eLTE5.0 eAPP610 V100R005C00

Product Description(3GPP)

Issue	02
Date	2018-03-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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://www.huawei.com

Email: support@huawei.com

Contents

1 Positioning and Highlights

About This Chapter

This chapter introduces the background information and main features of the eAPP610.

3GPP-MC series standards are a new public safety standard framework for enabling mission-critical communication (including voice, video, and data services). They are collaboratively formulated by trunking communication standards organizations, government regulatory bodies, and operators based on LTE and 3GPP-compliant network evolution. 3GPP-MC is short for Third Generation Partnership Project Mission Critical.

This section describes the product positioning of the eAPP610.

This section describes the product highlights of the eAPP610.

1.1 Product Positioning

This section describes the product positioning of the eAPP610.

The eAPP610 can be used in various industries (such as the public security, transportation, and energy industries) by providing dispatching functions for multimedia services (such as voice, data, and video).

1.2 Product Highlights

This section describes the product highlights of the eAPP610.

The eAPP610 features the following:

- Multimedia dispatching: Voice, Push to Talk (PTT), video, images, and text are supported to apply to different application scenarios.
- Converged communications: Voice calls, video calls, Short Message Service (SMSs), and location services between trunking users and Push-to-talk over Cellular (PoC) users

are provided, along with support for joint groups and traversal between enterprise and public networks.

- Ease of deployment: All terminals in the eAPP system can be remotely configured and all user permission policies are managed on the eUDC in a centralized manner.
- User-friendly GUI: Operations are performed by only clicking or dragging on the Graphical User Interface (GUI) using the mouse, and multiple languages are supported.
- High reliability: Core devices, such as the eMDC and eNodeB, can adopt dual-host backup to escape a network-wide breakdown in case of a single-host failure, providing high reliability communications.
- High scalability: eAPP610s can be cascaded or a larger-capacity eAPP610 can be selected to accommodate extended user quantity.
- Ample communication modes: The eAPP610 can interwork with a wide variety of networks and devices such as Public Switched Telephone Network (PSTN), Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), Universal Mobile Telecommunications System (UMTS), Terrestrial Trunked Radio (TETRA), MT1327, and satellite networks and devices.
- Various secondary development interfaces: Interfaces to upper-layer applications are provided for smooth application migration or low-cost development of new applications by customers and partners.

2 Product Functions

About This Chapter

This section introduces the devices in the eAPP610 and their functions.

Figure 3-1 shows an eAPP610 in an LTE wireless trunking system.

Figure 2-1 Position of the eAPP610 in the network

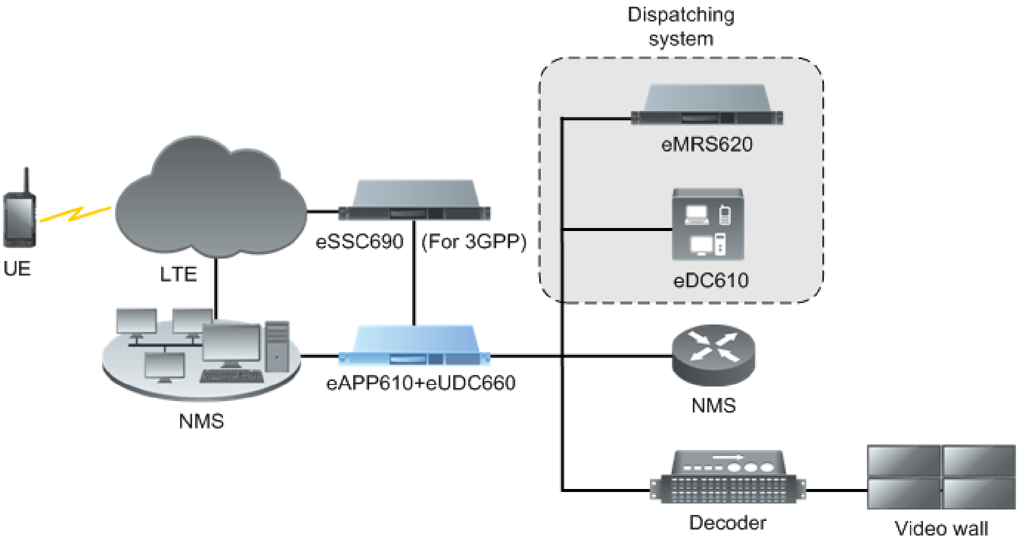


Table 3-1 lists the functions of the eAPP610 and other devices in the wireless trunking system.

Table 2-1 eAPP610 and other devices in the wireless trunking system

NE Name	Function
LTE	LTE: indicates the LTE network, including eNodeBs and the core network. The eNodeB must support Multimedia Broadcast multicast service Single Frequency Network (MBSFN). The core network consists of the MME, S-GW, P-GW, HSS, PCRF, MBMS-GW, MCE, and

NE Name	Function
	BM-SC.
UE	A UE can be a handheld UE or a non-handheld UE.
Network management system	The system equipment is managed by two NMSs. The U2000 manages eNodeBs and core network devices. The eOMC910 manages the eUDC660, eAPP610, eMRS620, and broadband access terminals.
eUDC660	The Enterprise User And Device Controller (eUDC) is a user device management platform.
eAPP610	eMDC (Enterprise Multimedia Dispatching and processing Center) is a core device of the eAPP610. It controls all services and processes media flows. **NOTE** Currently, the eUDC660 and eAPP610 are deployed on the same server.
eMRS620	The Enterprise Multimedia Recording and playback Server (eMRS) is a multimedia recording and playback server that provides media recording, on-demand services, and management functions, and processes camera access. **NOTE** Based on the network scale, the eMRS620 can be co-deployed with the eAPP610, or be deployed alone.
eSSC690	The Enterprise SIP Signalling Core (eSSC), the exclusive SIP signaling core device in 3GPP networking mode, provides the SIP proxy function. **NOTE** Based on the network scale, the eSSC690 can be co-deployed with the eAPP610, or be deployed alone.
eDC610	The Enterprise Dispatching Console (eDC) is the dispatching console, providing interface-based management for services including voice, video, SMS, MMS, and Geographic Information System (GIS) services.
Interconnection gateway	Interconnection gateways include: • PLMN gateway: provides access to the Public Land Mobile Network (PLMN) to implement interworking of the eAPP610 with the PLMN. • PSTN gateway: provides access to the Public Switched Telephone Network (PSTN) to implement interworking of the eAPP610 with the PSTN. • TETRA gateway: provides access to other trunking networks to implement interworking of the eAPP610 with other Terrestrial Trunked Radio (TETRA) networks. • eUPG670: As a unified narrowband gateway developed on the eAPP610 software platform, it implements interconnection with narrowband systems, such as TETRA, and provides voice group call and group selection functions.

NE Name	Function
Decoder	The decoder is a device connecting the dispatching system and the video wall, decoding video and audio files and providing support for large video wall decoding services.

3.1 Voice Trunking Services

This section describes the voice trunking services of the eAPP system.

3.2 Video and Data Services

This section describes the video and data services of the dispatching system.

2.1 Voice Trunking Services

This section describes the voice trunking services of the eAPP system.

Table 3-2 describes voice trunking services provided by the eAPP system.

Table 2-2 Voice trunking services

Service	Description
P2P call	Point-to-point (P2P) calls, or private calls, can be made between trunking users or between a trunking user and a dispatcher. There are two modes for P2P calls: • Full-duplex communications: Only the two parties who participate in the P2P call can hear each other. Both parties can speak at the same time. • Half-duplex communications: Only the two parties who participate in the P2P call can hear each other. Only one party can speak at a time, and the other party can only listen. Half-duplex communications are not supported in the NAT scenario.
Group call	Group calls are made between several mobile stations or between mobile stations and an eDC610. Group calls are half-duplex point-to-multipoint (P2MP) communications.
Emergency call	Emergency calls are special calls with the highest priority, allowing information to reach the called party within the shortest time.
Group scan	Group scan is used to search for groups for listening.
Floor preemption	During a group call, a higher-priority user can get the call floor from a lower-priority user. The priority of the floor varies with the priority of the user. A high-priority user can always get the call floor.
Later entry	This feature allows delayed participation into a group call for members that fail to participate when the call is initiated.

Service	Description
Forced call release by the eDC610	An authorized eDC610 can release a P2P call or a group call.
Time-limited call	The duration of a floor in a group call, a P2P call, or a call connected to a PSTN user is configurable.
Broadcast call	Static broadcast call configuration is supported. Listening users in a broadcast call cannot preempt the floor.
Incoming/Outgoing call barring	Incoming calls or outgoing calls (including the interworking gateway numbers) made to or from a user can be barred. Incoming/Outgoing call barring affects only P2P calls.
Interconnection and interworking of different systems	Users in an enterprise network can perform P2P calls with PSTN/PBX users and PLMN users, and group calls with TETRA users and external 350 MHz ultra short wave stations.
Dynamic regrouping	An eDC610 user may create a dynamic group of selected static groups and users. The dynamic group is allowed with infinite calling times. Dynamic groups are open to query, modification and deletion.
Temporary group	A dispatcher can create a temporary group of selected users. The temporary group is automatically deleted when the call is ended.
Ambience listening	A dispatcher authorized with ambience listening can, bypassing a terminal, open the terminal mic and transfer the voice to the network. There is no visual, audio or vibration prompt displayed on the screen of the target terminal. When the terminal processes audio/video service, the ambience listening is stopped automatically.
Console patching	A dispatcher can combine multiple static groups into a patch group.
Attendant forwarding	After user A establishes a P2P call with the eDC610, a dispatcher can use the attendant forwarding feature to establish a call between user A and user B directly.
Call forwarding	This feature can forward a P2P call for a user to another one before the user answers the call.
Multiple calls on-hold	An eDC610 can receive multiple common P2P calls concurrently. The dispatcher can answer any call as required.

2.2 Video and Data Services

This section describes the video and data services of the dispatching system.

Table 3-3 shows the video and data services of the dispatching system.

Table 2-3 Video and data services

Service	Description
Video surveillance	A dispatcher can observe HD video uploaded by fixed cameras and handheld terminals on an eDC610 to monitor persons and devices in real time.
Video uploading from handheld terminals	HD and SD video can be uploaded by handheld terminals to an eDC610. Emergency video upload and one-button video upload are supported.
Video distribution	A dispatcher can distribute video uploaded to an eDC610 to one or more specified display entities, such as another eDC610, a handheld terminal, and a decoder. The video can be played with the sound or without the sound on these display entities.
Video collaboration	Concurrency of video services and trunking voice services is supported.
P2P video call	A handheld terminal can make a P2P video call to another handheld terminal to achieve face-to-face communication with the front cameras built in the handheld terminals.
GIS	A mobile terminal can report GIS information to an eDC610 on which a dispatcher can locate the mobile terminal in the GIS map. The period for reporting GIS information is configurable. The system provides an offline GIS map and supports the ArcGIS map that uses TPK or MPK data.
Tracing and playback	A dispatcher can specify a terminal for real-time tracing. A traced terminal reports its GPS location information in real time. The eDC610 can display all GPS locations of traced terminals after automatic tracing is enabled. This feature enables a user to query the GPS data of a terminal within a specified period and play back the terminal's track on the GIS map.
Circling terminals	A dispatcher can circle a certain range on the map and initiate a group call to all terminals within this circle.
Video transcoding	High-resolution video streams can be converted to low-resolution video streams in real time. Distribution of video after being transcoded is supported.
Video adaptation	This feature supports uplink adaptation for the video services of handheld terminals. When the video service is at the edge of a cell or in an area with weak signals, this feature adjusts parameters, such as the bit rate and frame rate, to ensure video quality and avoid black screens.
SMS	SMs can be made by a terminal user or an eDC610 user to another terminal user or another eDC610 user, or to the group to which another terminal user or another eDC610 user belongs.
Status SMS	Status information can be predefined. The eDC610 can receive status information from terminal users.

Service	Description
MMS	Point-to-point or point-to-group MMSs are available between terminal users, between the eDC610 and terminal users, and between eDC610s. A multimedia message can include text, graph, and voice information. One-button picture upload is supported.

3 Introduction to the eAPP610

About This Chapter

This section introduces the structure, specifications and metrics of eAPP610.

4.1 Product Structure

This section describes the physical structure of the eAPP610.

4.2 Technical Specifications

This section describes specifications of the eAPP610.

3.1 Product Structure

This section describes the physical structure of the eAPP610.

