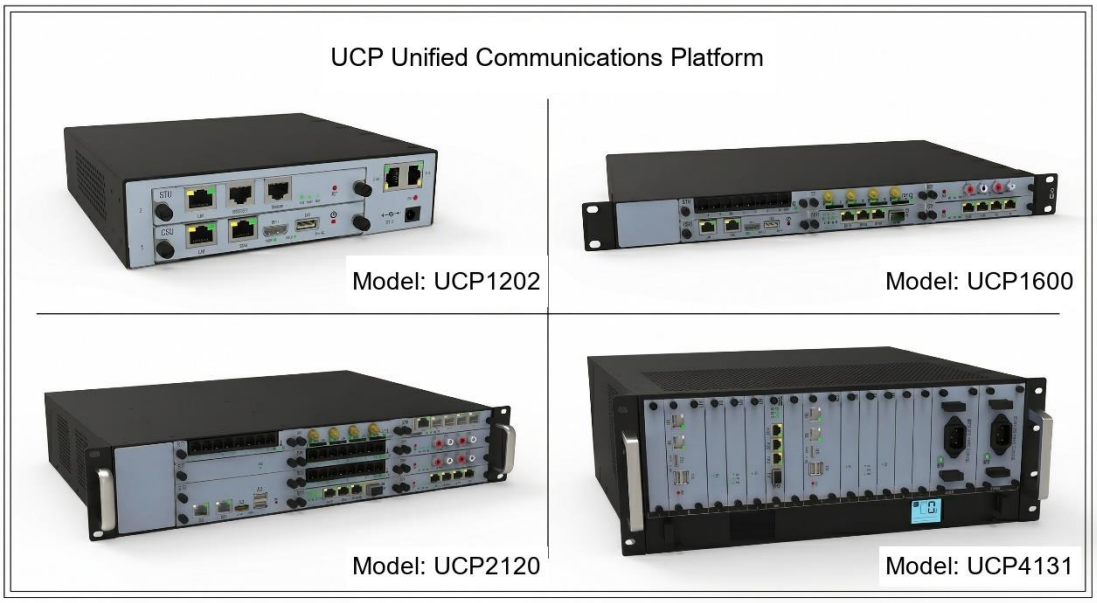
UCP Unified Communications Platform



Address: Room 624, 6/F, Tsinghua Information Harbor, Shukan Building, Qingxiang Road, Longhua Street, Longhua District, Shenzhen 518109, China

Website: https://www.openvoxtech.com /

Tel: +86-755-66630978

Email: sales@openvoxtech.com, support@openvoxtech.com

Welcome

Thank you for choosing the UCP Unified Communications Platform. We hope you make full use of this feature-rich communications platform. If you need technical support, please contact us at +86-755-66630978.

About This Manual

This manual introduces the UCP Unified Communications Platform. Please read this manual carefully before configuring its features.

Declaration

OpenVox Communication Co., Ltd. hereby declares that this series complies with the essential requirements and other relevant provisions of CE and FCC. The information in this document is subject to change without notice. OpenVox Communication Co., Ltd. makes no warranties with respect to this guide, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. OpenVox Communication Co., Ltd. assumes no liability for any errors contained in this guide, nor for any incidental or consequential damages arising from the furnishing, performance, or use of this guide.

目录

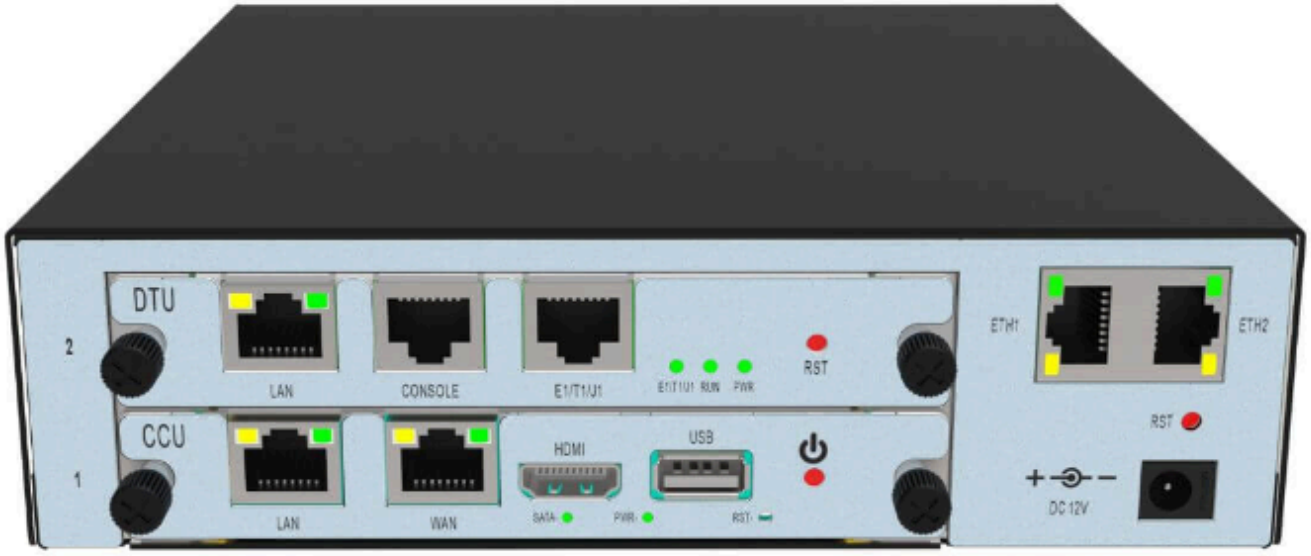
1 Technical Specifications

1.1 Overview

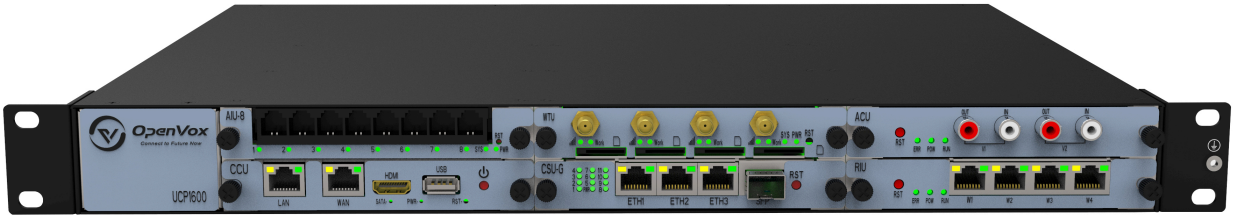
OpenVox Unified Communication Platform (UCP) is an ideal integrated solution for data, voice, and video, suitable for small and medium-sized enterprises, and can be widely deployed in industries such as government and enterprise call systems, commercial call centers, and dispatch centers. The core concept of UCP is that users can select business modules and main control modules with different functions and performance according to their own needs. These modules are connected to the backplane through dedicated communication connectors via high-speed Ethernet. OpenVox Unified Communication Platform is not merely a single VoIP gateway or IPPBX product, but a unified communication platform covering a full range of telephony interfaces and IPPBX functions.

UCP has four models: UCP1202, UCP1600, UCP2120, and UCP4131. Each model supports a variety of interfaces such as FXS/FXO/GSM/WCDMA/LTE/E1/T1/audio/radio and magnetic interfaces, and supports CPU main control modules based on the general X86 architecture, which can be flexibly installed in IPPBX systems or other business systems.

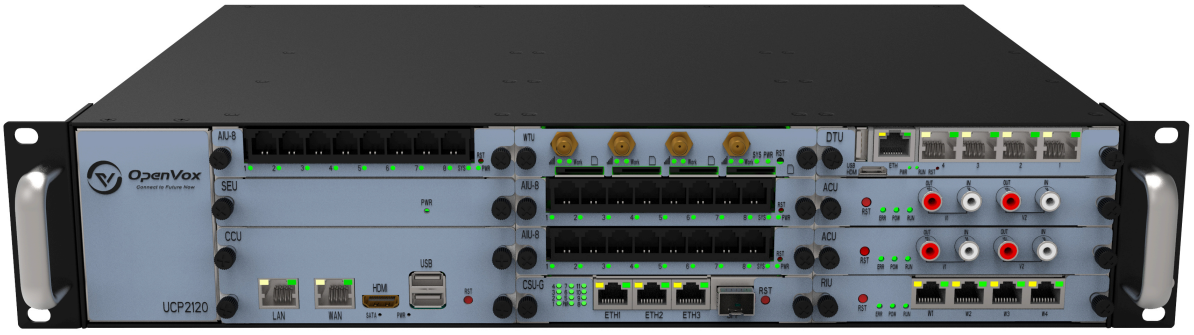
The UCP1202 appearance diagram is shown below.



