

**HUAWEI SE2900 Session Border Controller
V300R002C10**

Product Description

Issue **01**
Date **2016-01-15**

Copyright © Huawei Technologies Co., Ltd. 2016. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

Contents

1 About This Document	1
2 Product Positioning	2
3 Highlights	7
3.1 Large Capacity and High Integration.....	7
3.2 Large-Capacity Encryption and Decryption	9
3.3 Flexible Resource Allocation.....	10
3.4 Efficient Platform	12
3.5 Efficient Operation and Maintenance	16
3.6 High Reliability	19
3.7 Industry-leading Security Defense Capability	25
4 Services and Functions	31
4.1 Feature Matrix	31
4.2 A-SBC Basic SW	43
4.2.1 SIP Call.....	43
4.2.2 Media Policy.....	44
4.2.3 MSRP Proxy	46
4.2.4 DNS Query	47
4.2.5 Virtual SBC.....	48
4.2.6 SIP Keepalive and NAT Traversal	49
4.2.7 Address Overlapping.....	51
4.2.8 Topology Hiding	54
4.2.9 IP Layer Security	55
4.2.10 Signaling Plane Security	57
4.2.11 Media Plane Security	58
4.2.12 SIP over TCP	60
4.2.13 DSCP Remarking.....	60
4.2.14 H.248 Proxy.....	61
4.3 I-SBC Basic SW	63
4.3.1 SIP Call.....	63
4.3.2 Media Policy.....	64
4.3.3 MSRP Proxy	65
4.3.4 Address Overlapping.....	65

4.3.5 Topology Hiding	68
4.3.6 IP Layer Security	69
4.3.7 Signaling Plane Security	71
4.3.8 Media Plane Security	72
4.3.9 SIP over TCP	73
4.3.10 DSCP Remark	74
4.3.11 REFER Proxy	75
4.4 Optional Features	75
4.4.1 SIP over TLS	75
4.4.2 MSRP over TLS	76
4.4.3 RFC2198 Redundancy	77
4.4.4 Media Bypass	78
4.4.5 SIP Header Manipulation	84
4.4.6 Diameter Mediation	85
4.4.7 SRTP	85
4.4.8 Firewall Traversal	86
4.4.9 QoS Assurance	87
4.4.10 IMS-AKA/IPSec	90
4.4.11 ATCF/ATGW	91
4.4.12 P-CSCF	92
4.4.13 E-CSCF/EATF	94
4.4.14 Flexible Routing	95
4.4.15 SIP-I/SIP-T	96
4.4.16 SIP over SCTP	98
4.4.17 IPSec Tunnel	99
4.4.18 IPv6	99
4.4.19 IP-PBX Trunking	101
4.4.20 Audio Transcoding	102
4.4.21 Charging	104
4.4.22 Security Enhancement Function	106
4.4.23 Redundancy of Core Network	108
4.4.24 SIP-H.323 Interworking	111
4.4.25 Standard Definition/High Definition Video	113
4.4.26 Dual-System Hot Backup	114
4.4.27 Security Traversing Gateway	117
4.4.28 VoLTE Roaming	117
4.4.29 VoWiFi Access	118
4.4.30 MSRP B2BUA	119
5 Product Architecture	121
5.1 Hardware Structure	121
5.1.1 Physical Structure	121

5.1.2 System Architecture	125
5.2 Software Architecture	127
6 Interfaces and Protocols	134
6.1 Physical Ports	134
6.2 Protocols and Interfaces	137
6.3 Standards Compliance	146
7 Application Scenarios	147
7.1 SE2900 in the RCS Solution	147
7.2 SE2900 in the VoBB Solution	149
7.3 SE2900 in the VoLTE Solution	151
7.4 Application of the SE2900 in Network Interconnection	155
7.5 SE2900 on the NGN	160
8 Operation and Maintenance	162
8.1 Fault Management	163
8.2 Configuration Management	165
8.3 Performance Management	167
8.4 Security Management	168
8.5 Charging Management	169
9 Technical Specifications	172
9.1 Performance Specifications	172
9.2 Reliability Specifications	186
9.3 Power Consumption Specifications	187
9.4 Cabinet Specifications	188
9.5 Environment Specifications	189
9.6 EMC Specifications	190
9.7 Environment Requirements	193
9.7.1 Storage Environment	193
9.7.2 Transportation Environment	195
9.7.3 Operating Environment	197
10 Differences Between the SE2900 and SE2600	200
11 Acronyms and Abbreviations	210

1 About This Document

Overview

This document briefs Huawei SE2900 session border controller (abbreviated as SE2900 or SBC), covering various aspects such as product positioning, features, services and functions, product structure, interfaces and protocols, application scenarios, and technical specifications.