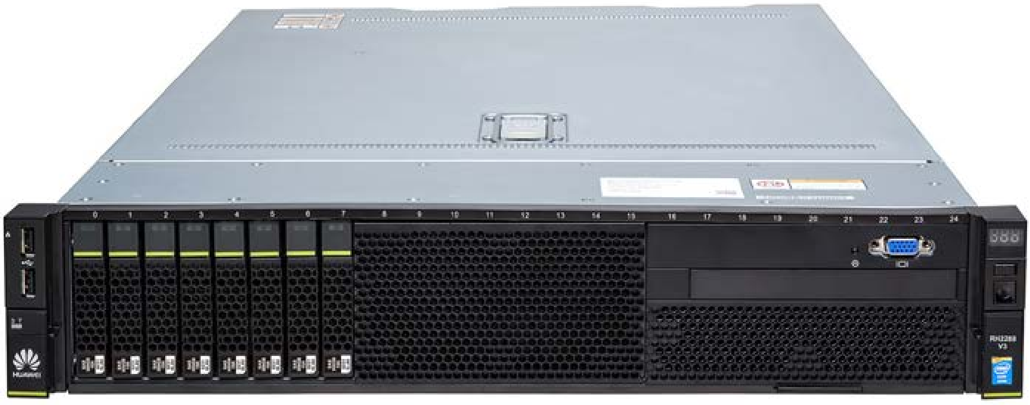
The eAPP610 uses a Huawei RH2288H V3 (large-sized) server.

The Huawei RH2288H V3 (large-sized) server, as shown in Figure 4-1, uses five 1200-GB hard disks. For details, see the third-party device document *eAPP_Server_Tecal_RH2288H V3_User Guide*.

NOTE

- When the eMRS620 is deployed independently, it must be deployed on a Huawei RH2288H V3 (large-sized) server and uses twelve 4-TB hard disks.
- When the eSSC690 is deployed independently, it must be deployed on a Huawei RH2288H V3 (large-sized) server and uses five 1200-GB hard disks.

Figure 3-1 Exterior of the Huawei RH2288H V3 (large-sized) server



3.2 Technical Specifications

This section describes specifications of the eAPP610.

Specifications of the Huawei Tecal RH2288H V3 Server

Mechanical Specifications	
Form	2 U rack server
Dimensions (H x W x D)	86.1 mm × 447 mm × 708 mm
Weight	About 27 kg
Electrical Specifications	
Working voltage	100 V AC to 240 V AC
Power	• Large-sized server: < 481 W • Medium-sized server: < 224 W
Hardware Configuration	
Processor	• Large-sized server: 2 x X86 series-2600MHz-1.8V-64bit-145000mW -Haswell EP Xeon E5-2697 v3-14Core-with heatsink CPU • Medium-sized server: 2 x X86 series-2400MHz-1.8V-64bit-85000mW-Haswell EP Xeon E5-2620 v3-6Core-with heatsink CPU
Chipset	Intel C610
Memory	• Large-sized server: 64 GB • Medium-sized server: 32 GB

Storage	• Large-sized server: 5 x 1200 GB hard disks • Medium-sized server: 4 x 600 GB hard disks
Network port	• Large-sized server: – 2 x 10 GE – 4 x GE • Medium-sized server: 4 x GE
Port	• Front panel – 2 x USB 2.0 – 1 x DB-15 video port • Rear panel – 2 x USB 3.0 – 1 x DB-15 VGA – 1 x DB-9 serial port – 1 x RJ-45 system management port • Built-in ports – 1 x USB 3.0 – 2 x Mini SSD hard disk (SATA DOM) ports – 1 x dual-SD port (for the embedded system management program) or 1 x built-in SD card for the BMC management system
Fan	Four hot-swappable counter-rotating fans, supporting fan redundancy
Power module	Two hot-swappable 1+1 redundant PSUs, 750 W AC
System management	• UEFI • Huawei iMana, supporting IPMI, SOL, KVM over IP, and virtual media, and providing one 10/100/1000 Mbit/s RJ45 management network port • Supporting network connectivity status indicators (NCSIs)
Security	• Power-on password • Administrator password • TPM • Chassis cover opening event recording • Front bezel
Video card	The mainboard integrates a display chip, providing 32 MB video memory and supporting up to 1920x1200 resolution at 60

	Hz in 16 M colors.
Operating system	SUSE Linux Enterprise Server 11 SP3

Capacity Specification

Table 4-1 describes the capacity counters of the eAPP610.

Table 3-1 eAPP610 capacity counters

Category	Item	Value
User or group registration	Number of registered (online) users	[0,100000]
	Number of registered (online) groups	[0,10000]
	Number of dynamic group members	Each dynamic group supports up to 8 groups, 200 individual users, and 250 wired users. The total number of users must not exceed 4000.
	Number of patch groups	100
	Number of patch group members	A maximum of 20 static groups subscribed by the eAPP610 are supported.
	Number of static groups	Each static group supports up to 250 wired users.
	Number of temporary groups	Each temporary group supports up to 8 groups, 64 individual users, and 16 wired users. The total number of users must not exceed 1000.
Voice service	Maximum number of concurrent voice services **NOTE** The concurrent video capability can be extended to the concurrent voice capability based on the ratio of 1:1. If there is no video service, the number of concurrent voice services doubles.	Voice + video ≤ 4000 x 2
Video service	Maximum number of concurrent video services (D1) **NOTE** The resource consumption ratio of the video service is	2000

Category	Item	Value
	1080P:720P:D1:CIF:QCIF (that is, 4:2:1:0.5:0.5).	
	Maximum number of channels to which a video source can be distributed	16
	Number of concurrent upload and surveillance channels of a video source	10
Transcoding service	Maximum number of concurrent voice transcoding channels (AMR<->G.711)	90
	Maximum number of concurrent video transcoding channels (D1 -> CIF) **NOTE** Maximum number of concurrent video transcoding channels refers to the maximum number of channels of video sources for transcoding. Video transcoding resource consumption ratio is (1080P->CIF):(720P->CIF):(D1->CIF) (that is, 4:2:1).	4
Video input and output	Fixed camera concurrent access capability (D1) **NOTE** The fixed camera access function is integrated on the eMRS620.	N/A
	Video projection capability	256
SMS/MMS	Maximum time for saving an offline SM	48 hours
	Minimum number of offline SMs that can be stored	5000
	Maximum number of concurrent SMs	50 pieces/s
	Maximum data volume per MMS message attachment	20 MB
	Maximum number of	20 pieces/s

Category	Item	Value
	concurrent MMs	
GIS service	Maximum number of terminals concurrently performing GIS services (period: 60s) **NOTE** Conversion formula for the report period of other services: Number of terminals carrying concurrent GIS services = Number of terminals carrying concurrent GIS services (period: 60s) x Report period/60 For example: Number of terminals carrying concurrent GIS services (period: 30s) = Number of terminals carrying concurrent GIS services (period: 60s) x 30/60	30,000
	Delay from the GIS terminal to the server (second)	2
	Maximum period for saving GIS data (day)	30
eDC610	Maximum number of GIS terminals subscribed to one eDC610	1000
	Maximum number of eDC610 accesses	200
Fixed camera	Maximum number of registered fixed cameras	10,000
	Maximum number of fixed cameras for polling	16
	Switch time of fixed cameras for polling	30s
Number of TMGI resources		200

When the eAPP610 is used for user plane expansion, the transcoding and service concurrency deliver better performance. Table 4-2 describes related counters.

Table 3-2 Capacity counters of the eAPP610 (for user plane expansion)

Item	Value

Item	Value
Maximum number of concurrent video transcoding channels (D1 -> CIF) **NOTE** This counter is applicable only to video transcoding and does not improve other capabilities of the eAPP610.	- H.264 D1->CIF: 72 - H.265 D1->CIF: 64
Maximum number of concurrent voice transcoding channels (AMR<->G.711) **NOTE** This counter is applicable only to voice transcoding and does not improve other capabilities of the eAPP610.	720

NOTE

When *N* eAPP610s are added to improve the service concurrency, the new concurrency capability for voice and video services is (1 + *N*) x original capability (including the transcoding capability). Up to three eAPP610s can be added to improve the transcoding capability and up to two eAPP610s can be added to improve the service concurrency capability.

The server supports the improvement of both the service concurrency and transcoding capabilities, and at most five eAPP610s are allowed in the network after the expansion.

4 Decoders

About This Chapter

This section introduces the product structure, functions and specifications of all the decoders used in the Dispatching System. The decoders in use are HIKVISION **DS-6308D-T**, **DS-6400HD-T** and **DS-6400HD-T-JX** series.

5.1 DS-6308D-T

This section describes the product structure, product functions, and product specifications of the DS-6308D-T decoder.

5.2 DS-6400HD-T

This section describes the product structure, product functions, and product specifications of the DS-6400HD-T series decoder.

5.3 DS-6400HD-T-JX

This section describes the structure, functions, and specifications of DS-6400HD-T-JX series decoders.

4.1 DS-6308D-T

This section describes the product structure, product functions, and product specifications of the DS-6308D-T decoder.

4.1.1 Product Structure

This section describes the appearance of the DS-6308D-T decoder.

Figure 5-1 shows the appearance of the **DS-6308D-T** decoder.

Figure 4-1 Appearance of the DS-6308D-T decoder

4.1.2 Product Functions

This section describes the functions of the DS-6308D-T decoder.

Functions of the **DS-6308D-T** decoder are as follows:

- Supports adding intelligent analysis information of the front-end encoder to the decoded images.
- Supports Video Graphic Array (VGA) and British Naval Connector (BNC) outputs. **DS-6308D-T** is capable of decoding 16 streams at CIF/8 streams at 4CIF/4 streams at 720p, where the first VGA output supports 1/2/4/9/16 multi-camera display and other VGA outputs and BNC outputs support 1/2/4 multi-camera display.
- Supports active decoding and passive decoding.
- Supports receiving real-time data in the manner of direct access to the front-end device or stream media forwarding.
- Supports decoding and outputting of remote recording files.
- Supports transparent channel transmission and remote control on Pan Tile Zoom (PTZ) connected to the Digital Video System (DVS) or Digital Video Recorder (DVR).

4.1.3 Product Specifications

This section describes the product specifications of the DS-6308D-T decoder.

Model		**DS-6308D-T**
Audio/video output	BNC output	8 channels, BNC port, resolution: PAL standard 704×576, NTSC standard 704×480
	VGA output	4 channels, resolution 1280×1024 @ 60 Hz, 1280×720 @ 60 Hz, 1024×768 @ 60 Hz

Model		**DS-6308D-T**
	Audio output	12 channels, BNC port (linear level, Resistance: 600 Ω)
Audio/video decoding parameter	Video decoding capability	16 streams at CIF (Common Intermediate Format)/8 streams at 4CIF/4 streams at 720P
External ports	Voice input	One BNC port (level: 2.0Vp-p; Resistance: 1000 Ω)
	Voice output	One BNC port (linear level, Resistance: 600 Ω)
	Network port	One RJ45 port, 10 Mbit/s/100 Mbit/s/1000 Mbit/s self-adaptive network port
	Serial port	One standard RS-485 serial port
		One standard RS-232 serial port
	Alarm input	4 channels
	Alarm output	4 channels
Others	Power supply	AC 220V
	Power consumption	≤ 50W
	Operating temperature	-10°C to +55°C
	Humidity	10% to 90%
	Chassis	19 inch and 1U high
	Dimensions (length × depth × height)	440 mm × 300 mm × 45 mm
	Weight	≤ 5.20 kg

4.2 DS-6400HD-T

This section describes the product structure, product functions, and product specifications of the DS-6400HD-T series decoder.

Designed for the high-definition video monitoring system, **DS-6401HDI-T** series HD video/audio decoder is developed on the basis of TI platform, Linux operating system and Netra processor, ensuring high reliability and stability of system running.

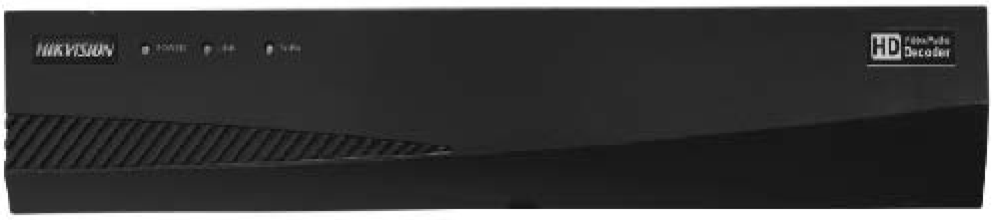
DS-6401HDI-T series HD video/audio decoder is capable of decoding video at 5MP resolution and outputting decoded video via BNC, VGA and HDMI interfaces, and it also supports multiple-protocol and multiple-stream transmission mode. The decoded video can be displayed on video wall or large screen.