The UCP1600 appearance diagram is shown below.



The UCP2120 appearance diagram is shown below.



The UCP4131 is shown below.

1.2 Hardware Architecture

The UCP unified communication platform hardware adopts a highly modular design, with a compact and well-organized front-and-rear layout. The front of the chassis is equipped with multi-slot hot-swappable interface board positions for installing the main control board, switching board, SEU storage expansion board, WTU wireless service board, FXO/FXS trunk board, E1/T1 digital trunk board, and other modules, meeting different deployment needs through optional modules. The backplane provides high-speed bus interconnection, ensuring low-latency and high-bandwidth data exchange between the main control board and each interface board.

The main control board integrates a multi-core processor and DSP acceleration unit to achieve mixed codec and service processing for voice signals. Combined with redundant fans and a wide-range input power module, it ensures continuous and stable operation in various environments. The management panel includes Ethernet management port and USB port, supports Web-based graphical configuration and unified network management, and reserves a serial port for local CLI maintenance. It supports a wide operating temperature range of 0°C–50°C and humidity environments up to 95% non-condensing, providing flexible and reliable voice switching solutions for small and medium-sized enterprises.

2 Product Highlights

2.1 Rich Services and Interfaces

- Friendly and intuitive interface interaction allows even new users to quickly get started with configuration and maintenance.
- High-availability architecture supports load balancing, ensuring continuous service capability under high concurrency.
- Supports GSM / LTE / analog / E1 & T1 / audio / intercom / magnetic interfaces to meet access requirements in different scenarios.

2.2 High Reliability, Low Cost

- Uses a telecom-grade hardware and software platform with the LINUX operating system. UCP2120 and

UCP4131 support 1+1 power backup.

- UCP2120 and UCP4131 support active-standby main control boards. Business interruption caused by main board network cable failure or other abnormalities can be recovered on the standby board, and ongoing voice calls are not affected during active-standby switching.

- UCP1600, UCP2120, and UCP4131 support dual-device active-standby. Ongoing voice calls are not affected during active-standby switching.

- As an IP voice switching device, it can reduce enterprise operation and maintenance costs.

2.3 Flexible Deployment, Easy Maintenance

- Supports single-node networking and distributed networking, offering flexible deployment.

- Supports unified network management, meeting the needs of centralized operations and efficient management.

- Built-in Web management system provides fast deployment and daily configuration functions.

- Built-in Web self-service system provides meeting reservation and personal service management functions.

3 Supported Services

3.1 Basic Voice Service

- **Internal user interoperability**: The unified communication platform supports bidirectional interoperability among all kinds of narrowband and broadband terminals (analog phones, SoftPhone, SIP phones, Desktop Client, SIP attendant consoles, IADs, etc.). Internal users can act as both calling and called parties for high-quality voice calls, meeting communication needs for mixed multi-terminal deployment within a local network.

- In**teroperability based on narrowband trunks**: Through E1/T1 digital trunks or AT0 analog trunks, it seamlessly interconnects with PSTN and traditional TDM PBX networks. Internal users can make and receive calls bidirectionally with the trunk counterpart. It supports PRA and QSIG protocols, with a maximum of 30 channels per E1 and 23 channels per T1, enabling reliable interoperability with the traditional telephone network.

- **Interoperability based on broadband trunks**: Through SIP trunks, it interconnects with IP PBX, softswitch systems, or IMS networks. Internal users can call the counterpart users bidirectionally. It supports standard SIP protocol and multiple codec switching, enabling highly compatible voice

communication across networks and platforms and ensuring service interoperability in multi-vendor environments.

- **Call permission control**: Supports four basic call permission levels: internal, local, domestic long-distance, and international long-distance. It also supports customized permission configuration, allowing outbound permission rules to be flexibly set according to different user levels and business needs, achieving refined permission control and security management to meet special enterprise call permission requirements.

- **Number analysis and processing**: Intelligent analysis of calling and called numbers is performed through prefix codes and number length to implement outbound/inbound permission control and call routing. It supports a maximum number length of 32 digits, 16 internal digits, 1,024 calling-number analyses and 2,048 called-number analyses, and provides 1,024 number translation types.

- **Voice processing and codecs**: Built-in echo cancellation, JitterBuffer, and other voice optimization functions. It supports TOS/DSCP and RTCP protocols, and is compatible with multiple codec formats such as G.711 (A/U-Law), G.729a/b, iLBC, G.722, G.722.1, G.722.2, and Opus, and supports codec priority switching and dynamic selection.

- **Fax**: Fully supports circuit-switched T.30 fax, packet-switched T.38 fax, and G.711 transparent transmission. The end-to-end delay for T.38 must be controlled within 3 seconds and the network must not exceed 4 transcoding gateways. Fax pass-through under G.729 encoding is supported by renegotiating to G.711, ensuring fax service reliability.

3.2 Supplementary Services

- **Voice call**: Supports point-to-point voice calls between PBX internal users or between internal and external telephone users, providing stable and reliable voice communication services to meet daily enterprise office communication needs.

- **Video call**: Supports point-to-point real-time video calls between two video phones. Both parties can see each other's video in real time, improving the intuitiveness and interactivity of remote communication, suitable for HD video conference scenarios.

- **Local number query**: Users can quickly query their own extension number by dialing a specific prefix code preconfigured in the system, making it convenient to know the number information of the currently used terminal at any time and improving number management convenience.

- **Calling line identification presentation**: When a call arrives, the caller's phone number is automatically displayed on the called user's phone screen, helping users identify the caller before answering and improving call recognition efficiency, making it easier to decide whether to answer or record the call information.

- **Calling line identification restriction**: When a user initiates a call as the caller, the system automatically hides the caller number on the called terminal, protecting the caller's number privacy, suitable for special call scenarios where the real number needs to be hidden.

- **Built-in ringback tone service**: The system plays a personalized enterprise-customized ringback tone or prompt tone to the caller, replacing the traditional ringing tone, enhancing the enterprise brand image and professionalism, improving the customer calling experience, and supporting various custom ringback tone configurations.

- **Call hold**: During a call, the user can temporarily suspend the ongoing voice call and place it on hold, and resume it at any time when needed. The other party hears hold music during this period, suitable for scenarios where temporary handling of other matters is required.

- **Call park**: The user can place the current call on hold, then resume the held call on any other phone within the local network using a park retrieval code. If it is not retrieved within the timeout, the system will automatically release the call, and the held party will hear a busy tone, making it convenient for mobile call pickup.

- **Multiple calls**: A user can handle multiple incoming and outgoing calls simultaneously on a single phone terminal, but only one active voice call can be maintained at a time, while other calls remain on hold. Fast switching between calls is supported, improving phone usage efficiency

- **Call waiting**: When a user is on a call and a third-party user calls that user, the system sends a call waiting tone to remind the user that another call is waiting. The user may choose to keep the current call and answer the new call or reject the new call.

- **Call transfer**: During a call, the user can press the transfer key on the phone to transfer the current call to a third-party user, exiting the call and achieving seamless call transfer, suitable for office scenarios where calls need to be handed over to other colleagues.

- **Call deflection**: When the phone is ringing and the user has not answered, pressing the transfer key directly can immediately deflect the incoming call to a designated third-party number, without the user having to answer it, suitable for quickly redirecting calls to relevant personnel.

- **Call forwarding**: Depending on the user's status (unconditional, busy, no answer, offline, etc.), incoming calls are automatically forwarded to a preset number. Multiple forwarding modes can be flexibly configured to ensure calls are not missed and to improve reachability and business continuity.

- **Hotline:** After the user handset goes off-hook, the system automatically calls a preset target number, enabling quick call connection without manual dialing, suitable for emergency calls and dedicated line calls that require fast access to a specific number.

- **Call pickup**: A user can answer an incoming call ringing on another phone, supporting both directed pickup and group pickup modes, facilitating team collaboration and call handling, and improving response capability.

- **Automatic callback:** After dialing a busy or unanswered internal number, the user registers a callback request. When the called user becomes available again, the system automatically calls both parties to establish the connection, avoiding repeated dialing and improving call success rate.