This document helps you know the main functions of the SE2900, such as security and signaling/media proxy, that are used in solutions, such as VoBB, Rich Communication Suite (RCS), and VoLTE.

Intended Audience

This document is intended for:

- Management personnel and planning and design personnel of carriers
- Huawei marketing engineers

Change History

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

Issue	Release Date	Description
02	2015-04-07	Second release.
01	2015-01-16	First release.

2 Product Positioning

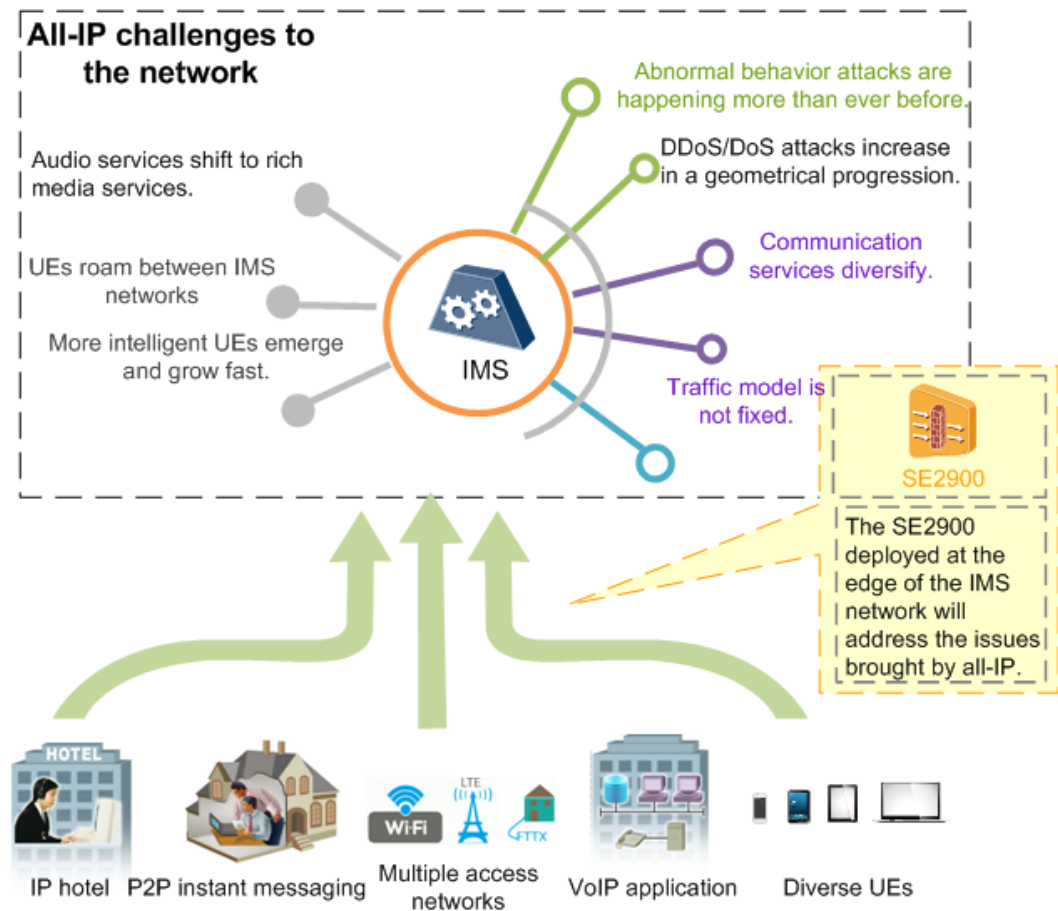
SE2900 Positioning

VoLTE and fixed mobile convergence (FMC) impose new requirements for the SBC (a border gateway of an all-IP network):