4.2.1 Product Structure

This section describes the appearance of the DS-6400HD-T series decoder.

Figure 5-2 shows the appearance of the **DS-6400HD-T** series decoder.

Figure 4-2 Appearance of the DS-6400HD-T series decoder



4.2.2 Product Functions

This section describes the functions of the DS-6400HD-T series decoder.

Functions of the **DS-6400HD-T** series decoder are as follows:

- Supports adding intelligent analysis information of the front-end encoder to the decoded images.
- Supports High Definition Multimedia Interface (HDMI), VGA, and BNC outputs.
- The image resolution of HDMI outputs is up to 1920 × 1080 and the image resolution of VGA is up to 1280 × 1024.
- Supports decoding 4 channels of video stream at 1080p resolution, 8 channels of video at 720p resolution and 16 channels of video at 4CIF resolution.
- Supports active decoding and passive decoding.
- Supports receiving real-time data with direct access to the front-end device or stream media forwarding.
- Supports decoding and outputting of remote recording files.
- Supports transparent channel transmission and remote control on PTZ connecting to the DVS or DVR.

4.2.3 Product Specifications

This section describes the product specifications of DS-6400HD-T series decoders.

Model	DS-6401HD-T	
Audio/Video output	VGA output	One channel, resolution:

Model	**DS-6401HD-T**	
		1280x720@60 Hz, 1280x1024@60 Hz, 1024x768@60 Hz
	HDMI output	One channel, resolution: 1600x1200@60 Hz, 1920x1080 (1080p)@60 Hz, 1920x1080 (1080p)@50 Hz, 1280x720@60 Hz, 1280x1024 @60 Hz, 1024x768@60 Hz
	Audio output	One channel, RCA port
	Decoding capability	Four channels of 1080p video services/Eight channels of 720p video services/16 channels of 4CIF video services or services with a lower resolution
	Number of displayed images	1/4/9/16
	Network port	One RJ45 port, a self-adaptive Ethernet port supporting 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s
	Serial port	One standard RS485 serial port
		One standard RS232 serial port
	Alarm input	Four channels
	Alarm output	Two channels
Others	Power supply	12 V DC
	Power consumption	≤ 15 W
	Operating temperature	–10°C to +55°C
	Operating humidity	10% to 90%
	Dimensions (W x D x H)	220 mm x 148 mm x 45 mm
	Weight	≤ 1.12 kg

4.3 DS-6400HD-T-JX

This section describes the structure, functions, and specifications of DS-6400HD-T-JX series decoders.

DS-6400HD-T-JX series decoders are rack-mounted HD video/audio decoders, providing a strong support for large-scale video wall decoding services. In compliance with the Advanced Telecommunications Computing Architecture (ATCA), DS-6400HD-T-JX series decoders are capable of:

- Decoding HD videos (with 5 MP or a lower resolution)
- Outputting videos over various ports
- Providing data transmission in compliance with multiple network transmission protocols and code streams

A DS-6400HD-T-JX decoder is composed of a single-chassis DS-6464-T and a video/audio output board DS-6408HD-T-B. A maximum of eight audio/video output boards (DS-6408HD-T-B) can be installed.

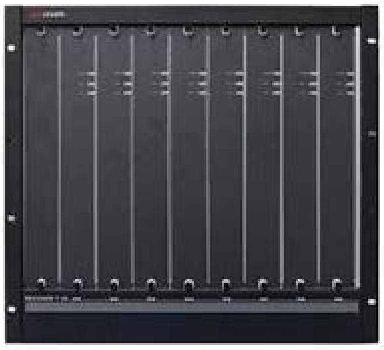
In this version, the DS-6432HD-T-JX (which has four decoder boards) and DS-6464HD-T-JX (which has eight decoder boards) are used.

4.3.1 Product Structure

This section describes the appearance of the DS-6400HD-T-JX series decoder.

Figure 5-3 shows the appearance of the **DS-6400HD-T-JX** series decoder.

Figure 4-3 Appearance of the DS-6400HD-T-JX series decoder



4.3.2 Product Functions

This section describes the functions of the DS-6400HD-T-JX series decoder.

- Hardware Architecture:
  - Standard rack design and carrier-class Advanced Telecom Computing Architecture (ATCA) cabinet system.
  - Pluggable modular design and a maximum of 8 video/audio output boards supported.
  - Duplicate power supply (optional) to ensure steady and reliable system operating.
- Video/Audio Output:

  - Video/Audio output over HDMI, VGA, Digital Visual Interface (DVI), and BNC ports.
  - Audio/Video decoding at a maximum of 1920 × 1080 resolution over HDMI and DVI ports.
- Video/Audio decode: Each video/audio output board decoding one channel of video at 1080p resolution, two channels of video at 720p resolution, or four channels of video at 4CIF resolution.
- Network Functions:
  - Receiving real-time data with direct access to the front-end device or stream media forwarding.
  - Each video/audio output board providing one 10/100/1000 Mbit/s adaptive Ethernet port.
- Video/Audio output board supporting restoration of factory settings by one-key.

4.3.3 Product Specifications

This section describes the product specifications of the DS-6400HD-T-JX series decoder.

Model	DS-6400HD-T-JX	
Service configurations	Chassis system	Chassis and power adapter.
	Video/Audio output board	A maximum of 8 video/audio output board supported
Video/Audio outputs (DS-6401HD-B board)	HDMI output	8 channels, resolution: 1600 × 1200@60 Hz, 1080p (1920 × 1080p)@60 Hz, 1080i (1920×1080i)@60 Hz, 1080p (1920 × 1080p)@50 Hz, 1080i (1920×1080i)@50 Hz, 1280 × 720@60 Hz, 1280 × 1024@60 Hz, 1024 × 768@60 Hz
	DVI output	8 channels, resolution: 1600 × 1200@60 Hz, 1080p (1920 × 1080p)@60 Hz, 1080i (1920×1080i)@60 Hz, 1080p (1920 × 1080p)@50 Hz, 1080i (1920×1080i)@50 Hz, 1280 × 720@60 Hz, 1280 × 1024@60 Hz, 1024 × 768@60 Hz
	VGA output	8 channels, resolution: 1600 × 1200@60 Hz, 1080p (1920 × 1080p)@60 Hz, 1080i (1920×1080i)@60 Hz, 1080p (1920 × 1080p)@50 Hz, 1080i

Model	DS-6400HD-T-JX	
		(1920×1080i)@50 Hz, 1280 × 720@60 Hz, 1280 × 1024@60 Hz, 1024 × 768@60 Hz
	Audio output	8 channels, one DB15 port
Video/Audio decoding parameters (DS-6401HD-B board)	Video decoding resolution	1080p, UXGA (Ultra extended Graphics Array), 720p, SXGA (Super extended Graphics Array), and 4CIF
	Video decoding capability	1 channel of 1080p/2 channels of 720p/4 channels of 4CIF
	Number of displayed images	1/4/9/16
External ports (DS-6401HD-B board)	Voice intercom input	1 channel, 3.5 mm audio port (level: 2.0Vp-p, resistance: 1 KΩ)
	Network port	One RJ45 10M/100M/1000M adaptive Ethernet port
	Serial port	One standard RS-232 serial port
Others	Power supply	AC 220 V
	Power consumption	≤ 350 W
	Operating temperature	-10°C to +50°C
	Humidity	10% to 90%
	Chassis	19 inch 6U chassis
	Dimensions (length × depth × height)	482.6 mm × 279.3 mm × 443.7 mm
	Weight	≤ 22 kg (full configuration)

5 Interworking Gateway

About This Chapter

This section describes the PSTN, PLMN, and TETRA gateways used by the eAPP610 to interwork with enterprise network gateways.

This section describes the product structure, and product specifications of the PLMN gateway.

This section describes the product structure, and product specifications of the PSTN gateway.

This section describes the product structure, and product specifications of the TETRA gateway.

5.1 PLMN Gateway

This section describes the product structure, and product specifications of the PLMN gateway.

PLMN gateway adopts the Dinstar **DWG2000F-8** series gateway or NICEUC **NC-MG320** wireless gateway.

DWG2000F-8 series gateway is a multi-functional GSM, CDMA, and Wideband Code Division Multiple Access (WCDMA) Voice over Internet Protocol (VoIP) product based on IP, which provides the GSM/CDMA/WCDMA network access functions. With the development of users and telecom service, mobile network and fixed network integration will be steadily increasing. **DWG2000F-8** series gateway provides high quality VoIP service which perfectly meets the requirement.

NC-MG320 wireless gateway can help operators, enterprises, Small Offices and Home Offices (SOHOs), and virtual operators achieve good and inexpensive VoIP solutions. As a full-featured IP-based VoIP gateway for GSM/CDMA/WCDMA wireless networks, **NC-MG320** provides stable network configuration, powerful functions, and good voice quality. This wireless gateway adopts the mainstream chip technology and supports E1, GSM/CDMA/WCDMA, Session Initiation Protocol (SIP), and IP Multimedia Subsystem (IMS) interfaces.

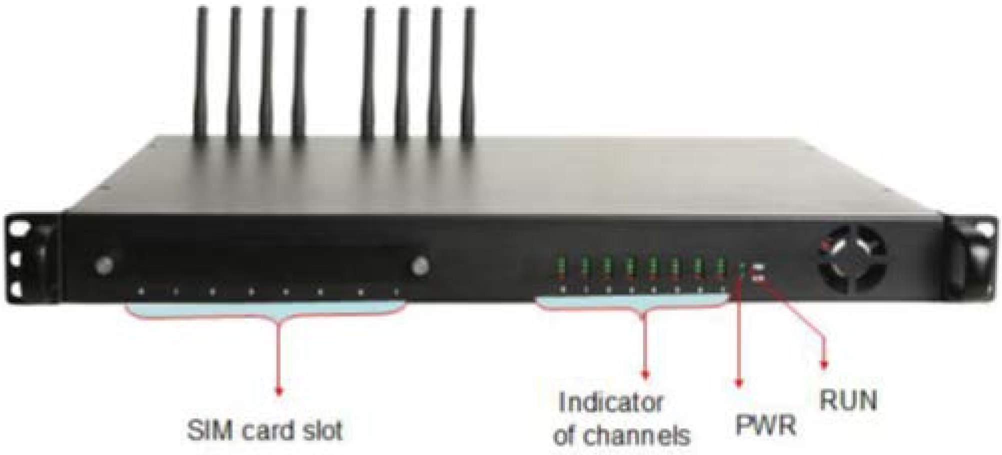
5.1.1 Product Structure

This section describes the front view and rear view of Dinstar DWG2000F-8 series gateway and NICEUC NC-MG320 wireless gateway.

Dinstar DWG2000F-8 series gateway

Figure 6-1 shows the front view of the Dinstar **DWG2000F-8** series gateway.

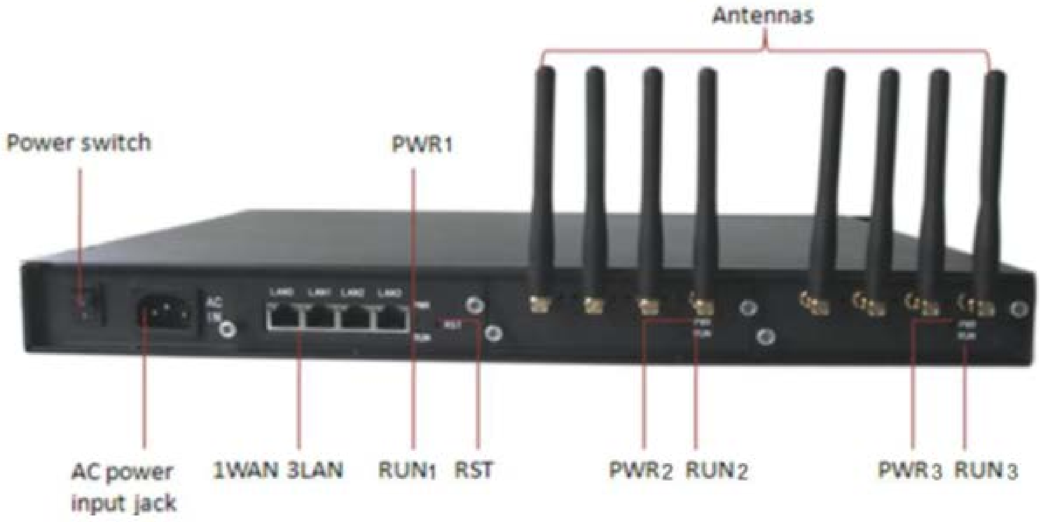
Figure 5-1 Front View of DWG2000F-8 series gateway



SIM Card Slot	SIM Card Slot
Indicator of Channels	• Red: Bright is using, not bright is not using • Green: Signal Strength of GSM/CDMA/WCDMA
PWR	Power Status of Device
RUN	Operating status: slow flash indicates no registration, flash indicates registration, no flash indicates initialization, not bright indicates no running

Figure 6-2 shows the rear view of the Dinstar **DWG2000F-8** series gateway.