- **Speed dial:** Users can use customized short numbers instead of longer full phone numbers for quick dialing, greatly reducing dialing time and making numbers easier to remember, improving dialing efficiency for frequently called numbers.

- **Do Not Disturb:** After a user enables Do Not Disturb, the system temporarily stops all incoming calls to that user's phone or soft terminal, preventing interruptions. The caller will hear a busy tone or prompt tone, suitable for meetings, rest, and other times when interruptions are not desired.

- **Forced insertion:** Authorized attendants can forcibly join an ongoing call between internal users, forming a three-party call and enabling call monitoring or intervention, suitable for special management scenarios such as call supervision or emergency assistance.

- **Forced release**: Authorized attendants can forcibly disconnect an ongoing call between internal users, immediately terminating the call, suitable for special management control scenarios such as illegal call management or emergency call release.

- **One number service**: Binds one user number to multiple terminal devices. When a call comes in, all bound terminals ring simultaneously, and the user can answer on any ringing terminal. Once answered on one terminal, the others stop ringing, enabling unified access across multiple terminals.

- **Three-party call:** The user can add a third party to the current call without interrupting it, enabling three parties to communicate online at the same time. It supports multi-party collaboration and business discussion, improving communication efficiency and is suitable for multi-person call scenarios.

- **Alarm service:** Users can preset alarm reminder times through the phone or Web interface. The phone rings automatically at the scheduled time to remind the user. It supports one-time or periodic alarm settings and is suitable for meeting reminders, schedule management, and other time reminder scenarios.

- **Hold music:** The system plays enterprise-customized waiting music or prompt tones to users in the call hold state, applicable to call hold, call transfer, call park, and other service scenarios, improving the waiting experience and presenting a professional enterprise image.

- **Absent service:** After a user registers the absent service, other users calling that user will hear an

absence prompt tone played by the system, informing the caller that the called user is currently absent and avoiding ineffective waiting, thereby improving communication efficiency.

- **Paging broadcast:** Uses the telephone system to simultaneously broadcast one-way voice messages to all members in a specified group, enabling one-to-many rapid information delivery, suitable for emergency notifications or public broadcast scenarios where a group needs to receive information at the same time.

- **Advanced manager secretary**: Binds the manager's phone line with the secretary's phone line. Incoming calls ring both simultaneously. The manager can answer directly, or the secretary can answer first, screen the call, and then transfer it to the manager for handling, achieving call filtering and efficient management and improving office efficiency.

- **Emergency call**: In any state such as IP phone locked, unregistered, or call-restricted, the user can directly dial a specific emergency number to place an outgoing call without being affected by any call restriction, ensuring smooth emergency communication and user safety.

- **Cancel all services:** Users can dial a specific prefix code to cancel all registered supplementary service configurations with one click, quickly restoring the default state, while the user's basic service permissions remain unaffected, making it convenient to manage supplementary service settings in batches.

- **Voice service password modification:** The voice service password is used for security authentication in outbound restriction, password-based call restriction, one-number service, service cancellation, voicemail, and other services. Users should regularly change the password through dialing or the Web interface to improve the security and protection of voice services.

- **Busy Lamp Field (BLF):** By using programmable keys on an IP phone to subscribe to the real-time call status of other internal users (idle/busy/ringing/offline), users can know the other party's status before calling and increase call success by calling when the line is idle, improving communication efficiency.

- **Call permission control:** When a user initiates a voice call, the system automatically determines whether the call is allowed based on the caller number's call permission level and the callee prefix's call type. Permission rules can be flexibly configured according to enterprise needs to achieve refined call management.

- **Blacklist/whitelist call restriction**: The system automatically allows or rejects calls from specific numbers according to preconfigured system-level or personal-level blacklist and whitelist rules, achieving number-level call filtering and control and improving communication security and management efficiency.

- **Anonymous call restriction**: When the system cannot obtain the caller's number information, it

automatically prevents the call from being connected, and the called user's phone does not ring, effectively preventing malicious harassment calls and anonymous calls and protecting user communication **security.**

- **Outgoing call restriction:** Users can temporarily restrict the outgoing call permission of the phone by dialing a specific prefix code and entering a password, preventing others from using the phone freely to make external calls. It is suitable for public area phones or temporary outbound restriction security management scenarios.

  \

- **Hunt group:** Users with the same job function or in the same department are organized into a hunt group and configured with a unified access code. After a call dials the access code, the system automatically distributes the call to group members according to a policy such as sequential, cyclic, or random distribution. Once one member answers, the others stop ringing.

- **Simultaneous ringing:** Multiple numbers are bound to one main number. When the main number is called, the terminals of the main number and all bound numbers ring simultaneously. Once any terminal answers, the others stop ringing immediately, enabling parallel call answering and improving call response efficiency.

- **Sequential ringing**: Multiple numbers are bound to one main number. When the main number is called, the terminals of the main number and bound numbers ring sequentially according to a preset order. Once any terminal answers, the others stop ringing, enabling priority-based answering and suitable for tiered response scenarios.

- **DID direct inward dialing**: External users can directly dial the internal users' direct-dial number (DID number) to establish a call connection without going through the automatic attendant extension transfer process, improving inbound efficiency and user experience, suitable for public direct-dial business numbers.

- **Automatic attendant**: Also known as Interactive Voice Response (IVR) service. After an external caller dials the switchboard number, the system plays voice navigation prompts, and the user follows the prompts to press keys or enter an extension number. The system automatically transfers the call to the target extension, achieving intelligent voice guidance and automatic transfer.

3.3 Advanced Services

- **User privilege tier management:** Users are divided into four privilege levels: default, normal, advanced, and privileged. Different levels have different supplementary service permissions and call permissions, and can be configured in association with working hours, enabling refined permission control and differentiated service management based on user level to meet enterprise tiered management needs.

- **Policy-based call restriction**: Supports combinations of multiple policies such as caller prefix-based restriction, system-level/personal-level blacklist and whitelist restriction, caller number Radius

authentication, anonymous call restriction, and out-of-network call time limits. The out-of-network call time limit can be configured with call duration and a reminder one minute before the limit is reached, enabling multi-dimensional call control.

- **Emergency call:** Under the premise that IP phones and the unified communication platform are network reachable, users can initiate a call to the emergency call center in any state. The system locates the geographical location according to the caller number and is not constrained by any call restriction scenario, ensuring smooth emergency communication.

3.4 Intelligent Routing

- **Multi-dimensional routing strategies**: When IP or TDM trunk failures occur, routes are automatically reselected. It supports various route selection strategies based on time period, tariff, load sharing, percentage, user level, and trunk link balancing, enabling automatic rerouting on failure and optimizing for the highest inter-office communication reliability and the lowest cost.

3.5 Voice Conference

- **Scheduled conference**: Users can reserve meetings through the Web self-service system. It supports three modes: self-access mode (participants dial the access code and enter ID and password), chairman-invoked mode (the chairman invokes via phone or Web), and system-invoked mode (the system automatically invokes at the preset time), meeting different conference organization needs.

- **Instant conference**: The conference chairman does not need to make a reservation in advance. They can directly dial the conference access code on the terminal to enter the conference room, and then use voice navigation or phone keys to invite participants to join the conference, enabling quick initiation and flexible invocation, suitable for temporary and urgent conference communication needs.

3.6 Voicemail Service

- **Voicemail service**: Stores and manages voice messages uniformly. Users can dial the retrieval prefix code anytime and anywhere to listen to messages. It supports four forwarding modes: unconditional, no answer, busy, and offline.

3.7 Automatic Attendant Service

- **Interactive voice response:** After an incoming call dials the switchboard number, voice prompts such as "Please dial the extension number" are played. It supports 256 switchboards (245 of which are user-defined scripts), 246 announcement recordings (each up to 300 seconds, total capacity 64 MB), switchboard-plus-extension direct dialing, and time-based playback, meeting diverse IVR requirements.

3.8 Attendant Console

- **Built-in attendant console:** A built-in hard-phone attendant console works with IP phones or POTS phones to provide attendant console services. Incoming calls wait in a queue, and the system automatically assigns idle agents to answer in sequence. It supports call transfer and the forced insertion and forced release functions, meeting basic attendant management needs.

- **External attendant console system**: Supports integration with third-party attendant console server systems and accepts attendant console client registration, enabling richer function expansion, including advanced agent management, call queuing, statistical reports, and other enhanced functions to meet the complex business needs of large call centers.