- Shift from hierarchical security defense to associated security defense
The shift to all-IP networks and integration of services, UEs, and access networks make the core network more vulnerable to attacks. DDoS/DoS attacks increase in a geometrical progression. Such abnormal behavior attacks as ultra-short calls are happening more than ever before. The SBC must be highly secure to defend against such attacks. The traditional SBC employs hierarchical security defense, including IP layer, media plane, signaling plane, and service security defense. Such a mechanism lacks effective coordination so that defense is inefficient. The shift from hierarchical defense to associated defense becomes inevitable. In addition, the SBC must be highly reliable and have a large capacity to combat IP network instability and traffic burst.
- Evolution from audio services to rich media services
Nowadays, VoLTE/Rich Communication Suite (RCS) services are rapidly developing and carriers begin to exchange rich media messages, such as video and instant messaging (IM) messages as well as audio messages. The I-SBC must be able to resolve the issues associated with rich media services, such as interworking, routing, roaming, and charging.
- Shift from single border control to comprehensive border control
The traditional SBC supports fixed VoIP services only. The SBC must have service integration and long term evolution capabilities to accommodate a variety of new services, including VoLTE, RCS, unified communications (UC), and WebRTC services. With the emergence of more intelligent UEs, change of user behavior, and diversity of service types, the traffic model is no longer fixed. The SBC must support flexible resource allocation and scalability.

Huawei SE2900 is launched to adapt to the situation. Figure 2-1 shows the SE2900 positioning.