Figure 5-2 Rear View of DWG2000F-8 series gateway

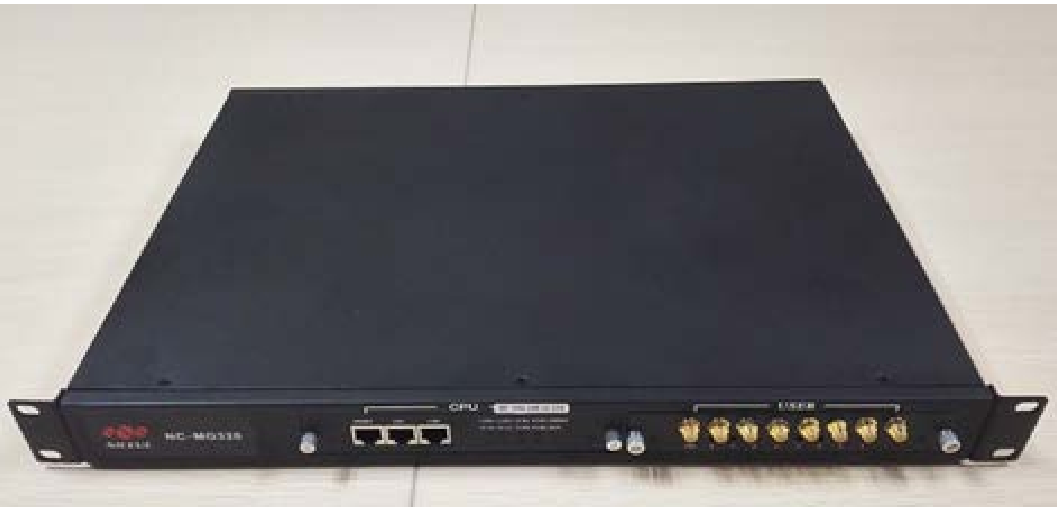


Power Switch	Power Switch
AC Power Input jack	AC Power Input jack
WAN	WAN interface
LAN	LAN interface
PWR1	The Power Status Of Device
RUN1	Operating status: slow flash indicates no registration, flash indicates registration, no flash indicates initialization, not bright indicates no running
PWR2	Power Status of User Board
RUN2	Communication Status of User Board and Controller Board, Flash indicates Good Communication
PWR3	Power Status of User Board
RUN3	Communication Status of User Board and Controller Board, Flash indicates Good Communication
RST	Long press will be configured to restore factory settings
Antennas	GSM/CDMA/WCDMA Antennas

NICEUC NC-MG320 Wireless Gateway

Figure 6-3 shows the appearance of NICEUC **NC-MG320** wireless gateway.

Figure 5-3 Appearance of NICEUC NC-MG320 Wireless Gateway



5.1.2 Product Specifications

This section describes the product specifications of Dinstar DWG2000F-8 series gateway and NICEUC NC-MG320 wireless gateway.

Dinstar DWG2000F-8 series gateway

Category	Description
Physical properties	• Power: input: 100-240 V, 50-60 Hz • Power consumption: < 38 W • Temperature: (operation): 0 °C to +40 °C, (storage): -20°C to +80°C • Operation Humidity: 5%-90% no condensation • Dimensions (W/D/H): 440 mm × 270 mm × 44 mm • Weight: 2.9 kg
Service specifications	• 8 SIM card slot • 2 LAN x 10/100 M Base-TX

NICEUC NC-MG320 Wireless Gateway

Category	Description
GSM/CDMA/WCDMA frequency band	GSM: 850\900\1800\1900 CDMA: 800 WCDMA-E: 900\2100@UMTS, 900\1800@GSM WCDMA-A: 850\1900@UMTS, 850\900\1800\1900@GSM

Category	Description
Number of VoIP channels	32 to 128
E1 trunk interface	0-4 E1
GSM/CDMA/WCDMA interface	8 channels
Ethernet port	Two 10/100/1000 MHz Base-T Ethernet ports
Serial port	One RS232 port (Console management port)
Interoperability	Compatible with devices of Cisco, Siemens, Avaya, Huawei, and ZTE
Power module	–48 V DC or 110-240 V AC
Maximum power	25 W
Transmission distances of phone cables	N/A
Dimensions	480 mm × 286 mm × 44 mm (1 U)
Weight	3.5 kg
Operating environment	Temperature: 0 °C to 50 °C; Humidity: 10% to 90% (non-condensing)

5.2 PSTN Gateway

This section describes the product structure, and product specifications of the PSTN gateway.

PSTN gateway adopts the NiceUC **NC-MG320** series gateway.

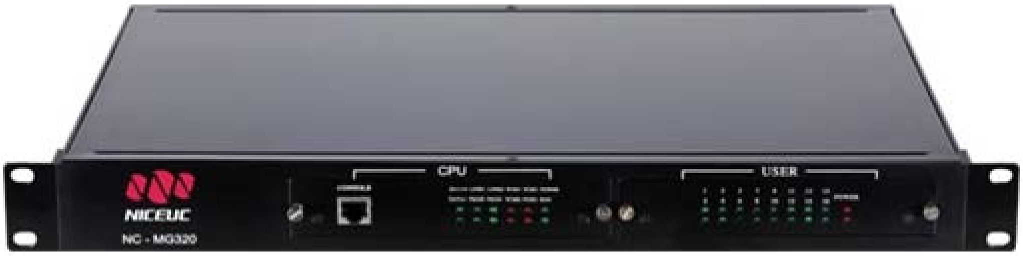
The PSTN gateway which is located at the interface between PSTN and IP, achieve the conversion among Foreign Exchange Office (FXO) interface, Foreign Exchange Station (FXS) interface, E1 and VoIP SIP, meanwhile complete the media stream transformation between the bearer channel of PSTN and IP.

5.2.1 Product Structure

This section describes the appearance of NiceUC NC-MG320 series gateway.

Figure 6-4 shows the appearance of NiceUC **NC-MG320** series gateway

Figure 5-4 Appearance of NC-MG320 Series Gateway



5.2.2 Product Specifications

This section describes the product specifications of the NiceUC NC-MG320 series gateway.

NiceUC **NC-MG320** series gateway features a compact structure, 1 U high, and can be mounted in a 19-inch standard cabinet or independently installed in a small equipment room. NiceUC **NC-MG320** series gateway supports 220 V AC power supply, adapting to different conditions in an equipment room.

Supported Signaling Protocols

Item	Specifications
Interface	FXO/FXS/SIP/E1
E1 signaling	ISDN PRI (ITU-T Q.931, Q.921)
	SS7 (ITU-T Q.700 series), 24 bits/14 bits PC, ISUP/TUP (need to be authorized)
	V5.2 (ITU-T G.964, G.965) (need to be authorized)
	R2 (need to be authorized)
	Q.SIG (need to be authorized)
VoIP protocol	SIP: • RFC3326 (Reason header in SIP messages) • RFC3372 (SIGTRAN and SIP-T) • RFC2327 (SDP) • RFC3398 (ISUP-SIP Mapping) • RFC3261 (SIP) • RFC5806 (Diversion Indication in SIP) • RFC2833 (DTMF) • RFC3362 (t.38) • RFC 3261 (SIP 2.0) • RFC3204 (MIME media types for ISUP and QSIG Objects) • RFC3578 (Mapping of ISUP overlap to SIP)
Audio	Codec:

Item	Specifications
encoding/decoding	• G.711 U-Law and A-Law • G.711 Appendix 1 • G.723.1 and G.723.1 Annex A • G.729 Annex A and Annex B • G.726 • GSM • ARM • ILBC
Network protocol	• IP • NAT • ICMP • ARP • HTTP • BOOTP • FTPS • TFTP • DHCP • PPPOE • SNMP • Diff-Serv
Echo cancellation	G.168 128 ms

Physical Properties

Item	Specifications
Input voltage	AC, 110 V to 240 V
Full-load Power	50 W
Dimensions (W × D × H)	480 mm × 286 mm × 44 mm (1 U)
Weight	3.5 kg
Temperature	0°C to 50°C
Relative humidity	< 80% RH

Configuration Details

Configuration Capacity	Physical Specifications

Configuration Capacity		Physical Specifications	
Configuration Type	Configuration Capacity	Port Name	Port Quantity
FXO/FXS	4 to 32	PCM port	0 to 4
E1/T1	0 to 4	4 line (RJ45)	8
VoIP channel	32 to 128	Network port	1
-	-	Serial port	1
-	-	Power port	1

5.3 TETRA Gateway

This section describes the product structure, and product specifications of the TETRA gateway.

TETRA gateway adopts the Microsys **ETS-8WP** wireless gateway.

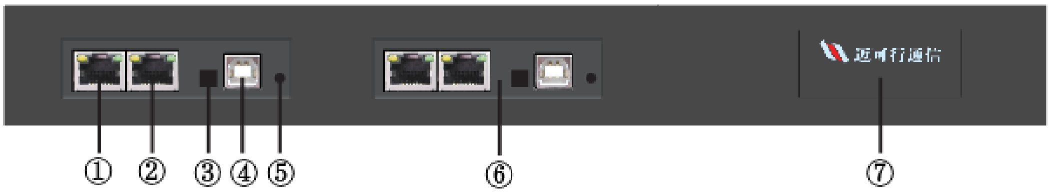
ETS-8WP is a short wave and ultra-short wave TETRA gateway, 1 U high, and can be mounted in a 19-inch standard cabinet. **ETS-8WP** supports the PTT signaling, AT commands, VOX, COR (carrier detect), channel change, PTT hotline, and rich specifications, applicable to various application scenarios and network sizes.

5.3.1 Porduct Structure

This section describes the front view and rear view of the Microsys ETS-8WP gateway.

An **ETS-8WP** trunking gateway is 1 U high and supports 19-inch standard rack installation. Figure 6-5 shows the front view of an **ETS-8WP**.

Figure 5-5 Front View of an ETS-8WP

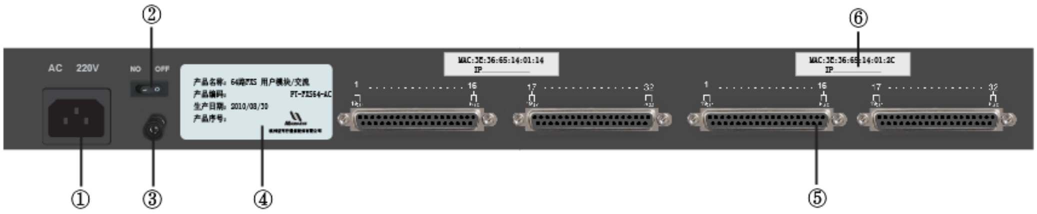


1	Ethernet port 1
2	Ethernet port 2
3	Three indicators are available. The first is the power indicator, the second is the running status indicator, and the third is the fault indicator. When the system starts up and runs properly, the power indicator is

	steady green, the running status indicator is blinking green, and the fault indicator is off. If a fault occurs, the fault indicator turns red.
4	Serial port
5	Reset button
6	Ports on board 2, identical in the meaning of each port described above
7	Trademark

Figure 6-6 shows the rear view of an **ETS-8WP**.

Figure 5-6 Rear View of an ETS-8WP



1	220 V power socket
2	220 V power switch
3	Ground terminal
4	Product information
5	Wireless ports
6	IP address and Media Access Control (MAC) address labels of boards

5.3.2 Product Specifications

This section describes the product specifications of the Microsys ETS-8WP gateway.

