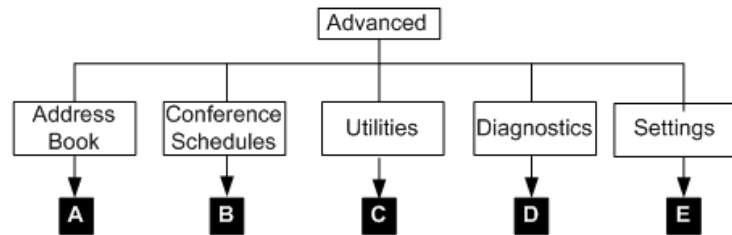
For questions about grounding the device, contact the device provider for technical support.

B Menu Structure of the Remote Controlled UI

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 B-1](#) shows the menu structure.

Figure B-1 Menu structure



NOTE

Only the TE60 supports 4E1 functions.

C Requirements on Room Layout and Lighting

When using the endpoint, pay attention to your sitting posture to avoid problems associated with your back. Do not stare at the monitor screen for a long time. This may harm your eyes or blur your vision.

Layout Precautions

- Ensure that there are no large or moving objects behind you. Otherwise, the video cannot be viewed clearly.
- Do not use striped patterns as the background.
- Do not hold a conference in a room that generates a lot of echoing.
- Do not place the endpoint near a sound source.

Lighting Precautions

To ensure high video quality, do not turn the lens towards bright lights.

D 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 D-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 D-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 D-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 D-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 9.4.1 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.

E Default Settings

To better use the endpoint, get to know the default values of common user names and passwords.

[Table E-1](#) lists the default user names and passwords for the endpoint.

Table E-1 Default user names and passwords

Item	Default Setting
Administrator password for the remote controlled UI	12345678
Administrator user name and password for the endpoint web interface	The default user name and password are admin and Change_Me respectively.
Upgrade password	Change_Me
Air content sharing password	Change_Me
User name and password for connecting the touch panel to the endpoint	The default user name and password are api and Change_Me respectively.
User name and password for logging in to the endpoint in Telnet mode	• Debug user: The default user name and password are debug and Change_Me respectively. • Administrator: The default user name and password are admin and Change_Me respectively. • Common user: The default user name and password are user and Change_Me respectively. • Test user: The default user name and password are test and Change_Me respectively. • Touch panel user: The default user name and password are apiuser and Change_Me respectively.
User name and password for logging	The default user name and password are root and

Item	Default Setting
in to the endpoint in serial port mode	Change_Me respectively.
Default IP address after the endpoint is restored to its default settings	192.168.1.1

F Glossary

Numerics

2 x Common Intermediate Format (2CIF)	A video format with a resolution of 352 x 576 pixels and using progressive scanning.
2 x Source Input Format (2SIF)	A video format with a resolution of 352 × 480 pixels and using progressive scanning.
2CIF	See 2 x Common Intermediate Format .
2SIF	See 2 x Source Input Format .
3G	See 3rd Generation .
3GPP	3rd Generation Partnership Project
3rd Generation (3G)	The third generation of digital wireless technology, as defined by the International Telecommunications Union (ITU). Third generation technology is expected to deliver data transmission speeds between 144 kbit/s and 2 Mbit/s, compared to the 9.6 kbit/s to 19.2 kbit/s offered by second generation technology.
4 x Common Intermediate Format (4CIF)	A video resolution of 704 x 576 pixels.
4 x Source Input Format (4SIF)	A video format with a resolution of 704 × 480 pixels and using progressive scanning.
4CIF	See 4 x Common Intermediate Format .
4SIF	See 4 x Source Input Format .