3.9 Call Detail Records

- **Call detail record management**: Automatically generates user call detail records and saves them to the call record pool. It supports integration with a call record server for centralized storage and processing of call records across multiple devices, provides a visual interface for query, deletion, transmission control, and other maintenance management, and supports combined queries and statistical analysis by caller/callee number, device IP, generation time, and other conditions.

3.10 Security

- **Protocol protection against attacks:** Management traffic and service traffic are isolated into different subnets through network-port diversion, and management traffic is bound to a specific network port to enhance security. It provides SSH encrypted login, supports SRTP media encryption and TLS signaling encryption, and comprehensively ensures voice data transmission security and system protection capability.

- **Password security**: The password must be changed when logging in to the Web interface for the first time. Web and command-line authentication use brute-force protection mechanisms (the account/IP is locked after 3 consecutive failures). HTTPS is used for Web login to transmit authentication information, and multi-layer protection ensures account and system access security.

- **Web security**: Each authorized page or Servlet request verifies the validity of the session ID and user operation permissions. User data is validated on the server side, HTML-encoded before output to the client to prevent malicious code and cross-site scripting attacks. The Web server has no high-level vulnerabilities after security scanning, ensuring Web application security.

4 Application Scenarios

4.1 Single-node Networking

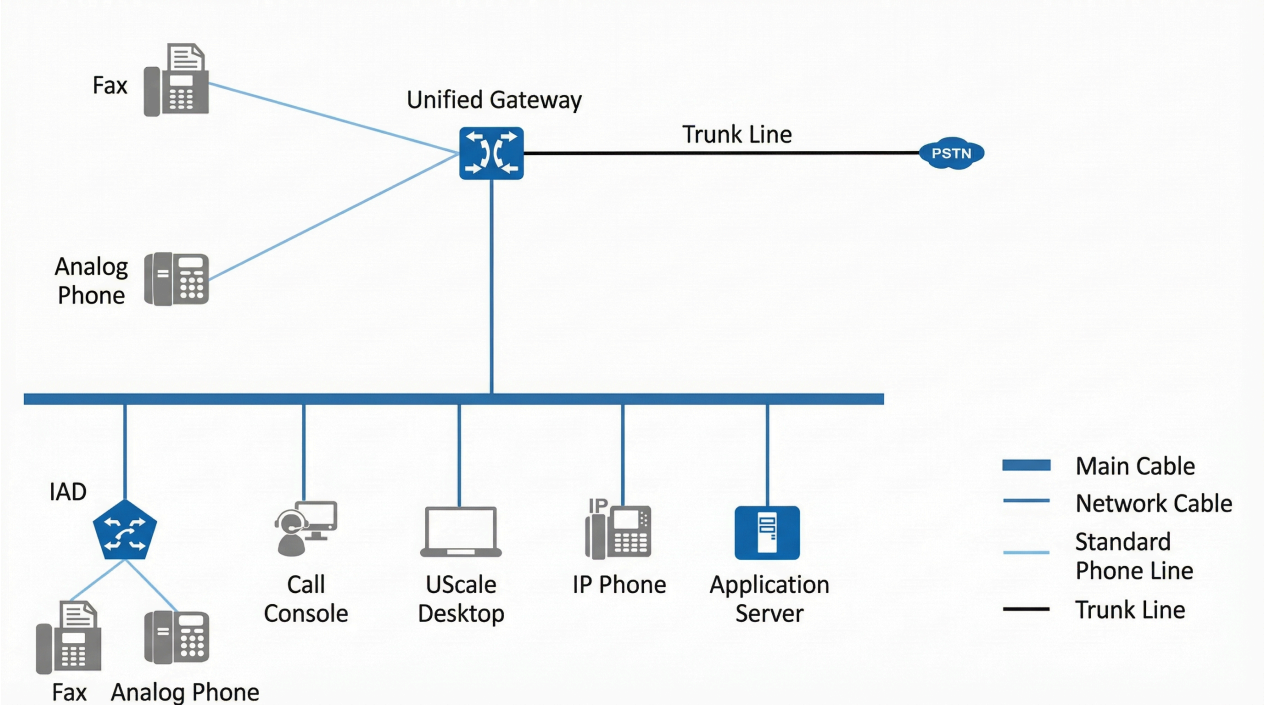
For user capacities below 4000 and with no branch offices, single-node networking can be used. The unified communication platform and business servers are deployed centrally in the enterprise data center, and all terminal users register centrally to the unified communication platform. In the case of small branch offices, IADs can be deployed to proxy user registration to the unified communication platform, or IP phones can be deployed to register to the unified communication platform.

The typical single-node networking solution is shown below.

Networking description:

- Analog phones and fax machines can access the unified communication platform through analog telephone lines. IP phones and SoftPhone terminals can access the unified communication platform through the IP network.

- The unified communication platform can connect to the PSTN through trunks.
- The unified communication platform provides enterprise users with voicemail and voice conference services.



4.2 Distributed Call Management Networking (Peer-to-Peer)

For enterprises with 800 to 4000 users, distributed call management networking in peer-to-peer mode can be adopted. Deploy the unified communication platform at 2 or 3 nodes to provide call services for each node independently. SIP trunks are used between nodes to interconnect and implement call routing between different nodes.

Networking description:

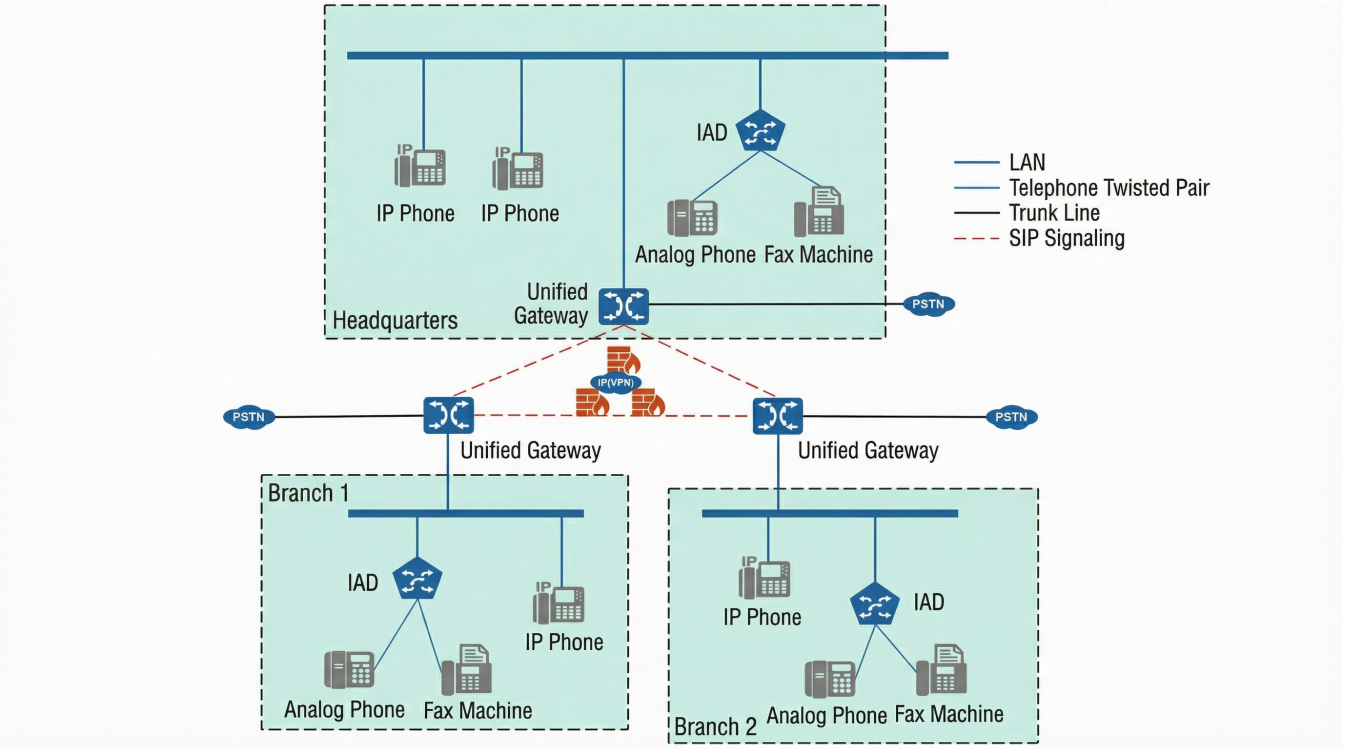
- Networking description: The unified communication platform is deployed at each node and is responsible for user registration, internal calls, and local PSTN calls within that node. The unified communication platforms are interconnected through SIP trunks to implement call routing between different nodes.