Technical Specifications

Item	Specifications
Wireless ports	DB37 ports, including an audio port, a PTT port, a COR port, and a five-wire serial port, each supporting four channels
Other ports	

Item	Specifications
Power supply	Rated voltage: 220 V voltage fluctuation: ±5% Frequency: 50 Hz±5% Wave form distortion rate of the phase-to-phase voltage: < 5%
Ground port	Ground resistance: ≤ 1 Ω
Ethernet port	10/100M adaptive
Dimensions and operating environment	
Dimensions (W × D × H)	440 mm × 328 mm × 45 mm
Weight	4 kg
Power consumption	Rated power: 45 W
Operating environment	Temperature: -10°C to +60°C Humidity: 10% to 90% non-condensing
Voice processing	
Voice encoding	G.711, G.723, G.729
Fax	T.30, T.38
Call completion rate	> 99%
Voice guarantee	QoS echo suppression (G.165/G.168-2000), voice priority (TOS), DiffServ jitter buffer, comfort noise generation (CNG), and voice activity detection (VAD)
Average call setup delay	< 100 ms
Reliability	
System availability	Availability ≥ 99.999%
Mean time between failures	> 20 years
System fault recovery time	< 15 minutes
Standard compliance	
Flame retardance	UL94V-0 materials
Electrical safety	UL 508, CSA C22.2/14, EN61010-1
EMC	EN50082-1(IEC801-2,3,4)CE
Surge protection	IEEE-472(ANSIC37.90)
Shock and vibration resistance	IEC68-2-6

6 eUPG670

About This Chapter

This section introduces the function, structure, and technical specifications of eUPG670.

7.1 Product Functions

This section describes the main functions of the eUPG670.

7.2 Product Structure

This section describes the software and hardware structures of the eUPG670.

7.3 Technical Specifications

This section describes technical specifications of the eUPG670, including its capacity specification, mechanical specifications, electrical specifications, environment requirements, external ports, surge protection specifications, and reliability specification.

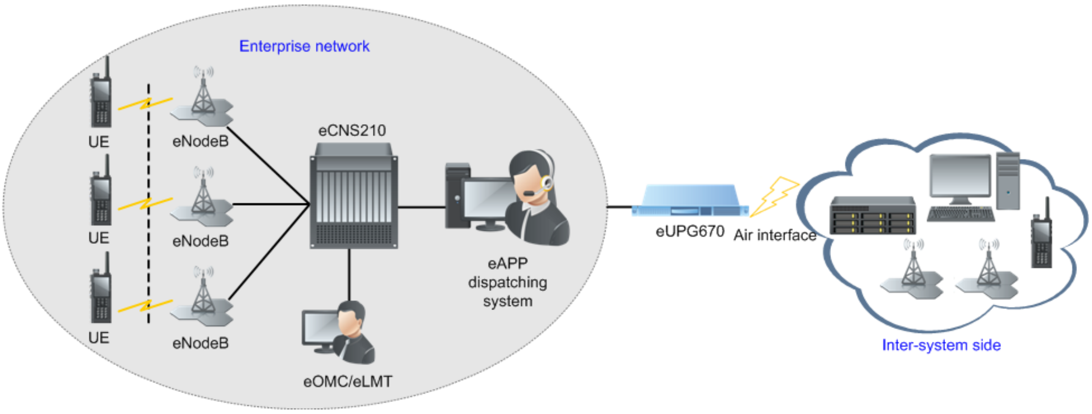
6.1 Product Functions

This section describes the main functions of the eUPG670.

Network Position

Figure 7-1 shows the network position of the eUPG670.

Figure 6-1 Network position of the eUPG670



eUPG670 is an integrated and vehicle-mounted product. It integrates functions of the traditional inter-system vehicle-mounted terminals and trunking gateway. The trunking gateway exchanges control-plane data with vehicle-mounted terminals through such ports as serial or general-purpose input/output (GPIO) ports, and directly connects to vehicle-mounted terminals through analog voice channels for user-plane data exchange.

The eUPG670 uses the following methods to connect the eUEs and inter-system terminals.

- The eUPG670 connects to the eMDC through Ethernet cables.
- Traditional vehicle-mounted terminals connect to the inter-system side over the air interface.

NOTE

The eUPG670 does not support independent geographic active/standby redundancy networking. It supports only geographic redundancy networking by connecting with the eAPP system of the enterprise network.

Functions

The eUPG670 supports the following service functions and operation and maintenance (O&M) functions:

- Service functions
  - Channel management supports management and configuration of channel resource between the enterprise network and the inter-system side.
  - Group selection on vehicle-mounted terminals supports obtaining group information and setting the current group through secondary development interfaces on vehicle-mounted terminals.
  - Group call service allows voice calls between groups on the enterprise network and those on the inter-system side.
- O&M functions
  - Configuration management allows operators to add, modify, delete, and query system parameters.
  - Alarm management allows querying active alarms of the system. The system displays alarms in real time. Users can view and analyze the alarms to troubleshoot problems.
  - Software management supports the installation of language packages and license management.

- Log management enables users to obtain logs of various types to diagnose problems, and to analyze system running status and services.

6.2 Product Structure

This section describes the software and hardware structures of the eUPG670.

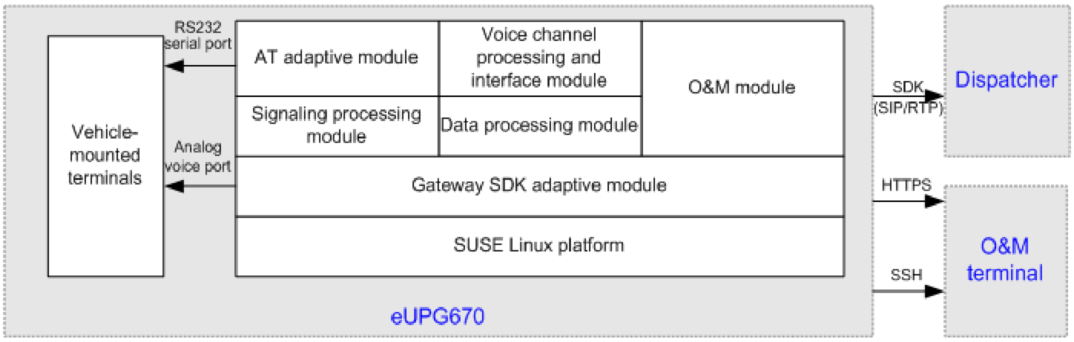
Software Structure

The eUPG670 uses the same software platform as the eAPP610 and also uses ACE-based (ACE is short for adaptive communication environment) self-development software platform.

- The software subsystems provide a basic platform for further development, operating, deployment, commissioning, maintenance, and upgrade for the eUPG670.
- The ACE-based software subsystems can work with third-party software or run on another OS (Linux) to provide a service-oriented distributed message architecture, basic components, and O&M functions.

Figure 7-2 shows the software structure of the eUPG670.

Figure 6-2 Software structure



Hardware Architecture

- Appearance

  The eUPG670 uses an indoor rack-mounted device with a 19-inch case-shaped structure and a height of 2 U. Figure 7-3, Figure 7-4, and Figure 7-5 show the appearance of the eUPG670.

Figure 6-3 Front view of the eUPG670

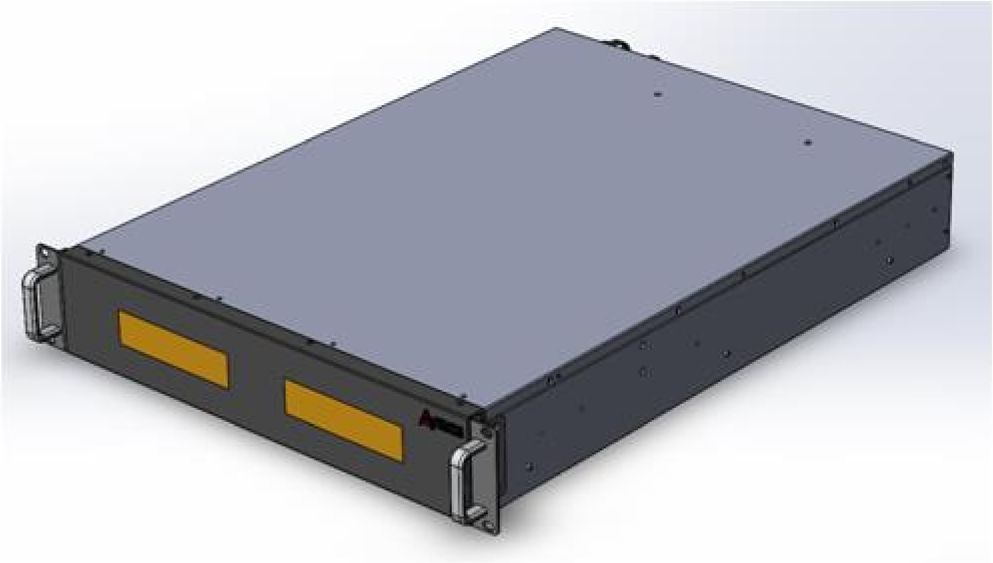


Figure 6-4 Rear view of the eUPG670

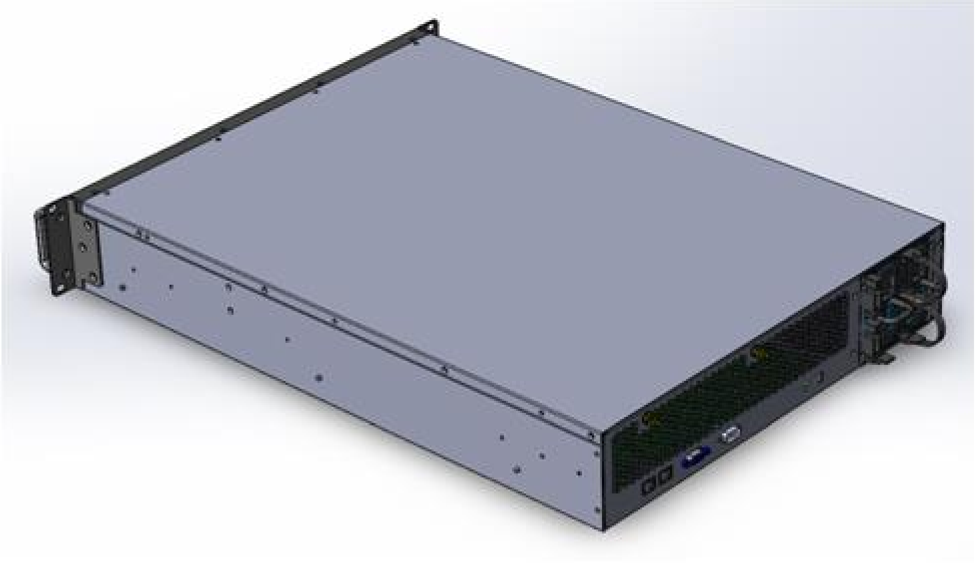
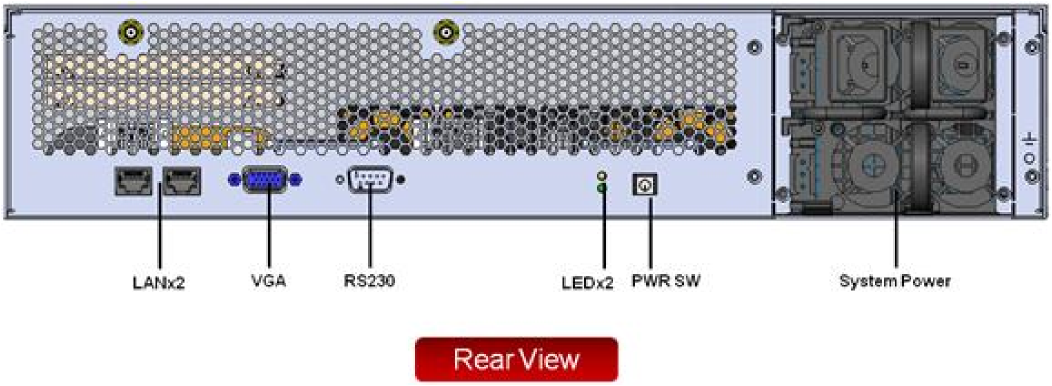


Figure 6-5 Rear panel of the eUPG670

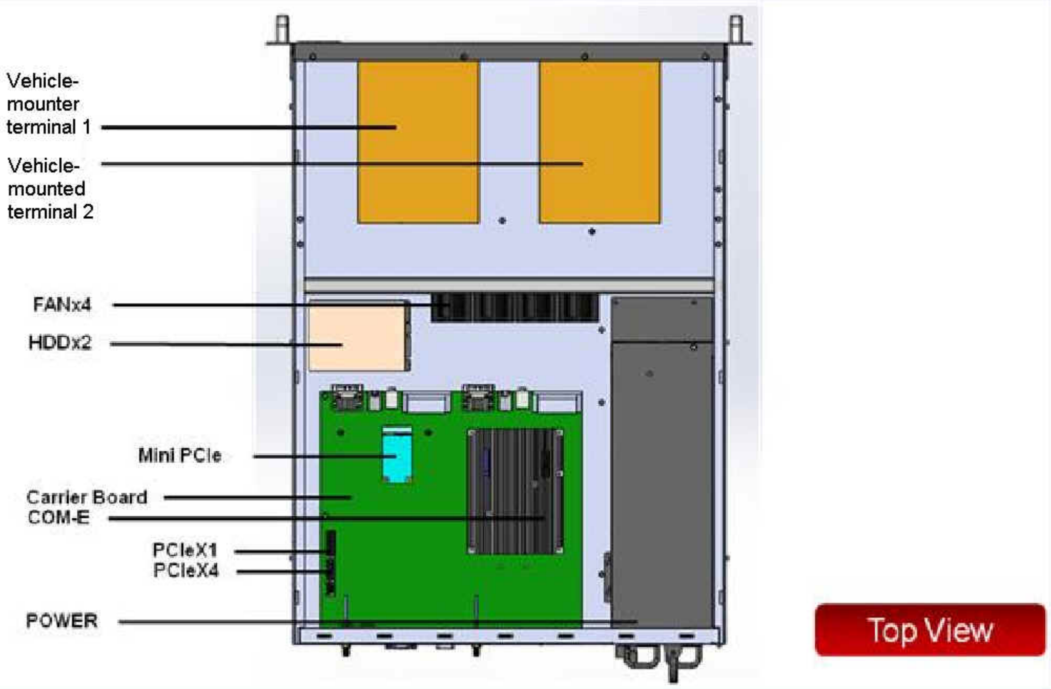


- Internal structure

  The eUPG670 provides two slots for installing two embedded vehicle-mounted terminals. The eUPG670 internally uses wires and cables to connect the inter-system vehicle-mounted terminals, x86 development board and its transfer board, power module, and RF ports, forming an independent working unit. See Figure 7-6.