A

AAC	advanced audio coding
AEC	See acoustic echo cancellation .
AES	See Advanced Encryption Standard .
AGC	automatic gain control

API	See application programming interface .
ASCII	American Standard Code for Information Interchange
Advanced Encryption Standard (AES)	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). It supersedes the Data Encryption Standard (DES). AES adopts a symmetric-key algorithm for both encrypting and decrypting the data, where the block size is 128 bits and the key size is 128 bits, 192 bits, or 256 bits.
acoustic echo cancellation (AEC)	A type of signal processing commonly used in teleconferencing. The speech from the far-end caller is broadcast by the speakerphone or the hands-free cellular phone and then repeats itself by bouncing off the inside surfaces of a room or car. This repetition of sound is called an echo. Echoes are picked up by the near-end microphone, creating a feedback loop where the far-end caller hears an echo of his or her own voice. AEC is developed to solve this problem.
application programming interface (API)	An application programming interface is a particular set of rules and specifications that are used for communication between software programs.
B	
BSP	board support package
balanced circuit	A circuit using two lines carrying equal but opposite signals.
built-in MCU	A built-in unit of an endpoint, by using the built-in MCU, the endpoint can hold a multipoint conference that supports multiple functions, such as site access, video exchange, audio mixing, data processing, and signaling interaction.
C	
CAS	See channel associated signaling .
CCS	See Common Channel Signaling .
CIF	Common Intermediate Format
Common Channel Signaling (CCS)	A signaling system used in telephone networks that separates signaling information from user data. A specified channel is exclusively designated to carry signaling information for all other channels in the system.
camera	A device for recording visual images in the form of photographs, movie film, or video signals.
certificate	The certificate, also called the digital certificate, establishes the association between the user identity and user public key. The certificate is issued by the third-party authority, and provides identity authentication for the communications parties.
chair site	A site that has chair control rights.
channel associated signaling (CAS)	A signaling system in which signaling information is transmitted within a dedicated voice channel. China Signaling System No. 1 is a type of CAS signaling.
conference	An IP multimedia session that have two or more participants. Each conference has a

	focus and can be identified uniquely.
conference service number	The number defined in conference settings on an MCU. On a video terminal, users can dial this number to join an ongoing conference to which the terminal has been added as a participant.
configuration file	A file that contains machine-readable operating specifications for a piece of hardware or software or that contains information on another file or on a specific user, such as the user's login ID.
congestion	Extra intra-network or inter-network traffic resulting in decreased network service efficiency.
D	
DHCP	See Dynamic Host Configuration Protocol .
DN	distinguished name
DNS	See domain name server .
DNS server	A device that can provide domain name resolution for the client on the network
DSCP	See differentiated services code point .
DVI	digital visual interface
DVI-I	digital visual interface-integrated
Dynamic Host Configuration Protocol (DHCP)	A client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting information the host requires to participate on the Internet network. DHCP also provides a mechanism for allocating IP addresses to hosts.
default settings	Parameter settings of a device when the device is delivered from a factory.
differentiated services code point (DSCP)	According to the QoS classification standard of the Differentiated Service (Diff-Serv), the type of services (ToS) field in the IP header consists of six most significant bits and two currently unused bits, which are used to form codes for priority marking. Differentiated services code point (DSCP) is the six most important bits in the ToS. It is the combination of IP precedence and types of service. The DSCP value is used to ensure that routers supporting only IP precedence can be used because the DSCP value is compatible with IP precedence. Each DSCP maps a per-hop behavior (PHB). Therefore, terminal devices can identify traffic using the DSCP value.
digital network	A telecommunication network where information is first converted into distinct electronic pulses and then transmitted to a digital bit stream.
domain name server (DNS)	A functional entity in the TCP/IP network. With deployment of the DNS, subscribers can access related servers using corresponding domain names. In the TCP/IP network, a domain name maps an IP address. Domain names are easier to remember but servers in the network communicate with each other using IP addresses. Therefore the DNS is used to convert domain names to corresponding IP addresses.
download	To obtain data from an upper-layer device or the server.
dual stream	During a conference, two channels of video streams can be sent or received simultaneously. One channel is used for transmitting video (such as the video

captured by a camera) and the other channel is used for transmitting presentation (such as a computer desktop). These two channels of videos can be displayed on two monitors.