Figure 2-1 SE2900 positioning

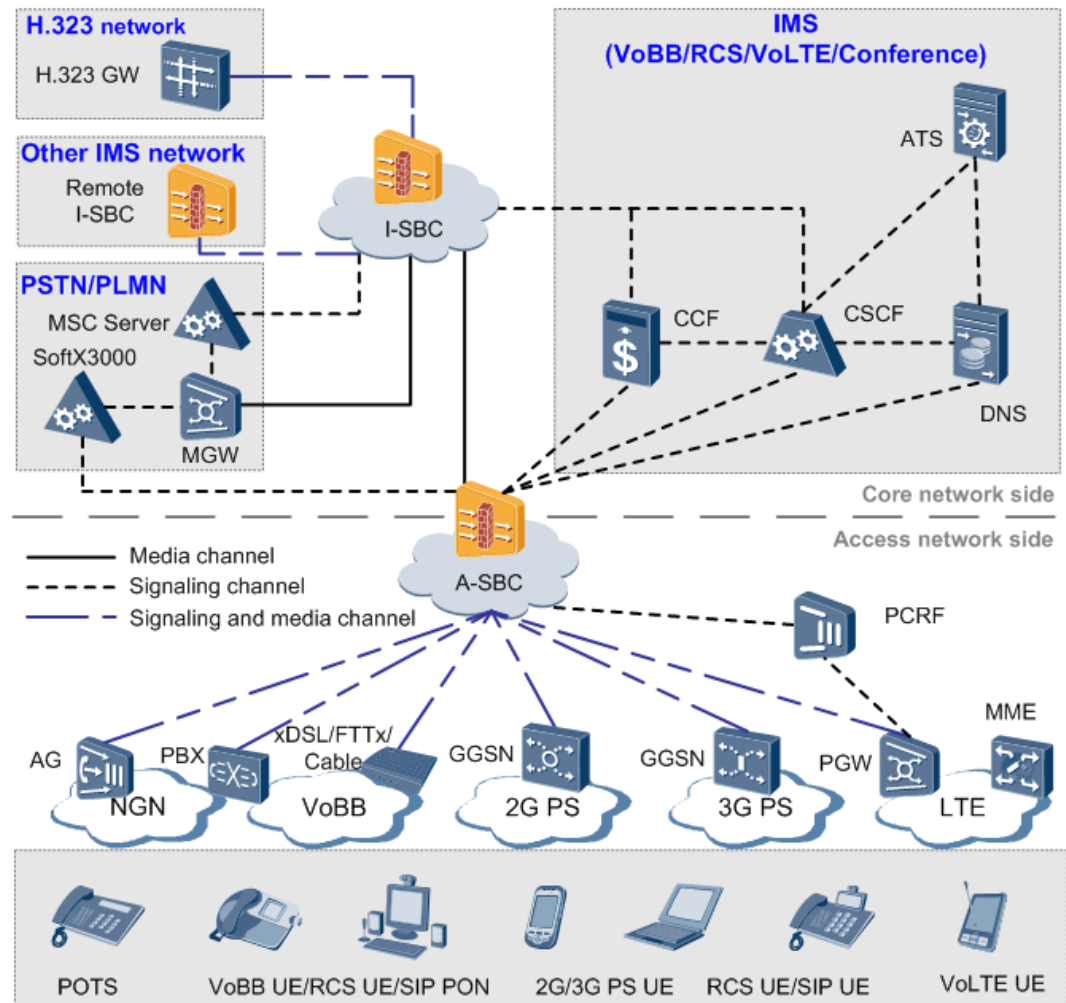


SE2900 Application

The SE2900 is a session border controller (SBC) that participates in the implementation of solutions, such as VoBB, RCS, VoLTE, Conference, Hosting UC and one network. The SE2900 is deployed at the border of different parts of an IP network or at the border of different IP networks to control voice, video, and data sessions. The functions of the SE2900 include access control, security, QoS, audio transcoding, media firewall, media/signaling proxy, NAT traversal, firewall traversal, flexible routing, network redundancy, and encrypted transmission of signaling/media.

The SE2900 can serve as an A-SBC or I-SBC. The SE2900 can be deployed at different locations on the network, depending on the functions it is expected to provide. (Figure 2-2 shows the SE2900 networking.) The SE2900 provides connectivity between the core network and the access network and between different IP networks, enabling services to be provided across networks.

Figure 2-2 SE2900 networking



AG: access gateway
 ATS: advanced telephony server
 CS: circuit switched domain
 DNS: domain name server
 GGSN: gateway GPRS support node
 I-SBC: interworking session border controller
 MGW: media gateway
 MSC: mobile switching center
 PBX: private branch exchange
 PS: packet switched domain
 UE: user equipment
 VoLTE: voice over LTE

A-SBC: access session border controller
 CCF: charging collection function
 CSCF: call session control function
 FTTx: fiber to the x
 H.323 GW: H.323 gateway
 LTE: Long Term Evolution
 MME: mobility management entity
 PGW: packet data network (PDN) gateway
 PCRF: policy and charging rules function
 RCS: Rich Communication Suite
 VoBB: voice over broadband
 xDSL: x digital subscriber line

The SE2900 serves as an A-SBC and supports UE access over the VoBB network, 2G/3G PS network (for example, Wi-Fi or WiMAX access). The SE2900 will be able to serve as an I-SBC and support the NGN and LTE access shown in Figure 2-2.

- When functioning as an A-SBC, the SE2900 can serve as the access border control function (A-BCF) and border gateway function (BGF):
 - A-BCF: deployed between the access network and the core network. It is responsible for protocol access and security at the control plane. The A-BCF supports SIP/H.248/MGCP access and instructs the BGF to implement media access and audio transcoding.
 - BGF: also deployed between the access network and the core network. It is responsible for media packet processing. The BGF supports RTP/RTCP/Message Session Relay Protocol (MSRP) access and audio transcoding.
- When functioning as an I-SBC, the SE2900 can serve as the interconnection border control function (IBCF) and BGF to implement interworking between two different networks (for example, two IMS networks).
 - IBCF: deployed between different core networks. It is responsible for protocol interworking and security at the control plane. The IBCF supports interworking between 3GPP SIP signaling and SIP/H.323 signaling and media interworking and audio transcoding by controlling the BGF. For example, on the one network, the IBCF supports interworking between the MSC server (MSOFTX3000) and the SoftX3000 through the MGW; on a network providing convergent conference services, the IBCF supports the H.323 gateway and the call session control function (CSCF).
 - BGF: deployed between two different core networks. It is responsible for media packet processing. The BGF supports RTP/RTCP/MSRP interworking and audio transcoding.
- The SE2900 provides the embedded NE function, reducing the complexity and saving the expenditure of deploying a separate NE.
 - Embedded P-CSCF
The P-CSCF is the entry point of the control plane on the IMS network (visited network). It is a proxy for all SIP messages, including REGISTER, INVITE, and Presence messages, from the access network (in the visited network) to the serving-CSCF (S-CSCF) or interrogating-CSCF (I-CSCF) in the home network.
Benefits
 - Embedded ATCF/ATGW
In eSRVCC handovers, the SE2900 provides an access transfer control function (ATCF)/access transfer gateway (ATGW) as well as a P-CSCF. The ATCF/ATGW is deployed between the P-CSCF and I-CSCF/S-CSCF, and media is anchored on the ATGW for calls during which a handover is likely to occur. During the handover of a UE, the ATCF anchors the media information of the UE on the ATGW so that the remote media information does not need to be updated when the UE is handed over from the E-UTRAN to a UTRAN or GERAN, minimizing call interruption.
 - Embedded E-CSCF/EATF
The emergency-call session control function (E-CSCF) enables the SE2900 to process and route emergency calls to an emergency center (EC). The emergency access transfer function (EATF) enables the SE2900 to anchor emergency calls and switch emergency calls from a packet switched (PS) network to a circuit switched (CS) network for call continuity.