  - The x86 development board processes inter-system inter-networking gateway software. The main board and transfer board provide extended ports and implements such functions as converting audio adapter signal and power signal.
  - The front panel can be uninstalled, facilitating operation to the inter-system vehicle-mounted terminal panel during maintenance and commissioning. In normal cases, the vehicle-mounted panel is not exposed to protect the vehicle-mounted terminal from being damaged or subject to misoperation due to external causes.

Figure 6-6 Internal structure of the eUPG670



6.3 Technical Specifications

This section describes technical specifications of the eUPG670, including its capacity specification, mechanical specifications, electrical specifications, environment requirements, external ports, surge protection specifications, and reliability specification.

Capacity Specification

Table 7-1 lists the capacity specification of the eUPG670.

Table 6-1 Capacity specification of the eUPG670

Counter Name	Specification
Concurrent voice services (channel)	2

Mechanical Specifications

Table 7-2 lists the mechanical specifications of the eUPG670.

Table 6-2 Mechanical specifications of the eUPG670

Counter Name	Specification
Dimensions (H x W x D)	86.1 mm (2 U) × 442 mm × 450 mm
Weight	No more than 12 kg
NOTE 19-inch cabinet (complying with the IEC297 standard) is used.	

Electrical Specifications

Table 7-3 lists the electrical specifications of the eUPG670.

Table 6-3 Electrical specifications of the eUPG670

Counter Name	Specification
Power voltage	• Rated input voltage: 100 to 240 V AC, 50/60 Hz • Voltage range: 90 to 264 V AC, 47 to 63 Hz
Maximum power	Power consumption must be no more than 480 W. The total power consumption of the main board and development board must be no more than 35 W.

Environment Requirements

Table 7-4 lists the environment requirements of the eUPG670.

Table 6-4 Environment requirements of the eUPG670

Counter Name	Specification
Operating temperature	–10℃ to +45℃
Storage temperature	–40℃ to +55℃
Relative humidity	5% to 95% (non-condensing)
Protection level	Waterproof and dustproof level: IP20
Heat dissipation	Air cooling (Air goes in from the front and out from the rear, or goes in from the left and out from the right.)

Reliability Specifications

Table 7-5 list the reliability specification of the eUPG670.

Table 6-5 Reliability specification of the eUPG670

Counter Name	Specification
MTBF	No less than 150,000 hours (target value)

External Ports

Table 7-6 lists the external ports of the eUPG670.

Table 6-6 External ports of the eUPG670

Port	Quantity	Connector Type	Description
Network port	2	RJ45	On the back panel, two auto-sensing 10/100 RJ-45 Ethernet ports are provided.
RF port	2	BNC type (female)	This item is used for connecting the antenna of the external vehicle-mounted terminal.
Audio output port	2	3.5 mm	Audio output ports on the back panel: Two 3.5 mm dual-channel audio detection jacks are provided with each supporting one-channel uplink and downlink voice playing (voice is not played by default). You can use the software to select uplink

Port	Quantity	Connector Type	Description
			or downlink voice playing.
PCIe port	2	PCIe slot	PCIe slots on the back panel: Two PCIe slots (E1 card or others) are provided. Expansion capability of four PCIe ports is reserved.
USB port	1	USB2.0	USB ports on the back panel: One USB2.0 host and a standard USB port are provided. Max current of 500 mA is supported.
Power input port	1	C14	On the back panel, one AC power input port is provided (with fuse and for three-prong plugs with LED indicator).

7 Typical Application Scenarios and Networking

About This Chapter

This section describes typical application scenarios and the networking deployment of the eAPP610.

7.1 Typical Application Scenarios

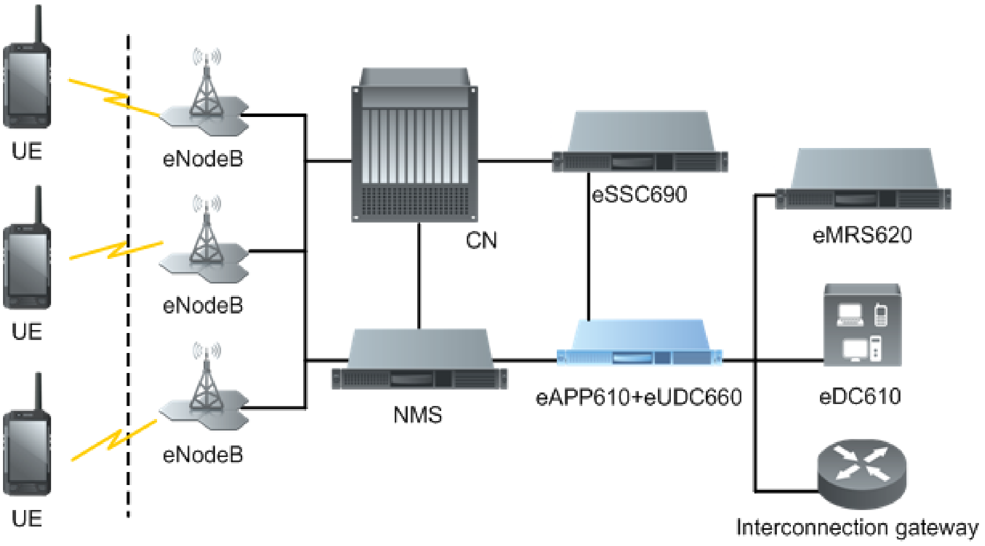
This section describes the typical application scenarios of the eAPP610.

The dispatching system consists of the eAPP610, eMRS620, eSSC690, eDC610, and interconnection gateway. In this scenario, the eAPP610 (eMDC) and eUDC660 are co-deployed, and the eMRS620, eSSC690, and NMS are separately deployed, as shown in Figure 8-1.

⚠ **NOTICE**

If the eAPP610, eMRS620, eSSC690, eUDC660, and NMS are co-deployed, the system specifications and service quality may not be ensured.

Figure 7-1 eAPP610 typical deployment



7.2 Networking of Master and Slave eAPP610s

This section describes the networking for the master and slave eAPP610s.

The eAPP610 allows servers to be deployed in master/slave networking to improve data processing efficiency. In normal cases, master and slave servers are used for the large/medium network scenario. See Figure 8-2, and Figure 8-3.

Figure 7-2 Networking of master and slave eAPP610s (master eAPP610, eUDC660, and eSSC690 co-deployed)

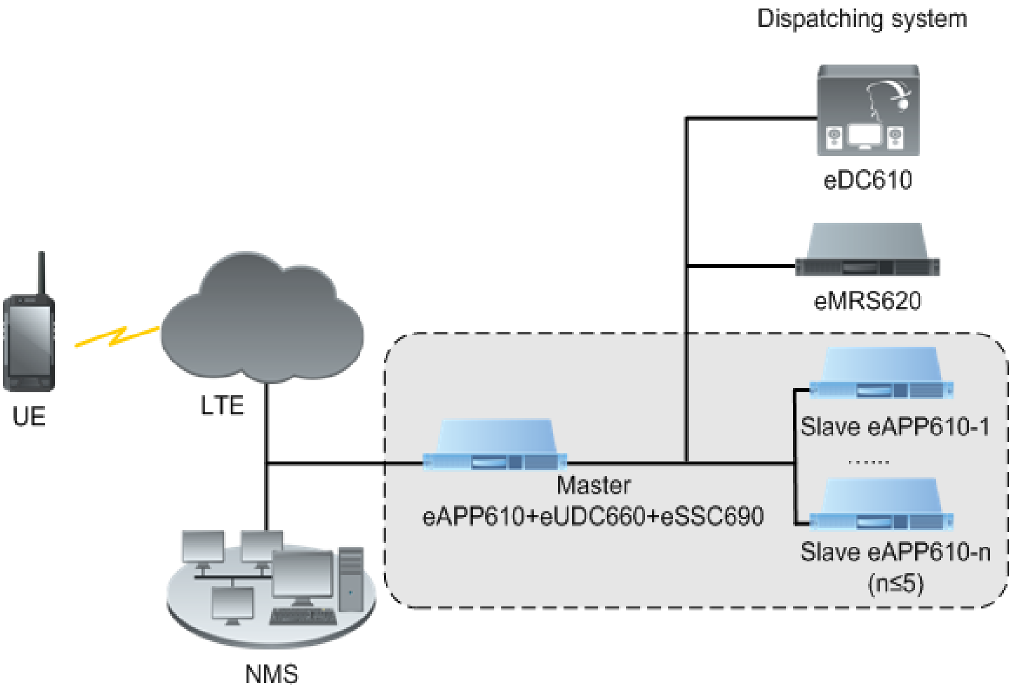
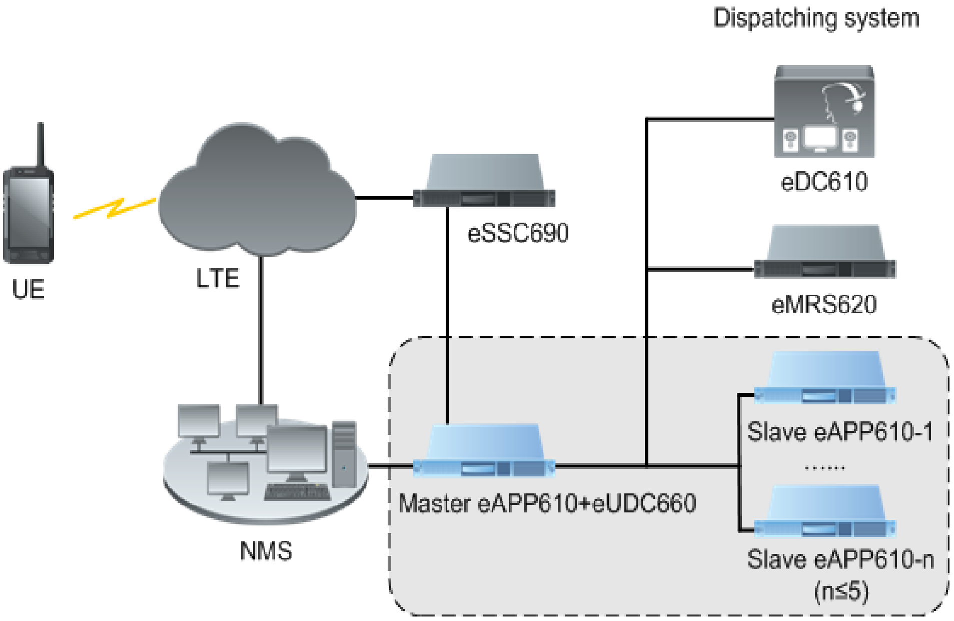


Figure 7-3 Networking of master and slave eAPP610s (master eAPP610 and eUDC660 co-deployed, and eSSC690 separately deployed)



The above networking involves the master and slave eAPP610.