E

- E1** An European standard for high-speed data transmission at 2.048 Mbit/s. It provides thirty-two 64 kbit/s channels. A time division multiplexing frame is divided in to 32 timeslots numbered from 0 to 31. Timeslot 0 is reserved for frame synchronization, and timeslot 16 is reserved for signaling transmission. The rest 30 timeslots are use as speech channels. Each timeslot sends or receives an 8-bit data per second. Each frame sends or receives 256-bit data per second. 8000 frames will be sent or received per second. Therefore the line data rate is 2.048 Mbit/s.
- ESN** See [electronic serial number](#).
- electronic serial number (ESN)** A 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.
- encryption** A function used to transform data so as to hide its information content to prevent it's unauthorized use.
- eye contact** A meeting of the eyes between remote and local participants.

F

- FTP** File Transfer Protocol
- FTPS** See [File Transfer Protocol over SSL](#).
- File Transfer Protocol over SSL (FTPS)** An extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.
- firewall** A combination of a series of components set between different networks or network security domains. By monitoring, limiting, and changing the data traffic across the firewall, it masks the interior information, structure and running state of the network as much as possible to protect the network security.

G

- G.711** Audio codec standard (A-law or U-law) that uses pulse code modulation (PCM). Its data rate is 64 kbit/s.
- G.722** Audio codec standard that uses adaptive differential pulse-code modulation (ADPCM). Its data rate is 48 kbit/s, 56 kbit/s, or 64 kbit/s.
- G.728** Audio codec standard that uses low-delay code excited linear prediction (LD-CELP). Its data rate is 16 kbit/s.
- GMT** Greenwich Mean Time
- GUI** graphical user interface

gatekeeper	An H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.
gateway	A device that connects two network segments using different protocols. It is used to translate the data in the two network segments.
gateway IP address	The IP address of a gateway. A gateway is a node that forwards packets between networks. Packets are sent to the gateway IP address when the destination network address resides in a different network to the sender.

H

H.239	A standard recommended by ITU-T. It enables a video conference to have simultaneous transmission of both video and data content (for example, computer desktop).
H.261	A video codec standard for video conferences at px64 kbit/s. Two formats are available, including CIF and QCIF.
H.263	A video codec standard for video conferences at low rates. Five formats are available, SQCIF, QCIF, CIF, 4CIF, and 16CIF.
H.264	Compared with H.263, H.264 can provide the same-quality video at half of the bit rate, with strong error resilience characteristics.
HD	high definition
HDMI	high definition multimedia interface
HTML	Hypertext Markup Language
HTTP	See Hypertext Transfer Protocol .
HTTPS	See Hypertext Transfer Protocol Secure .
Hypertext Transfer Protocol (HTTP)	An application-layer protocol used for communications between web servers and browsers or other programs. HTTP adopts the request-response mode. A client sends a request to the server. The request consists of two parts: request header and MIME-like message. The request header contains request method, uniform resource locator (URL), and protocol version. The MIME-like message contains request modifiers, client information, and possible body content. Upon receiving the request, the server responds with a status line. The status line includes the message's protocol version, a success or error code, and a MIME-like message, which contains server information, entity meta-information, and possible entity-body content. For details about HTTP, see RFC2616.
Hypertext Transfer Protocol Secure (HTTPS)	An HTTP protocol that runs on top of transport layer security (TLS) and Secure Sockets Layer (SSL). It is used to establish a reliable channel for encrypted communication and secure identification of a network web server. For details, see RFC2818.