- CCF can be embedded in the SE2900 or deployed as an external NE. Huawei provides the iCG9815, which is an IMS charging gateway, as the CCF.

The SE2900 provides access to NGNs and IMS networks and can serve as an I-SBC (IBCF + BGF) to implement interworking between two NGNs or IMS networks.

- IBCF: deployed between different core networks. It is responsible for protocol interworking and security at the control plane. The IBCF supports interworking between 3GPP SIP signaling and SIP/H.323 signaling and media interworking and audio transcoding by controlling the BGF. For example, on the one network, the IBCF supports interworking between the MSC server (MSOFTX3000) and the SoftX3000 through the MGW; on a network providing convergent conference services, the IBCF supports the H.323 gateway and the call session control function (CSCF).
- BGF: deployed between two different core networks. It is responsible for media packet processing. The BGF supports RTP/RTCP/MSRP interworking and audio transcoding.

3 Highlights

About This Chapter

- 3.1 Large Capacity and High Integration
- 3.2 Large-Capacity Encryption and Decryption
- 3.3 Flexible Resource Allocation
- 3.4 Efficient Platform
- 3.5 Efficient Operation and Maintenance
- 3.6 High Reliability
- 3.7 Industry-leading Security Defense Capability

3.1 Large Capacity and High Integration

As the number of IP network users increases rapidly, the number of VoIP users who register or access services concurrently is also on the rise, posing higher requirements on device performance. In addition, security is becoming an increasingly serious issue for information transmission on the IP network. To meet these challenges, the SBC must have higher capacity and processing performance.

The SE2900 uses the OSTA5.0 platform, high-performance chips, and high-speed bus technologies. These technologies enable the SE2900 to have higher computing capability than traditional servers. The SE2900 uses the cluster technology and distributed software architecture. Capacity can be expanded by adding SPUs so as to accommodate more users and service loads.

An SE2900 subrack is 3U high and supports a range of 250,000 users (when a pair of SPUA0s is installed) to 1,200,000 users (when two pairs of SPUA1s are installed) in the case of full SPU configuration. When SPUs and VPUs are installed in the ratio of 1:1, an SE2900 subrack supports a range of 250,000 users (when a pair of SPUA0s and a pair of VPUA0s are installed) to 500,000 users (when a pair of SPUA1s and a pair of VPUA1s are installed). The SE2900 supports self-cascading of a maximum of three subracks using BASE and Fabric buses. The SE2900 with three cascaded subracks supports a maximum of 4,000,000 users (when six pairs of SPUA1s are fully configured) as shown in Figure 3-1 and supports a maximum of 1,900,000 users (when three pairs of SPUs and three pairs of VPUs are configured) as shown in Figure 3-2.

Figure 3-1 Three-subrack cascading (when six pairs of SPUA1s are fully configured)