- IP phones, attendant console SIP users, UC soft terminal SIP users, analog phones proxied by IADs, and fax machines under each node all register to the unified communication platform of that node.

- The unified communication platform at each node can connect to the PSTN through PRA, QSIG, AT0, and other trunks to achieve local outbound calling.

- Business servers are all deployed at headquarters for centralized service processing.

  The typical distributed call management networking solution in peer-to-peer mode is shown below.



4.3 Distributed Call Management Networking (Converged Mode)

For enterprises with 4000 users, a distributed call management network in converged mode composed of four or more unified communication platforms can be adopted.

Networking description: The unified communication platform is deployed at each node and is responsible for user registration, internal calls, and local PSTN calls within that node. IP phones, attendant console SIP users, UC soft terminal SIP users, analog phones proxied by IADs, and fax machines under each node all register to the voice gateway of that node. The voice gateway of each node can connect to the PSTN through PRA, QSIG, AT0, and other trunks to achieve local outbound calling. The converged gateway provides call routing between nodes. The converged gateways, and the converged gateways and each voice gateway, are interconnected through SIP trunks. Multiple converged gateways can be deployed to achieve active-standby or load-sharing operation. Business servers are all deployed at headquarters for centralized service processing.

The typical distributed call management networking solution in converged mode is shown below.

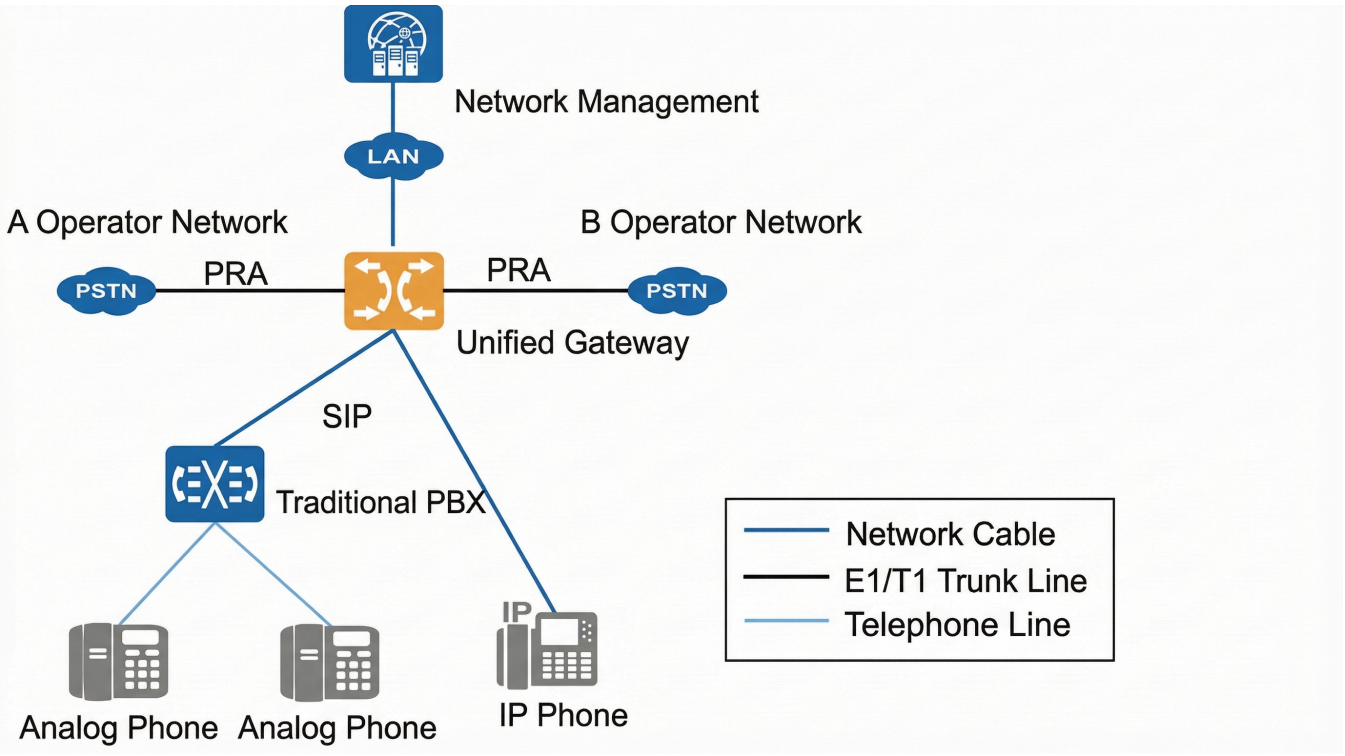
4.4 Traditional PBX bridging scenario

The traditional PBX interworking scenario is mainly used by enterprise network users who already use a traditional PBX but need a lower-cost and more feature-rich solution. By connecting the unified communication platform with the traditional PBX, the configured users under the original PBX remain unchanged, while VoIP voice services and other supplementary services are provided.

Networking description:

- All calls enter and exit through Operator B's network, and no outbound prefix needs to be dialed when making outbound calls. Failure-based rerouting is used. When routing through Operator B's network fails, calls are routed through Operator A's network instead.
- All calls enter and exit through Operator B's network, and no outbound prefix needs to be dialed when

making outbound calls. Failure-based rerouting is used. When routing through Operator B's network fails, calls are routed through Operator A's network instead. The typical traditional PBX networking diagram is shown below.



5. Performance Indicators

5.1 Physical Parameters

Parameter	UCP1202	UCP1600	UCP2120	UCP4131
Dimensions	50 mm (H) × 188 mm (W) × 202 mm (D)	44 mm (H) × 434 mm (W) × 330 mm (D)	88 mm (H) × 434 mm (W) × 330 mm (D)	176.8 mm (H) × 435.8 mm (W) × 330 mm (D)
Weight	1.5 kg	3.9 kg	5.6 kg	9.6 kg
Maximum power consumption at full configuration	< 36 W	< 64 W	< 170 W	< 340 W
Input voltage (AC power supply)	—	100 V	100 V	100 V
Input current (AC power supply)	Input current (DC power supply) 3 A	1 A	2 A	4 A
Power frequency (AC power supply)	—	50 Hz / 60 Hz	50 Hz / 60 Hz	50 Hz / 60 Hz

Parameter	UCP1202	UCP1600	UCP2120	UCP4131
Maximum output power (AC power supply)	36 W	75 W	200 W	400 W
Input voltage (DC power supply)	12 V	Not supported	-48 V	-48 V
Subscriber line distance	3.0 km (when the phone is not connected in parallel)			
Storage temperature	-40°C	-20°C	-20°C	-20°C
Operating temperature, long term	0°C			
Operating temperature, short term	Short-term operation means continuous operation of no more than 12 hours and no more than 8 days in total per year.			
Ambient humidity	5%			
Particle concentration in air	Less than 180 mg/m³			

5.2 Performance and Capacity

Model	UCP1202	UCP1600	UCP2120	UCP4131	Remarks
Recommended number of users	800	800	4000	4000	Only in UDP registration scenarios
Recommended concurrent calls	200	200	800	800	
Maximum number of analog users	16	64	160	160	One AIU-16 board supports access to 16 analog users
Maximum number of FXO interfaces	8	32	80	80	One AIU-8 service board provides 8 FXO interfaces

Model	UCP1202	UCP1600	UCP2120	UCP4131	Remarks
Maximum number of E1/T1 interfaces	4	16	40	40	One DTU service board provides 4 E1/T1 interfaces
Maximum number of wireless ports	4	16	40	40	One WTU service board provides 4 wireless ports
Maximum number of wireless cluster ports	4	16	40	40	