I

ID	See identity .
IETF	Internet Engineering Task Force
IMS	IP multimedia subsystem
IP address	A 32-bit (4-byte) binary number that uniquely identifies a host connected to the Internet. An IP address is expressed in dotted decimal notation, consisting of the decimal values of its 4 bytes, separated with periods; for example, 127.0.0.1. The first three bytes of the IP address identify the network to which the host is connected, and the last byte identifies the host itself.
IPv4	See Internet Protocol version 4 .
IPv6	See Internet Protocol version 6 .
ISDN	integrated services digital network
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
IVR	See interactive voice response .
Internet Protocol version 4 (IPv4)	The current version of the Internet Protocol (IP). IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each IPv4 address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.
Internet Protocol version 6 (IPv6)	An update version of IPv4, which is designed by the Internet Engineering Task Force (IETF) and is also called IP Next Generation (IPng). It is a new version of the Internet Protocol. The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits.
identity (ID)	The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.
initiate a multipoint conference	To initiate a multipoint conference by making calls from the video terminal or by using the Multipoint Control Unit (MCU) or the resource manager of the videoconferencing system. A multipoint conference contains at least two sites.
interactive voice response (IVR)	A telephone-based value-added voice service. Telephone users can dial a number specified by a carrier, and then follow the instructions to listen to, demand, and send voice information as required, or participate in interactive services, such as chats and making friends.
L	
LAN	See local area network .
LCD	liquid crystal display
LDAP	See Lightweight Directory Access Protocol .
LED	light emitting diode
Lightweight Directory Access Protocol	A network protocol based on TCP/IP, which allows access to a directory system agent (DSA). It involves some reduced functionality from X.500 Directory Access

(LDAP)	Protocol (DAP) specifications.
license	A permission that the vendor provides for the user with a specific function, capacity, and duration of a product. A license can be a file or a serial number. Usually the license consists of encrypted codes. The operation authority granted varies with the level of the license.
license file	The license file is an authorization for the capacity, functions, and validity period of the installed software. The license file is a .dat file that is generated using the special encryption tool according to the contract, and is delivered electronically. The customer needs to load the license on the device or software before the functions supported by the license are applicable.
local area network (LAN)	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building, featuring high speed and low error rate. Current LANs are generally based on switched Ethernet or Wi-Fi technology and run at 1,000 Mbit/s (that is, 1 Gbit/s).
local time	Display time of a local computer, which varies according to the time zone.
loopback test	The terminal can transmit audio or video data on a channel to simulate the actual application and test whether the output is satisfactory. A user can perform a local loopback test to check the local network connection or a remote loopback test to check the remote network connection. If a remote loopback test is performed, data is transmitted from the local site to a remote site, and then back to the local site.
M	
MAC address	A link layer address or physical address. It is six bytes long.
MCU	See multipoint control unit .
MD5	See message digest algorithm 5 .
MTU	See maximum transmission unit .
maximum transmission unit (MTU)	The largest packet of data that can be transmitted on a network. MTU size varies, depending on the network—576 bytes on X.25 networks, for example, 1500 bytes on Ethernet, and 17,914 bytes on 16 Mbit/s token ring. Responsibility for determining the size of the MTU lies with the link layer of the network. When packets are transmitted across networks, the path MTU, or PMTU, represents the smallest packet size (the one that all networks can transmit without breaking up the packet) among the networks involved.
message digest algorithm 5 (MD5)	A hash function that is used in a variety of security applications to check message integrity. MD5 processes a variable-length message into a fixed-length output of 128 bits. It breaks up an input message into 512-bit blocks (sixteen 32-bit little-endian integers). After a series of processing, the output consists of four 32-bit words, which are then cascaded into a 128-bit hash number.
multipoint call	A site makes calls to multiple sites, to hold a conference that has multiple participants.
multipoint control unit (MCU)	Data connection equipment used in a videoconferencing system. An MCU is used for terminal access, video exchange, audio mixing, data processing, and signaling exchange.

N

NAT	See Network Address Translation .
NTP	Network Time Protocol
Network Address Translation (NAT)	An IETF standard that allows an organization to present itself to the Internet with far fewer IP addresses than there are nodes on its internal network. The NAT technology, which is implemented in a router, firewall or PC, converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of them via internal tables that it builds. When packets come back from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine.
network layer	Layer 3 of the seven-layer OSI model of computer networking. The network layer provides routing and addressing so that two terminal systems are interconnected. In addition, the network layer provides congestion control and traffic control. In the TCP/IP protocol suite, the functions of the network layer are specified and implemented by IP protocols. Therefore, the network layer is also called IP layer.