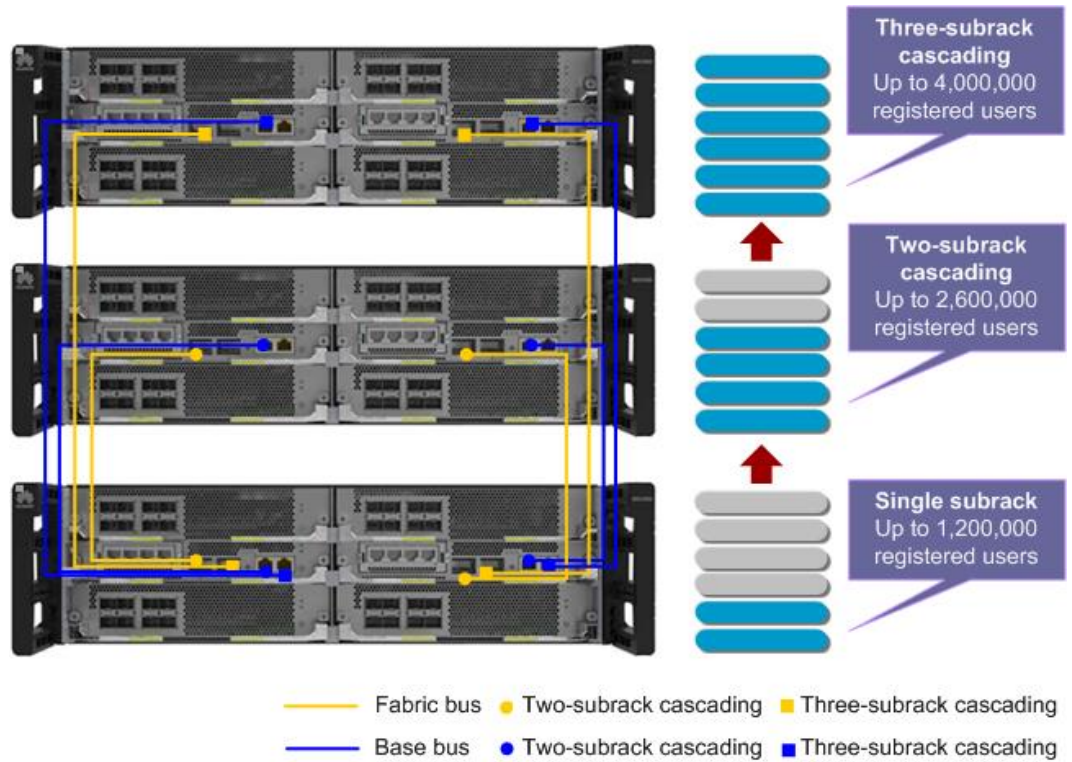
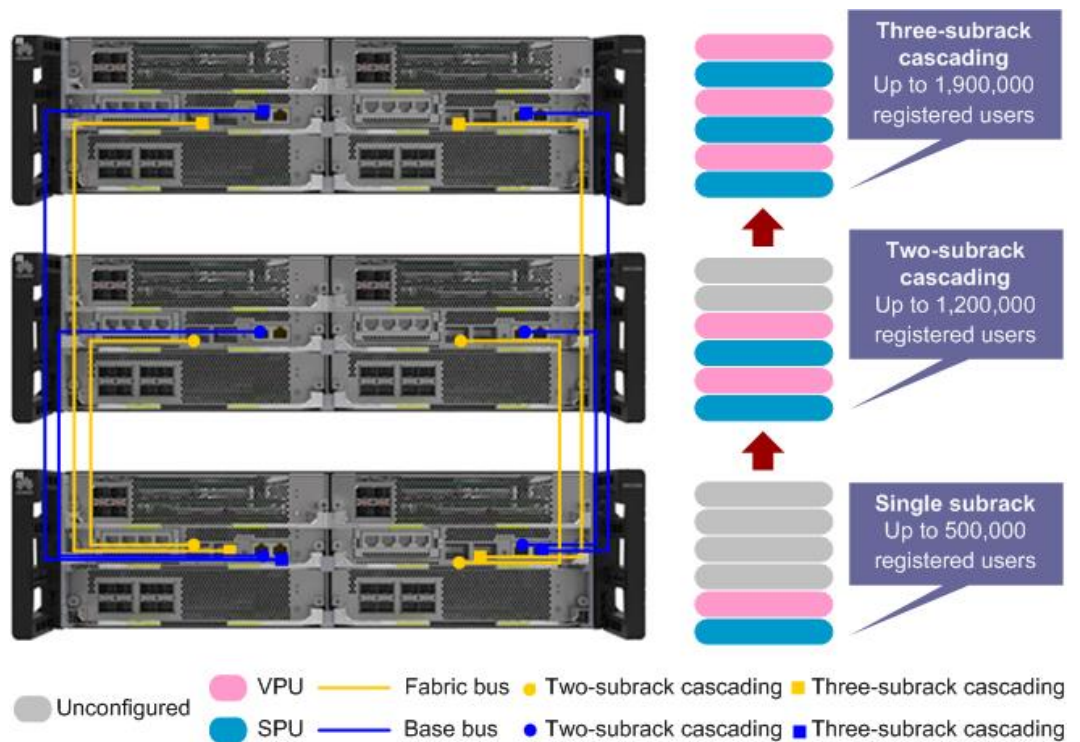