5.3 External Interfaces

Brief introduction to the unified communication platform unit board types

Type	Module Model	Interfaces Provided	UCP1202	UCP1600	UCP2120	UCP4131
General service board	RIU	2/4 wireless interfaces	Yes	Yes	Yes	Yes
General service board	ACU	2 groups of audio input/output interfaces	Yes	Yes	Yes	Yes
General service board	DTU	1/2/4 E1/T1/J1 interfaces; 1 Gigabit Ethernet port; 1 Mini HDMI port and 1 USB 2.0 port	Yes	Yes	Yes	Yes
General service board	WTU	4 GSM/WCDMA/LTE interfaces	Yes	Yes	Yes	Yes
General service board	AIU-16	16 FXS interfaces	Yes	Yes	Yes	Yes
General service board	AIU-8	8 FXS/FXO interfaces	Yes	Yes	Yes	Yes
Main control board	CCU-I-ALDER	Supports 2 Gigabit Ethernet ports, 1 HDMI port, and 1 USB 3.0 port	Yes	Yes	Yes	Yes
Storage expansion board	SEU	1 SATA interface	No	Yes	Yes	Yes
RAID module board	RSU	2 SATA interfaces	No	No	No	Yes
Main control board	CCU-I-TGL	Supports 3 Gigabit Ethernet ports, 1 HDMI port, 2 USB 3.0 ports, and 1 RST key	No	No	Yes	Yes
Switch board	CSU-G	3 Gigabit Ethernet ports, 1 SFP port	No	Yes	Yes	Yes

Type	Module Model	Interfaces Provided	UCP1202	UCP1600	UCP2120	UCP4131
Switch board	CSU-F	2 Fast Ethernet ports	No	Yes	Yes	Yes

5.4 Signaling Protocols

Purpose of the main signaling protocols supported by the unified communication platform

Signaling Protocol Name	Signaling Protocol Purpose
PRA	ISDN (Integrated Services Digital Network) user-network coding signaling, used to enable interoperability between the unified communication platform and ISDN switching equipment, allowing the unified communication platform to access E1/T1 trunks provided by ISDN switching equipment.
QSIG	QSIG signaling, used to enable interoperability between the unified communication platform and switching equipment that supports QSIG signaling, allowing the unified communication platform to access E1/T1 trunks provided by the switching equipment.
SIP	Session Initiation Protocol; used to enable interconnection between unified communication platform groups, and also to access IAD and SIP media packet terminals.
ATO	DC loop analog signaling, used for voice trunk connections between traditional PSTN networks and switches. It can leverage user-applied telephone lines to establish synchronized networking, enabling voice interconnection and providing a simple and effective method for call access.
SSH2	Secure Shell protocol; provides secure remote operations and terminal connections in non-secure networks, used for configuration and debugging of the unified communication platform.
SNTP	Simple Network Time Protocol; used for time synchronization services from the unified communication platform to IP terminals or voice devices.
SNMP v3	Simple Network Management Protocol; used for management and reporting of the unified communication platform.

6. Security Maintenance

With the development of technology and the market, especially the growing informatization and openness of communication systems, products are facing more and more security attacks from viruses, malicious users, and hackers, and security threats are becoming more serious. Implementing systematic security protection for products is also a requirement of many operators and enterprises, as well as the regulations and laws of many countries and regions. Security to a product is like national defense and the military to a country; its importance is self-evident. Therefore, operators or enterprises need to build and maintain security barriers for the entire application system from multiple layers, detecting and handling possible security issues in advance.

Because security risks emerge continuously, it is difficult to fully ensure application system security by relying on technology alone. Therefore, operators need to establish a security management system based on security maintenance recommendations and issues discovered in daily operations to ensure the system operates safely and normally.

6.1 Application Layer Security

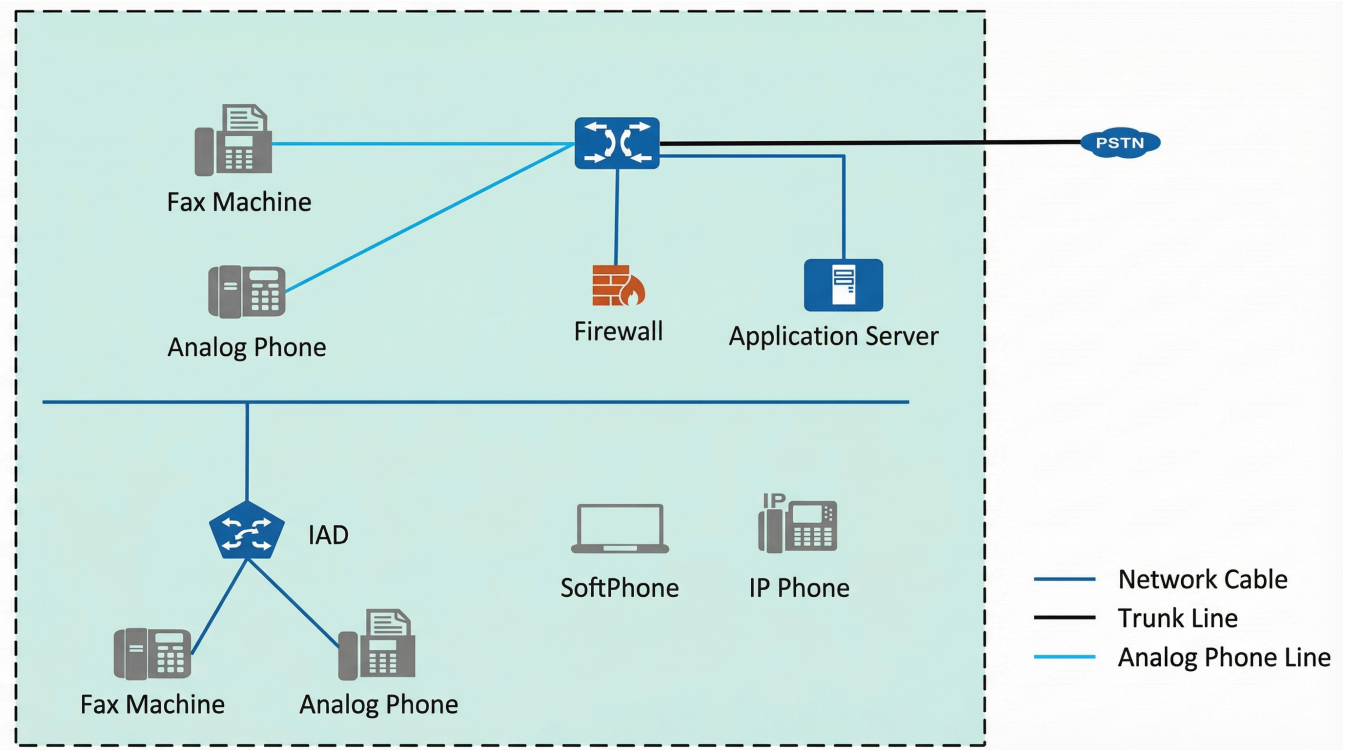
The default account and password list for the main network elements of the unified communication platform is shown in the following table

Functional Module	Default Account and Password	Description
Web Management System	Advanced administrator username: "admin", configuration password: "admin123". Ordinary administrator username and password are both user-defined.	Advanced administrator performs number management, trunk management, system configuration, resource query, etc. on the unified communication platform. This password is the same as the Config mode password in the command line. Ordinary administrator is created by advanced administrator "admin". Both username and initial password are user-defined, mainly used for hierarchical business management in the Web system.
Web Self-Service System	Username and password configured by the user themselves.	Used for ordinary users to log in to the Web interface to configure services.
TLS	Decrypt the built-in TLS certificate of the device.	
Radius Shared Key	Password configured by the user.	Used for encrypting and verifying Radius messages when interfacing with the Radius server.
Night Service	Password configured by the user.	
Authentication Password	Password configured by the user.	In centralized call management networking, this is the data synchronization authentication password between local node and main node. This parameter must be consistent with the "Data Synchronization Authentication Password" value under "System Management → Device Management" on the local node.
Voice Service	Service password configured by the user.	For the method of changing the service password, please refer to "Voice Service Password Modification Usage" for configuration.