- Master eAPP610: It processes the control-plane data and manages the slave eAPP610. One dispatching system can be configured with only one master eAPP610. The eUDC660 is deployed on the server housing the master eAPP610.
- Slave eAPP610: It processes user-plane data. One dispatching system can be configured with at most five slave eAPP610s.

8 Typical Configurations

This section describes the typical configurations of the NEs in a dispatching system.

Table 9-1 lists the typical configurations of the dispatching system.

Table 8-1 Typical configurations

NE Name		Large/Medium Network Scenario
eAPP610	eAPP610	Huawei Tecal RH2288H V3 (large-sized) server
Other dispatching system devices	eMRS620	Huawei Tecal RH2288H V3 (eMRS)
	eDC610	Lenovo ThinkCentre M710t
	eSSC690	Huawei Tecal RH2288H V3 (large-sized) server
	Video decoder	• DS-6308D-T • DS-6400HD-T • DS-6400HD-T-JX
	PLMN gateway	Optional
	PSTN gateway	Optional
	TETRA gateway	Optional
	Huawei eUPG670	Optional
NOTE Select a video decoder from the preceding models as required.		

9 Operation and Maintenance

This section describes the operation and maintenance functions of the eAPP610.

Configuration Management

Configuration management implements management on users, groups, and eMDC services, and performs configuration on the online service and device data.

The eAPP610 supports the following configuration management functions:

- Configuring parameters for the eMDC, including adding, removing, modifying, or querying the configuration
- Backing up and restoring configuration data files
- Providing ports for connecting the eAPP610 to the NMS

Alarm Management

Alarm management allows querying active alarms of the system. The system displays alarms in real time. Users can view and analyze the alarms to troubleshoot problems.

The eAPP610 supports the following alarm management functions:

- Reporting and clearing alarms
- Synchronizing alarm information between the eAPP610 and the NMS
- Implementing alarm-related operations on the NMS, including operations of manually clearing an alarm, synchronizing alarm information, and querying alarms

Log Management

Log management allows you to obtain various logs recorded by the system, so that fault diagnosis, system running status analysis, and service analysis can be performed.

The eAPP610 supports the following log management functions:

- System logs: record the system running status, including service initiation and release.
- Operation logs: record user operation information, for example, user logins.
- CDR logs: record detailed information of all calls in the system, including the call type, caller, callee, start time, end time, and call result.
- Performance logs: record user-plane data.

- Service logs: record the ambience listening, GIS subscription, GIS track tracing, video upload, recording playback, recording download, and recording query services.
- User logs: record user logins and terminal deregistration when multiple users use the same handheld terminal by logging in to it in turns.
- Device logs: record terminal login parameters, including the IMEI, IMSI, request type, request time, request result, result information, terminal IP address, terminal type, terminal version, manufacturer and terminal model.
- Security logs: record events related to the system security, including login, logout, user change, role change, license digital signature, and security management change.

License Management

License management allows you to download the latest license file to a specified directory on the server and then activate the license file to update the license items.

The following license functions are available on the eAPP610:

- License upload and activation
- License file decryption, loading, and activation
- License change notifications
- License expiration alarming
- License invalidity

Resource Monitoring Management

During routine maintenance or in the event of a system exception, a user can locate a fault based on the real-time monitoring information obtained by using the system resource monitoring function.

The eAPP610 supports the following resource monitoring management functions:

- Monitoring processes
- Monitoring the hard disk, memory, CPU, and database

Device Management

During routine maintenance, the device management function is used for managing and maintaining the device.

The eAPP610 supports the following device management functions:

- Hardware configuration: Configures the application mode (eAPP610) and host IP address (Internet Protocol).
- Configuration of the service type based on the hardware type
- Service restart

Software Management

This function enables you to upgrade software and patches, install language packages, and manage licenses of the eAPP610. Software and patch rollback is supported upon upgrade failures.

10 Reliability

In a dispatching system, the eAPP610 works in 1+1 active/standby mode to achieve geographic redundancy for reliability considerations.

When the active eAPP610 works properly, it processes all services, and the standby eAPP610 has no service load (but may have performance consumption of data synchronization). When the active eAPP610 is unavailable, the standby eAPP610 takes over the services. During a switchover, services on the active eAPP610 are interrupted, and then the standby eAPP610 provides services as an active eAPP610. The services could be restored within 8 minutes.

Switching policies for other dispatching system devices are as follows:

- eDC: Floating IP addresses are used between an active eAPP610 and a standby eAPP610, and the eDC uses a floating IP address to log in to an eAPP610. During an active/standby switchover, the eDC interrupts all ongoing services and receives no new services. The status of users and groups subscribed to the eDC are changed after the switchover. You must re-log in to the eDC after an active/standby switchover.
- Recording server: An active eAPP610 and a standby eAPP610 for geographic redundancy connect to different recording servers, which must be configured separately.
- Interconnection gateway: An active eAPP610 and a standby eAPP610 connect to interconnection gateways that have different configurations. The differences in their configurations require no synchronization.

11 Product Security

About This Chapter

This section describes security feature principles of the eAPP610.

11.1 Device Security

This section describes device security principles of eAPP610.

11.1.1 Operating System Security

OS security is fundamental to proper eAPP610 system running and authorized user operations. An OS with vulnerabilities is easily attacked by hackers, viruses, and worms, resulting in problems such as network service interruptions, information loss, data corruption, and low running efficiency.

The eAPP610 runs the SuSE Linux OS. The following measures are designed to address security risks encountered by this OS:

- OS security hardening: Enhance the security of the services, password configurations, file rights, and kernel parameters of the Linux OS to prevent hacker attacks without affecting services.
- OS log management: Use the log audit function provided by the Linux OS to monitor the operating status of the system in real time and to detect and track intruders.
- OS security patch: Analyze OS patches regularly and release OS security patches every six months. Follow the urgent patch release procedure to release major security patches.

File System Security

- Forbidding unauthorized users from accessing sensitive information in the Linux OS
- Deleting all files without owners
- Deleting all null links
- Setting the system UMASK to 027
- Strictly defining user path variables
- Setting strict access rights for root user's directories

System Access Authentication and Authorization

- Session timeout setting: If a session remains inactive for 5 minutes, the session times out, and all information displayed on the console is cleared.
- Pluggable Authentication Modules (PAM): The PAM can implement security functions, such as user verification and data encryption. Users can also set customized configurations on the PAM.

Security Improvement of Accounts and Passwords

- Forbidding unneeded accounts.
- Setting the password complexity requirements. The password of a Linux account must be alphanumeric and at least 8-character long.
- An account is locked automatically if incorrect passwords are entered for five consecutive times. The account is unlocked automatically after 5 minutes.

Records of OS Logs

Linux OS logs are classified into operation logs and system logs. A centralized log server manages all Linux OS logs to improve log management efficiency, ensuring log security, reducing log query workload, and rapidly tracking attackers when a PC is attacked. Table 12-1 describes the log files.

Table 11-1 Log files

Log File	Log Type	Save Path	Description
utmp	Login log	/var/run/utmp	Records information about login users.
wtmp	Login log	/var/log/wtmp	Records information about user login and logout, data exchange, power-off, and restart.
messages	System log	/var/log/messages	Records information about the hardware, software, and system; and monitors the system events. The save paths of logs can be configured by specifying the file **/etc/syslog-ng/syslog-ng.conf**.
auth.log	System log	/var/log	Records login events, including login errors, usage logs of the **su** command, and other authentication events.

System Tool Usage Suggestions

- Tool tcpdump

  In the system deployment phase, you need to use this tool to commission and verify the interconnections with external components. Only the **root** user has the rights to use the tcpdump tool. tcpdump is a network sniffing tool, which may cause information to be sniffed. Therefore, exercise caution when using this tool.

- Tool gdb

  In the product maintenance phase, if a user-mode process becomes abnormal, use the gdb debug tool to quickly and conveniently locate a fault. Only the **root** user has the rights to use the gdb tool. gdb may cause information to be sniffed. Therefore, exercise caution when using this tool.

11.1.2 Database Security

Database security is essential to the security of NE data and legal user operations. Proper usage and maintenance of a database are crucial to ensuring system security.

Database Right Management

Database rights are configured based on the minimum rights principle. When operated by an account with the minimum rights, the database is less vulnerable to attacks when the OS commands are executed.

Table 12-2 describes the database accounts

Table 11-2 Database accounts

Account	Description	Permissions	Password Acquisition Method
eltedbm	The administrator account of the MySQL database. Manages and operates the MySQL database.	Highest rights on the database	System administrator
odb_user	The OM account of the MySQL database. Connects to and accesses the database.	Basic management and access permissions on the database	OM user

Database Access Control

The database access right can be controlled based on user types.

The details are as follows:

- Application software ownership: Accounts who manage a piece of application software have the full control rights to the application software. Therefore, do not assign a single account the rights to manage all application software.
- Database management rights: Accounts with these rights can modify the database configurations and rights. Therefore, clearly define database management rights for each account. If a user requires only the right to store data in the database, assign only the right to store data to the user.
- Rights on database directories and files: Assign different access rights to different users (the permission to read, write, or execute database files, or the permission to access database directories).
- Rights to view owners of database service processes or daemon processes: Accounts with such rights can view the owners of database service processes or daemon processes, thereby determining whether the owners are specified accounts.

Identification and Authentication for Database Users

Database users can access database objects only after they pass the identification and authentication.

- User account authorization: For security concerns, do not allow all OS accounts to access a database; allow only authorized accounts to access the database.
- Rights assignment to the database administrator: The database administrator has the highest right. Therefore, when assigning rights to the database administrator, exercise caution to prevent potential security threats.
- Assignment of rights to access a database: Assign database access rights with caution to prevent unauthorized users from accessing the database.

Database Encryption and Network Security

Remote authentication is provided to ensure network security. Data is encrypted for transmission over networks to ensure data integrity.

- Data encryption: Database account passwords are encrypted and stored. By default, passwords of database users are stored in the internal Hash algorithm. The database administrator cannot identify the actual passwords of users. The imported and exported NE data files are also encrypted to prevent data leakage.
- Whitelist mechanism: only devices in the whitelist can connect to the database.
- Transmission encryption: Transport Layer Security (TLS) encryption is supported in remote connection to the MySQL database.

11.2 Network Security

This section describes network security principles of the eAPP610.

11.2.1 Triple-plane Isolation

To ensure the network security of users, the eAPP610 divides the network into different planes.

- Operation plane: the OM port for the eAPP610 system to communicate with the WebUI, eUDC660, and NMS.

- Control plane: the service control port for NEs, such as the eDC610, UE, eCN, gateway, eMRS620, eSSC690, and other eAPP610 NEs.
- User plane: the user data port for the NEs, such as the eDC610, UE, eCN, gateway, eMRS620, eSSC690, and other eAPP610 NEs.

The eAPP610 assigns the operation plane, control plane, and user plane with different IP addresses to achieve mutual isolation. The control plane and user plane are unified and use the same IP address.

11.2.2 Port Service

On open All-IP networks, attackers usually use vulnerabilities in the external services provided by networks to launch attacks against network devices. eAPP610 hardened the following two aspects to strictly control the access right of network services.

- Eliminating unneeded external services

  For open ports and services over these ports on the eAPP610 after the elimination, see *eAPP610 Communication Matrix* released with the product documentation.
- Forbidding network services to listen to the IP addresses that do not actually provide services

  The eAPP610 forbids ports on which external network services are provided to listen to the IP addresses that do not actually provide services, thereby preventing attackers from accessing the system using these IP addresses.

11.2.3 Transmission Security

The eAPP610 supports and uses the Secure Sockets Layer (SSL) protocol to encrypt OM transmission channels.

The SSL protocol is a security connection technology for servers and clients. It provides a confidential, trusted, and identity-authenticating connection to two application layers. Currently, SSL is regarded as a standard security measure and is widely applied to the web service, File Transfer Protocol (FTP), and telnet.

Identity Authentication

Identity authentication checks whether a communication individual is the expected one. SSL authenticates servers and clients based on digital certificates. Clients and servers have their own identifiers. The identifiers are numbered by the public key. To verify that a user is legitimate, SSL requires digital authentication during data exchange in the SSL handshake procedure.

Connection Confidentiality

Data is encrypted before transmission to prevent data from being hacked by malicious users. SSL uses encryption algorithms to ensure the connection confidentiality.

Data Integrity

Any tampering on data during transmission can be detected. SSL establishes a secure channel between the client and the server so that all the SSL data can reach the destination intact.