Figure 3-2 Three-subrack cascading (when three pairs of SPUs and three pairs of VPUs are configured)





NOTE

The functions of BASE bus and Fabric bus are as follows:

- BASE bus: provides a control path for the management plane and is mainly used for loading software and transmitting alarm and maintenance information.
- Fabric bus: provides data channels for the service plane of the system and is mainly used for transmitting service-related messages.

SPUs operate in 1+1 backup mode to meet the reliability requirements on large-capacity services, such as the VoLTE service. VPUs operate in load-balancing mode to meet the requirements for conversion between codecs used by different users. The SE2900 is space-saving and easy to deploy, and meets the requirements for centralized management. It can be placed together with other core servers in one cabinet.

The SE2900 has the following advantages:

- Reduces the costs and labor in device maintenance.
- Reduces the number of NEs on the network, which simplifies the network architecture.
- Reduces power consumption and rent.

The SE2900 also has high-performance forwarding capability. Each subrack supports 40 Gbit/s forwarding capability.

3.2 Large-Capacity Encryption and Decryption

As more and more smart phones are available on the market, the number of people who use smart phones to surf the Internet is also on the rise. People install various applications on their smart phones. Telecommunications vendors are also opening more interfaces on their devices. All these factors combined leads to an explosion in the behavior of eavesdropping around the world. In addition, numerous software designed to intercept user information also poses serious threats to people's privacy and communications security. In such a situation, providing secure call services to users is inevitably a key consideration for carriers. On the IP network, SIP signaling is transmitted in plaintext, which is insecure. However, existing security defense mechanisms, such as HTTP Digest authentication, cannot implement secure signaling transmission. In RTP packetization, no data verification or encryption is performed. Therefore, security and integrity cannot be ensured during data transmission.

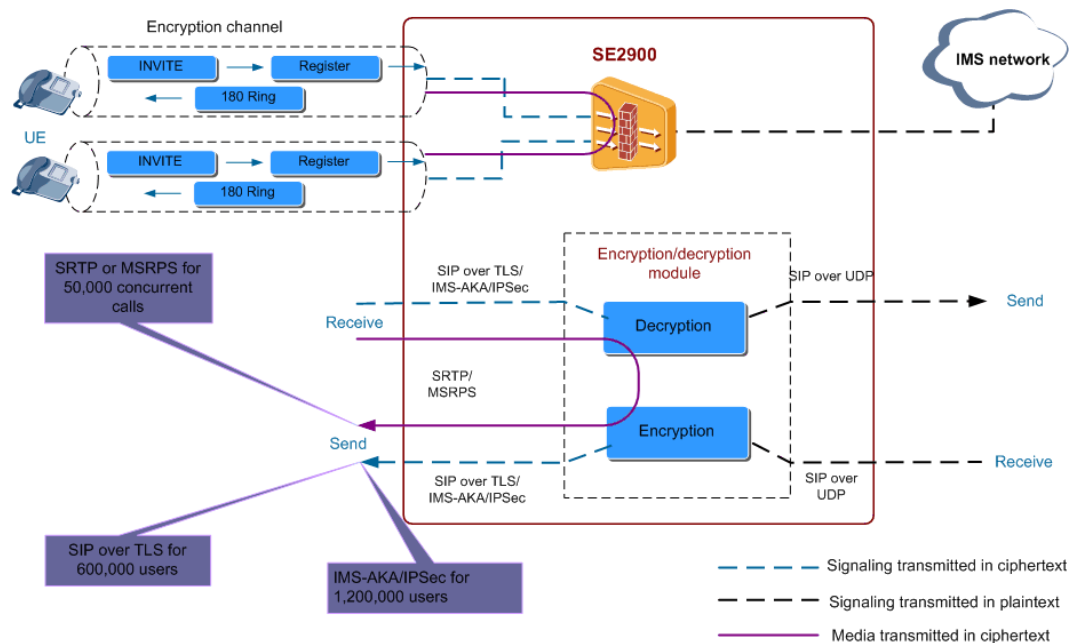
Carriers are shifting from price-oriented competition to improving service quality, offering richer services, and exploring the potential demands of users. In such a situation, carriers must be able to ensure the reliability and security of the value-added services they provide.