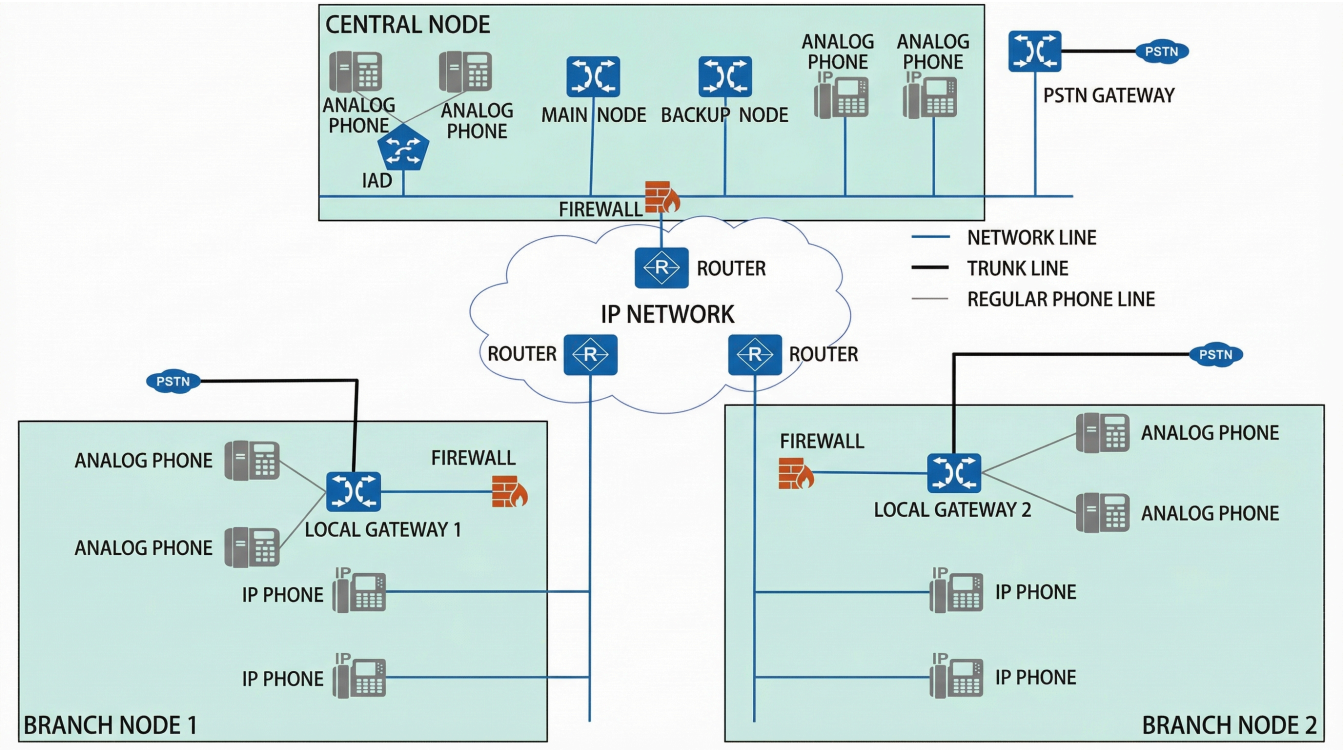
6.2 Network Layer Security

6.2.1 Basic Networking

Networking and security domain isolation: Deployed at the enterprise network egress and ingress, and at user access points, it provides firewall functions and can filter information entering and leaving the enterprise network. It also provides filtering functions and can develop access policies for the unified communication platform according to the communication matrix, forming a security barrier between networks. **Single-node secure networking**

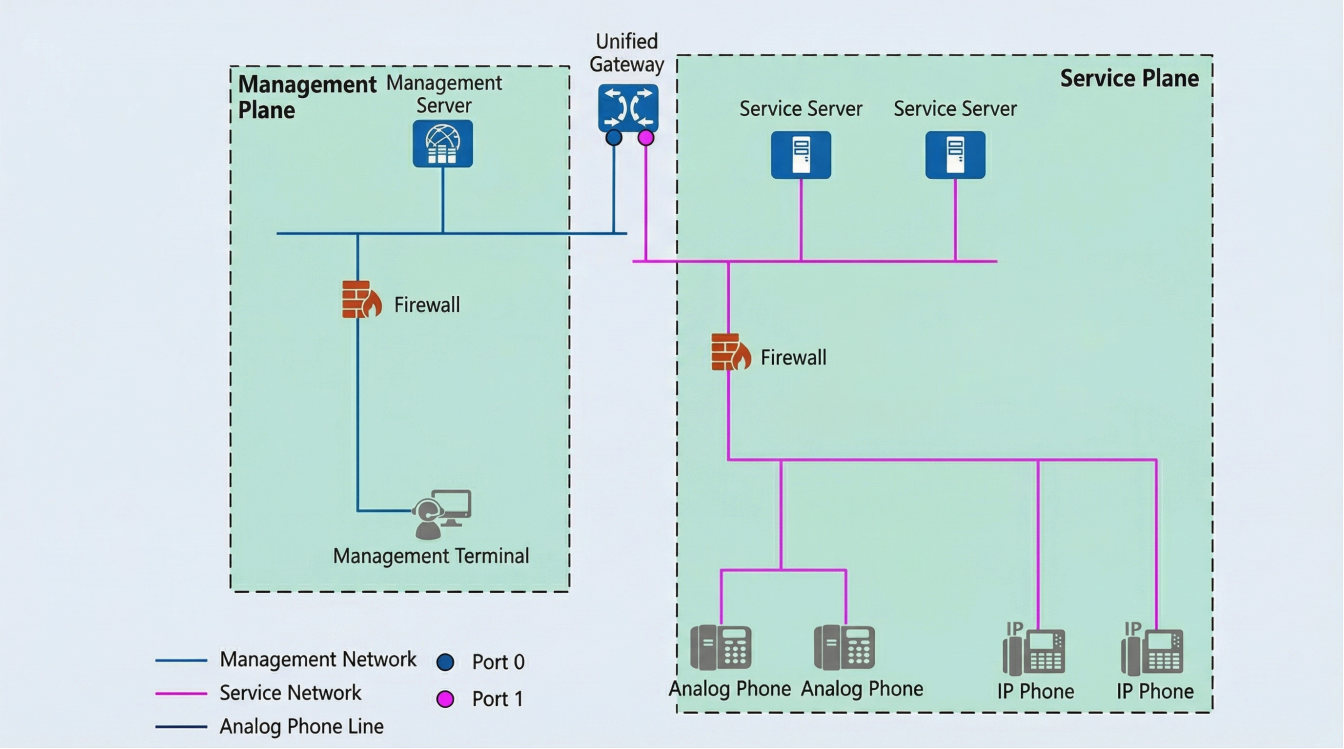


Unified communication platform centralized call management secure networking planning

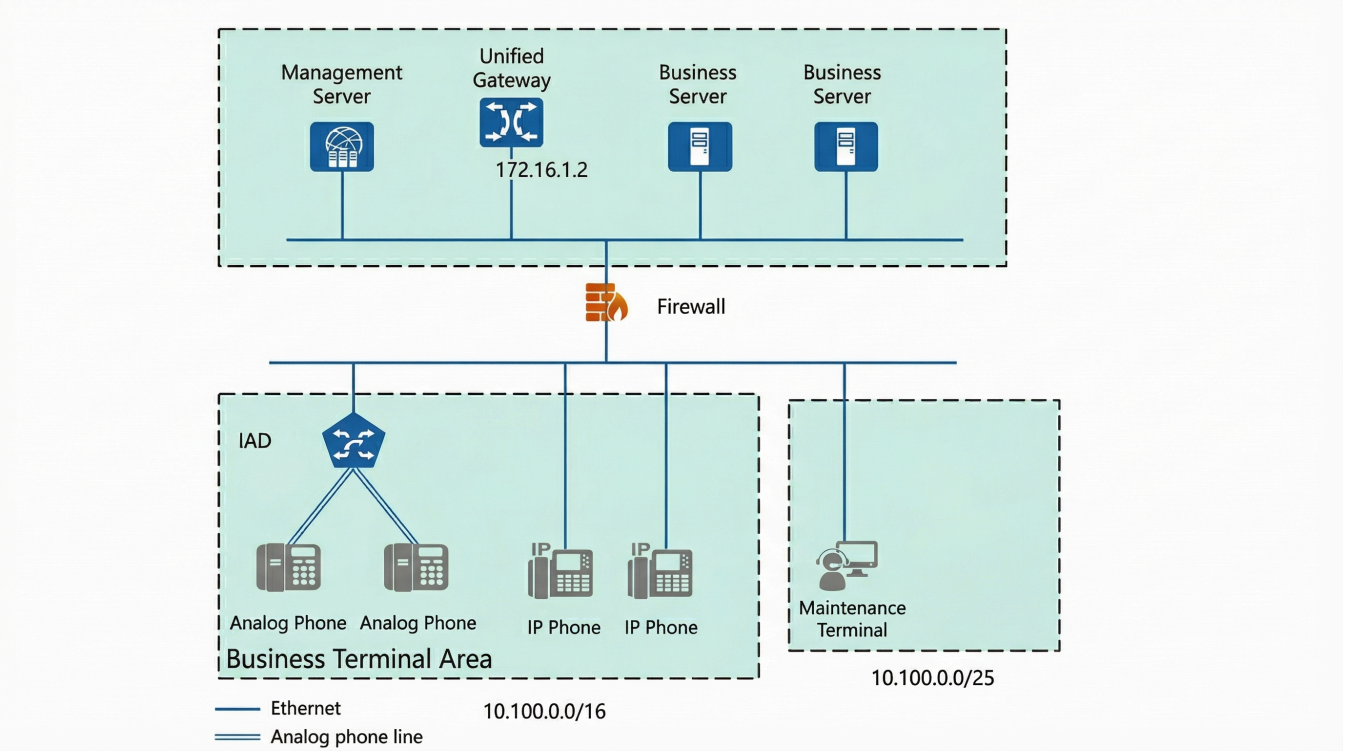


6.2.2 Management Plane Isolation Scheme

Scheme 1: Physical isolation Configure dual-network-port mode on the main control board of the unified communication platform to achieve physical isolation between the management plane and the service plane, ensuring that the management plane is invisible to the service plane. The networking is shown below.