11.3 Application Security

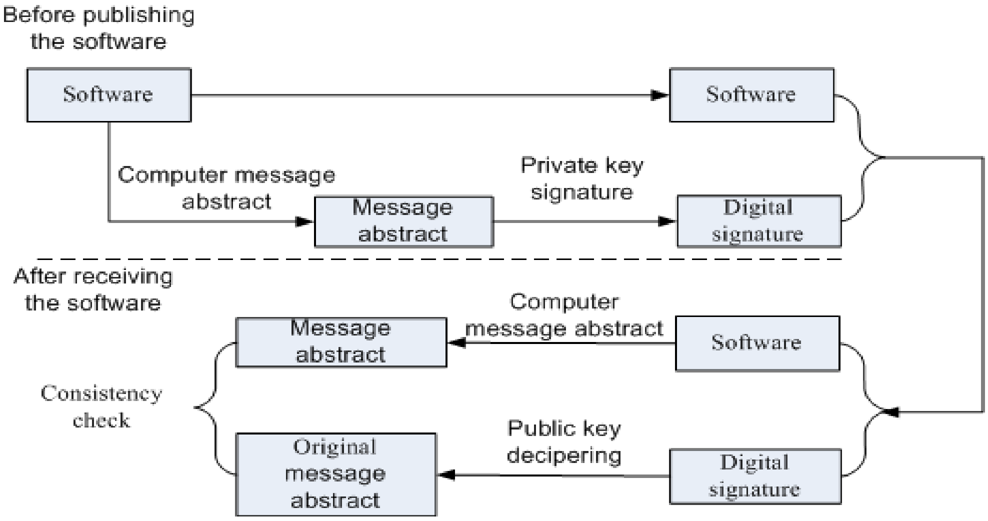
This section describes application security principles of eAPP610.

11.3.1 Digital Signature of Software

A digital signature of software is used to verify the software source during the process from software release to application. Digital signatures ensure software integrity and reliability.

When software is released, the digital signature is put on the software package, and information about the digital signature is released with the software package. The software package is still digitally signed when it is downloaded on an NE. Before using a software package, the NE verifies the digital signature carried by the software package. If the verification is successful, the software is complete and reliable and therefore can be used. If the verification fails, the software package is invalid and cannot be used. Figure 12-1 shows the principle of the digital signature of software.

Figure 11-1 Digital signature of software



- Before a software package is released, all files in the software package are signed with digital signatures. That is, after message abstracts of all files in the software package are calculated, private keys are used to sign on message abstracts, thereby obtaining the digital signature of a software package.
- When a software package with digital signatures is loaded to an NE through media such as the software release platform, the NE first verifies the digital signature of the software package. That is, the NE uses public keys to decrypt the digital signature and obtain the original message abstract. At the same time, a new message abstract is obtained through calculation. The original and new message abstracts are compared with each other.
  - If the two message abstracts are consistent, the verification is successful, and the software can be installed or be used for upgrade.
  - If the two message abstracts are inconsistent, the verification fails, and the software cannot be installed or be used for upgrade.

Public keys used in software digital signatures exist in security storage areas of NEs and they cannot be queried or exported.

11.3.2 OM Security

OM engineers manage and maintain the system, including managing and maintaining data required for system running, performance measurement (traffic measurement) data, and alarm information.

The system provides effective OM methods and tools to ensure normal system running, reduce operation expenditure, and improve service quality. The OM security measures are as follows:

- Account security
- Login security
- Password security
- OM transmission channel security
- Web security
- Log security

Account Security

Users who can log in to the WebUI of the eAPP610 are listed as follows:

- admin: default administrator with the highest permissions
- eDC610 user: a user with fixed permissions which is registered with the eUDC660 but can only log in to the WebUI of the local eAPP610 system.
- New user: a customized user created by the **admin** on the WebUI. Permissions of a new user depend on the role granted to it.

A role is a set of operation permissions. A user must be granted with only one role. The eAPP610 system provides default roles and supports role customization on the WebUI.

Login Security

A user must be authenticated to log in to the WebUI. User accounts and passwords are stored on a local server for local authentication.

Table 12-3 describes the detailed lockout policies of the WebUI.

Table 11-3 Lockout policy

Parameter	Value Range	Description
Lockout setting	1 to 720 Unit: minute	If no operation is performed within the configured time, the eAPP Management System automatically exits the operation page and returns to the login page. The default value is 10 minutes.
Lockout policy	• YES • NO	Specifies whether the account lockout policy is selected. • YES: The system applies the account lockout policy. • NO: The system does not apply the account lockout policy. The default value is **YES**.

Parameter	Value Range	Description
Max Login Retry Num	1 to 99	Specifies the maximum number of login attempts allowed for an account before the account is locked out. The default value is **5**.
Auto Unlock Time	1 to 999 Unit: minute	The lockout duration is controlled by a system timer. That is, the duration is not affected by sudden changes of the system time. The default value is **30** minutes.

Password Security

For the eAPP610 system, password policies such as the customized password complexity and expiration policy can be applied to passwords of OM accounts. Table 12-4 describes detailed information about password policies.

Table 11-4 Password policy

Parameter	Description
Password rules	The password must contain at least three of the following character types: • Lowercase letters: If this option is selected, a password must contain at least one lowercase letter. • Uppercase letters: If this option is selected, a password must contain at least one uppercase letter. • Digits: If this option is selected, a password must contain at least one digit. • Characters: If this option is selected, a password must contain at least one character from **`~!@#$%^&*()-_=+\\|[{}];:'",<.>/?** and **space**. By default, **Lowercase letters**, **Uppercase letters**, and **Characters** are selected.
Minimum password length	Specifies the minimum

Parameter		Description
		length of a password. The value is a string of 8 to 128 characters. The default value is **8**.
Change password cycle		Specifies the validity days of a password. The default value is **180**.
Change password interval		Specifies the minimum day interval at which the password is changed. The default value is **1**.
Warning of expiration interval		Specifies the number of days for notifying a user of the expiration date of the password in advance. The default value is **5**.
Password reuse interval		Specifies the number of lately used passwords that cannot be reused this time. The default value is **3**.
Password attempts times		Specifies the maximum number of login attempts. If you entered wrong passwords for the times defined in this parameter, the account is locked. The default value is **5**.
Auto Unlock Time		Specifies the time before a locked account is automatically unlocked. The unit is minute and the default value is **30**.
Forced to change the password of the first time login		Specifies whether to force a new account to change the password upon first login.
Password modification		Common users can change their own passwords. The administrator can change passwords of other users.
Account validity period		Specifies the validity period of an account. The default value is **180** days.
User policy of no login within a period	Enable (default setting)	Specifies the policies for users who have not logged in to the system for *N* days. • Disable: Disables users

Parameter		Description
		- who have not logged in to the system for *N* days. - Delete: Deletes users who have not logged in to the system for *N* days. By default, the value is **60** days and the policy is **Disable**.
	Disable	-
Account logon history switch		Specifies whether to display the historical access records of the current user. - Open: Display the historical access records of the current user. - Close: Do not display the historical access records of the current user. The default value is **Close**.
Login time/IP limit		Specifies whether to define time and IP addresses in user login. - Open: Enable this function. - Close: Disable this function. The default value is **Close**.
Users cannot log in simultaneously		Specifies whether to forbid a user to log in at different locations at the same time. - Open: Enable this function. When this function is enabled and the user succeeds in a new login attempt, a message is displayed, indicating that the previous login has been logged out because the account has logged in elsewhere. - Close: Disable this function. The default value is **Close**.
Weak password feature is enabled		Specifies whether to enable the weak password

Parameter	Description
	prevention function. ● Selected: Enable. Enabling this function prevents the usage of predefined weak passwords by users. ● Deselected: Disable. It is disabled by default.

OM Transmission Channel Security

The OM transmission channel provides man-machine interfaces and machine-machine interfaces for remote access and the interfaces are all carried over the IP network. The eAPP610 system implements strict encryption policies on these interfaces. Security encryption policies can be flexibly set based on the credibility of a network.

Table 12-5 describes the encryption policy for man-machine interfaces. Table 12-6 describes the encryption policy for machine-machine interfaces.

Table 11-5 Encryption policy for man-machine interfaces

Login Method	Security Protection Measure
SSH	As a secure encryption transmission protocol, Secure Shell (SSH) ensures the security of remote login sessions and network data transmission. Password authentication for SSH can be performed with local accounts or third-party RADIUS servers.
WebUI	WebUI data transmission is forcibly used during web-based login. Unencrypted channels are prohibited to transmit data.

Table 11-6 Encryption policy for machine-machine interfaces

Login Method	Security Protection Measure
FTPS	File Transfer Protocol over SSL (FTPS) uses the security encryption transmission protocol SSL.
ZMQ	The ZMQ component provides encryption for the transmission layer, encrypts message packets, and sets the SSL mode during initialization.

Web Security

OM accounts are used to log in to the Web UI, where local authentication and NMS authentication are available for password authentication. Rights for the administrator and rights for common users are supported. Common users can view only limited contents and they can operate an NE only after being authorized by the administrator.

Currently, following measures are taken to ensure the web security for the eAPP610 system:

- HyperText Transfer Protocol Secure (HTTPS) transmission encryption
- Strict account management and right control
- Automatic disconnection for idle connections
- Account lockout after the number of incorrect password attempts exceeds
- Password encryption using Password-Based Key Derivation Function (PBKDF2)

Log Security

The eAPP610 system records system logs, security logs, and operation logs. All non-query operations are recorded in operation logs.

A user can query and export logs using the log management function. Log management rights are under control and only users with the log management rights can query and export logs.

12 Glossary

This table provides the related glossary for reference.

Glossary	Full Name	Full Name
3GPP	Third Generation Partnership Project	Third Generation Partnership Project
AMR	Adaptive Multirate	Adaptive Multirate
ATCA	Advanced Telecom Computing Architecture	Advanced Telecom Computing Architecture
BNC	British Naval Connector	British Naval Connector
CDMA	Code Division Multiple Access	Code Division Multiple Access
CIF	Common Intermediate Format	Common Intermediate Format
CPU	Central Processing Unit	Central Processing Unit
DVI	Digital Visual Interface	Digital Visual Interface
DVR	Digital Video Recorder	Digital Video Recorder
DVS	Digital Video System	Digital Video System
eAPP	Enterprise Network Application Software System	Enterprise Network Application Software System
eMDC	Enterprise Multimedia Dispatching and processing Center	Enterprise Multimedia Dispatching and processing Center
eMRS	Enterprise Multimedia Recording and playback Server	Enterprise Multimedia Recording and playback Server
eUDC	Enterprise User And Device Controller	Enterprise User And Device Controller

Glossary	Full Name	Full Name
FXO	Foreign Exchange Office	Foreign Exchange Office
FXS	Foreign Exchange Station	Foreign Exchange Station
GE	Gigabit Ethernet	Gigabit Ethernet
GIS	Geographic Information System	Geographic Information System
GPS	Global Positioning System	Global Positioning System
GSM	Global System for Mobile communication	Global System for Mobile communication
GUI	Graphical User Interface	Graphical User Interface
HDMI	High Definition Multimedia Interface	High Definition Multimedia Interface
IMS	IP Multimedia Subsystem	IP Multimedia Subsystem
IP	Internet Protocol	Internet Protocol
MAC	Media Access Control	Media Access Control
MAN	Metropolitan Area Network	Metropolitan Area Network
MMS	Multimedia Messaging Service	Multimedia Messaging Service
NMS	Network Management System	Network Management System
P2P	Point-To-Point	Point-To-Point
PLMN	Public Land Mobile Network	Public Land Mobile Network
PoC	Push to talk over Cellular	Push to Talk over Cellular
PSTN	Public Switched Telephone Network	Public Switched Telephone Network
PTT	Push To Talk	Push To Talk
PTZ	Pan Tile Zoom	Pan Tile Zoom
QCIF	Quarter Common Intermediate Format	Quarter Common Intermediate Format
SDK	Software Development Kit	Software Development Kit
SIP	Session Initiation Protocol	Session Initiation Protocol
SMS	Short Message Service	Short Message Service
SOHO	Small Office and Home Office	Small Office and Home Office

Glossary	Full Name	Full Name
TETRA	Terrestrial Trunked Radio	Terrestrial Trunking Radio System
UE	User Equipment	User Equipment
UMTS	Universal Mobile Telecommunications System	Universal Mobile Telecommunications System
VGA	Video Graphic Array	Video Graphic Array
VoIP	Voice over Internet Protocol	Voice over Internet Protocol
WCDMA	Wideband Code Division Multiple Access	Wideband Code Division Multiple Access