O

optical fiber	A thin filament of glass or other transparent material, through which a signal-encoded light beam may be transmitted using total internal reflection.
----------------------	---

P

PIP	See Picture in Picture .
PPPoE	Point-to-Point Protocol over Ethernet
PSTN	See public switched telephone network .
PiP	Picture in Picture
Picture in Picture (PIP)	The Picture in Picture (PIP) service enables users to view an additional video in an overlay window.
password	A sequence of characters used to prove one's identity. It is used during a login process and should be highly protected.
ping	A method used to test whether a device in the IP network is reachable according to the sent ICMP Echo messages and received response messages.
point-to-point call	A site makes a call to another site, to hold a conference that has two participants.
presentation	During a conference, the local site shares the content input from a computer with remote sites, such as an excel file, a diagram, or slides.
public switched telephone network (PSTN)	A telecommunications network established to perform telephone services for the public subscribers. Sometimes it is called POTS.

Q

QoS	See quality of service .
quality of service (QoS)	A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

R

RAS	See Registration Admission and Status .
RS232	See Recommended Standard 232 .
RS422	The specification that defines the electrical characteristics of balanced voltage digital interface circuits. The interface can change to RS232 via the hardware jumper and others are the same as RS232.
RSE	Recording & Streaming Engine
RTCP	See Real-Time Transport Control Protocol .
RTP	real-time performance
Real-Time Transport Control Protocol (RTCP)	A protocol used to monitor data delivery. RTCP enables the receiver to detect if there is any packet loss and to compensate for any delay jitter.
Recommended Standard 232 (RS232)	A standard that defines the electrical characteristics, timing, and meaning of signals, and the physical size and pinout of connectors.
Registration Admission and Status (RAS)	A signaling set used for the connection between an H.323 gatekeeper and endpoints, and endpoint management.
route	The path that network traffic takes from its source to its destination. Routes can change dynamically.

S

SD	See standard definition .
SDI	See serial digital interface .
SHA	See secure hash algorithm .
SIF	Source Input Format
SIP	Session Initiation Protocol
SMC	service management center
SNMP	See Simple Network Management Protocol .

SNTP	See Simple Network Time Protocol .
SPL	sound pressure level
SRTP	See Secure Real-time Transport Protocol .
SSH	See Secure Shell .
SSID	service set identifier
SSL	See Secure Sockets Layer .
SVGA	Super Video Graphics Array
Secure Real-time Transport Protocol (SRTP)	A real time transport protocol with enhanced security and encryption mechanism-based RTP.
Secure Shell (SSH)	A set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. A feature to protect information and provide powerful authentication function for a network when a user logs in to the network through an insecure network. It prevents IP addresses from being deceived and simple passwords from being captured.
Secure Sockets Layer (SSL)	A security protocol that works at a socket level. This layer exists between the TCP layer and the application layer to encrypt/decode data and authenticate concerned entities.
Simple Network Management Protocol (SNMP)	A network management protocol of TCP/IP. It enables remote users to view and modify the management information of a network element. This protocol ensures the transmission of management information between any two points. The polling mechanism is adopted to provide basic function sets. According to SNMP, agents, which can be hardware as well as software, can monitor the activities of various devices on the network and report these activities to the network console workstation. Control information about each device is maintained by a management information block.
Simple Network Time Protocol (SNTP)	A protocol that is adapted from the Network Time Protocol (NTP) and synchronizes the clocks of computers over the Internet.
secure hash algorithm (SHA)	A technique that computes a 160-bit condensed representation of a message or data file, called a message digest. The SHA is used by the sender and the receiver of a message in computing and verifying a digital signature, for security purposes.
security	Protection of a computer system and its data from harm or loss. A major focus of computer security, especially on systems accessed by many people or through communication lines, is preventing system access by unauthorized individuals.
serial digital interface (SDI)	An interface that transmits data in a single channel in sequence.
serial port	An input/output location (channel) that sends and receives data to and from a computer's CPU or a communications device one bit at a time. Serial ports are used for serial data communication and as interfaces with some peripheral devices, such as mice and printers.
site	A group of IP systems with IP connectivity, which can be achieved independent of SP networks.
sleep mode	A mode that the telepresence system enters if no operation is performed on the touch