Scheme 2: Firewall policy control Configure access policies for the management plane on the unified communication platform and the firewall, allowing only IP addresses from the management terminal zone to access the URL or protocol ports of the management plane, thereby ensuring that these management entry points are invisible to the service terminal zone. The networking is shown below.



6.2.3 Network Security Maintenance

6.2.3.1 Unified Communication Platform Security Check

Key point 1: Check the unified communication platform password.

Key point 2: Check the device operating status. If the unified communication platform operates abnormally, local service unavailability or global service unavailability may occur, affecting system functions. You need to check the following items to ensure system availability:

- Call record pool status
- Single-board CPU utilization
- Single-board status
- User status

6.2.3.2 Firewall Security Check

Prerequisite: If a firewall is enabled in the network, you need to perform regular security checks on the firewall.

(1) Check system status information

- System version
- System clock
- Terminal users

- Initial configuration information
- Configuration information in the current view
- Current configuration information
- Debug switch status
- Technical support information
- ESN (Equipment Serial Number)

  \

(2) Check the configuration information of security zones

- If the firewall is placed between the internal network and the external network, the security zone configuration information and inter-zone security configuration information need to be checked.

(3) Check the default packet filtering action

- Check the default packet filtering action to understand which packets can be accepted and which packets need to be rejected. If incorrect configuration information is found, please modify it in time.

  \

(4) Check NAT configuration information

- If NAT traversal exists in the network, the address translation - -configuration and the corresponding current system configuration commodity scope need to be checked. If the configuration is incorrect, please modify it in time.

  \

(5) Check VLAN/IP information

- VLAN (Virtual Local Area Network) logically divides a physical LAN into multiple broadcast domains. Hosts within a VLAN can communicate directly, while VLANs cannot directly communicate with each other, thereby limiting broadcast traffic to a single VLAN. Because VLANs cannot directly access one another, network security is improved. Please check the VLAN enable status, VLAN configuration information, and whether the IP addresses are abnormal. If any abnormality is found, it must be handled promptly.

6.3 Management Layer Security

6.3.1 System Maintenance Security Principles

(1) Minimum principle

- Minimum services and components
- Distinguish the purpose and role of servers, and prohibit installation of unnecessary services and components.
- Internal components of services should also be reduced according to the above principle.

  \

(2) Minimum accounts

- Carry out strict account management and implement strict account policies.

- Strictly control the addition, modification, and deletion of accounts and groups in the system.
- Delete all accounts and user groups not in use on the system.

  \

(3) Minimum privileges

- Reduce the privileges of system services, groups, and accounts as much as possible.
- Strictly control the authorization of the operating system.
- Prohibit unnecessary accounts from accessing resources they do not need.

  \

(4) Dedicated principle

- Avoid using one host to serve multiple service roles whenever possible.
- Partition by dedicated use, isolating the partitions where systems, applications, and data reside.

  \

(5) Audit principle

- Monitor host operations through logs and other feasible methods.
- Audit failed access to important system resources.
- Audit successful access to critical system resources.
- Audit both successful and failed modifications to access control policies.

6.3.2 Recommended Protocol Selection

- The unified communication platform supports SSH protocol login.
- The unified communication platform supports access to the Web interface through HTTP/HTTPS protocols. To ensure system security, please use
- HTTPS when accessing the device Web interface through a browser.
- The unified gateway supports file loading and backup through TFTP/FTPS protocols. To ensure system security, please use the FTPS protocol when performing loading or backup operations on the device.

6.3.3 Account Maintenance Recommendations

System administrators should routinely inspect accounts, including:

- Whether accounts for the operating system and database are necessary, and whether temporary accounts have been deleted.
- Whether account privileges are reasonable.
- Inspect and audit account login and operation logs.

6.3.4 Password Maintenance Recommendations

The host administrator password should be kept by a designated person.

- Pay attention to encryption when transmitting passwords, and avoid sending passwords by email as much as possible.

- Passwords need to be stored in encrypted form.
- Please change accounts and passwords regularly, once a month.

6.3.5 Log Maintenance Recommendations

Use auditing and logging to help discover suspicious activity. The system must record logs for important operations, including system parameters, tariff configuration, and release.

(1) Check logs regularly Check system logs, application logs, and security logs regularly.

- If any abnormal logs are found, report them to the higher-level department in time.
- If the cause cannot be identified or the issue cannot be resolved independently, promptly seek help from OpenVox Communication Co., Ltd.

(2) Back up logs regularly Logs should be backed up regularly, and backup files should be archived on external media (disk, tape, optical disc, etc.).

Logs should be deleted in a timely manner after backup to free log space.

6.3.6 Backup Recommendations

For security protection purposes, perform backups before and after daily security configuration maintenance and fault handling.

6.3.7 Defect Reporting Recommendations

If a user reports to OpenVox Communication Co., Ltd. that the system has been attacked, the company will handle it in one of the following two ways depending on the specific situation of the attack:

- If a security incident occurs on site, OpenVox technical support engineers will provide remote or on-site support, working with the user's maintenance personnel to reduce the impact of the attack on the system and improve the handling process of the on-site incident report.

  \

- If no security incident occurs, OpenVox technical support engineers will enter the issue into the database and pass it to the R&D team. After the R&D team finds a solution, the technical support engineer will analyze the impact of implementing the solution on on-site services and provide recommended remediation steps.

6.3.8 Security Emergency Response Mechanism

Users need to establish an emergency response mechanism for security incidents so that, after a security incident occurs, production can be restored and problems resolved as quickly as possible, minimizing losses.

7 Standards Compliance

Protocol/technical compatibility standards

Protocol/Technology	Compliance Standards
PRA	YDN 034-1997 ISDN User-Network Interface Technical Specification, ITU-T G.962, ITU-T I.431, ITU-T Q.921, ITU-T Q.931

Protocol/Technology	Compliance Standards
QSIG	ITU-T G.962, ITU-T I.431, ITU-T Q.921, ECMA-142, ECMA-143, ECMA-148, ECMA-157, ECMA-163, ECMA-164, ECMA-165, ECMA-173, ECMA-174, ECMA-185, ECMA-186, ECMA-241, ECMA-242
SIP	RFC 3261–3263, RFC 3265, RFC 2976, RFC 3311, RFC 3420, RFC 3515, RFC 3842
SDP	RFC 2327-1998, RFC 3264
T.30	ITU-T T.30 (07/2003)
T.38	ITU-T T.38
Echo Cancellation	ITU-T G.165, ITU-T G.168
EMC	EN 55022:2006+A1:2007; CISPR 22:2006; EN 55024:1998+A1:2001+A2:2003; CISPR 24:1997+A1:2001+A2:2002; ETSI EN 300 386 V1.4.1:2008; VCCI V-3:2009; ICES-003:2004; AS/NZS CISPR 22:2006; IEC 61000-6-2:2005/EN 61000-6-2:2005; IEC 61000-6-4:2006/EN 61000-6-4:2007
Safety	IEC 60950; UL 60950; EN 60950; AS/NZS 60950
DTMF	ITU-T Q.23, ITU-T Q.24; RTP transmission; RFC 2833
Voice QoS	IEEE 802.1P/Q; TOS priority 0–7, service type 0–4; DSCP priority 0–63
SRTP	AES (128-bit)
TCP/IP protocols	IPv4; IPv6 (internal calls only, IPv4/IPv6 coexistence not supported)