	panel for a preset period of time.
standard definition (SD)	A video format with the resolution below 720p.
subnet mask	The technique used by the IP protocol to determine which network segment packets are destined for. The subnet mask is a binary pattern that is stored in the device and is matched with the IP address.
T	
T1	A North American standard for high-speed data transmission at 1.544Mbps. It provides 24 x 64 kbit/s channels.
TCP	See Transmission Control Protocol .
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporary Key Integrity Protocol
TLS	Transport Layer Security
Telnet	A standard terminal emulation protocol in the TCP/IP protocol stack. Telnet allows users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
Transmission Control Protocol (TCP)	The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.
time zone	A division of the earth's surface, usually extending across 15° of longitude devised such that the standard time is the time at a meridian at the center of the zone.
touch panel	The touch panel is connected to the telepresence system wirelessly. Without cable restriction, users can use the touch panel conveniently. From the touch panel, users can perform operations, such as dialing a number, calling a contact, answering or rejecting a call, controlling a conference, and switching the display mode.
U	
UDP	See User Datagram Protocol .
UI	user interface
URI	See uniform resource identifier .
URL	See uniform resource locator .
USB	See Universal Serial Bus .
UTC	Coordinated Universal Time
Universal Serial Bus (USB)	A serial bus standard to interface devices. It was designed for computers such as PCs and the Apple Macintosh, but its popularity has prompted it to also become commonplace on video game consoles and PDAs.

User Datagram Protocol (UDP)	A TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. UDP uses IP to deliver datagrams. UDP provides application programs with the unreliable connectionless packet delivery service. That is, UDP messages may be lost, duplicated, delayed, or delivered out of order. The destination device does not actively confirm whether the correct data packet is received.
uniform resource identifier (URI)	A uniform resource identifier (URI) is a member of this universal set of names in registered namespaces and addresses referring to registered protocols or namespaces. URI is used to locate available resources on the Web, including HTML documents, images, video clips, and programs.
uniform resource locator (URL)	An address that uniquely identifies a location on the Internet. A URL is usually preceded by http://, as in http://www.microsoft.com. A URL can contain more details, such as the name of a hypertext page, often with the file name extension .html or .htm.
V	
VGA	video graphics array
VLAN	virtual local area network
VoIP	See Voice over Internet Protocol .
Voice over Internet Protocol (VoIP)	A value-added service technology for IP calls. The VoIP service is a new IP telecom service. It can run on fixed and mobile networks and support flexible access points. Fees for VoIP subscribers are relatively low. Calls between VoIP subscribers who belong to the same carrier are free of charge.
W	
WAN	wide area network
WLAN	See wireless local area network .
WPA	See Wi-Fi Protected Access .
WPA-PSK	Wi-Fi protected access pre-shared key
Wi-Fi	See Wireless Fidelity .
Wi-Fi Protected Access (WPA)	A wireless security protocol replacing WEP and aiming to provide more powerful security performance for the IEEE 802.11 WLAN. WPA is a subset of IEEE 802.11i, whose core is IEEE 802.1x and TKIP.
Wireless Fidelity (Wi-Fi)	A short-distant wireless transmission technology. It enables wireless access to the Internet within a range of hundreds of feet wide.
wireless local area network (WLAN)	A hybrid of the computer network and the wireless communication technology. It uses wireless multiple address channels as transmission media and carries out data interaction through electromagnetic wave to implement the functions of the traditional LAN.

X

XGA Extended Graphics Array