The SE2900 uses SIP over TLS to transmit signaling and uses Secure Real-time Transport Protocol (SRTP) and Message Session Relay Protocol over TLS (MSRPS) to transmit media streams for access-side networks, such as the RCS and VoBB networks. Figure 3-3 shows SIP over TLS encryption and IMS-AKA/IPSec.

The SE2900 uses a dedicated encryption and decryption chip. The encryption and decryption performance specifications of one SE2900 subrack are as follows:

- SRTP or MSRPS for 50,000 concurrent calls
- SIP over TLS for 1,200,000 users
- IMS-AKA/IPSec for 1,200,000 users

Figure 3-3 SE2900 encryption



In the session creation or establishment procedure:

- After a TLS connection (effective for the whole registration phase) is established between a UE and the SE2900, the SE2900 uses TLS to encrypt SIP signaling messages between the UE and the SE2900. The TLS connection ensures secure transmission of signaling messages.
- The SE2900 supports IMS-AKA/IPSec. After a TCP/TLS connection is established between a UE and the SE2900 by using IMS-AKA/IPSec, the SE2900 uses TCP/TLS to encrypt SIP signaling messages between the UE and the SE2900. The TCP/TLS connection ensures secure transmission of signaling messages.
- The SE2900 supports SRTP and MSRPS. SRTP/MSRPS is used together with SIP over TLS. Packets from UEs in the untrusted zone are encrypted during transmission so as to avoid eavesdropping.

3.3 Flexible Resource Allocation

The development of multimedia services diversifies traffic models. For example, a great quantity of high-definition audio and video data will be involved in VoLTE services in the future, which requires massive media processing resources. Static Stream Control Transmission Protocol (SCTP) links between the SE2900 and core network consume a large number of signaling resources. Resource immobility has been unable to meet the requirements of dynamic user requirements and leads to a waste of resources. Flexible resource allocation improves resource usage efficiency, protecting existing investments.

By controlling the application types of SPUA0s/SPUA1s, the SE2900 supports the following traffic models:

- Default traffic model (0.08 Erl): The application types of the ISU and ESU are SEISU and SEESU respectively. This traffic model applies to SIP over UDP.

- Traffic model 1 (0.05 Erl): The application types of the ISU and ESU are SEISU1 and SEESU1 respectively. This traffic model applies to SIP over UDP/TLS/SCTP. (TLS: Transport Layer Security; SCTP: Stream Control Transmission Protocol)

If the process types in the two traffic models do not change, the SE2900 allocates different CPUs to processes. Compared with the default traffic model, the CPUs of BSU processes are enhanced and the number of BSU processes increases in traffic model 1. Figure 3-4 and Figure 3-5 show the application types of SPUA1s/SPUA0s and BSU process layout.

Figure 3-4 Application types of SPUA1s and BSU process layout

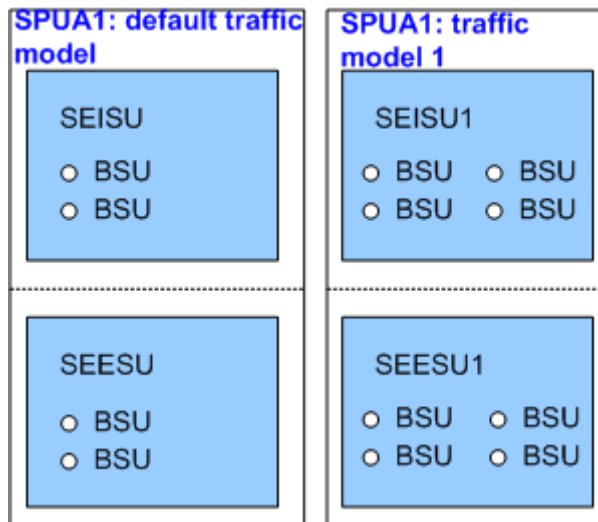
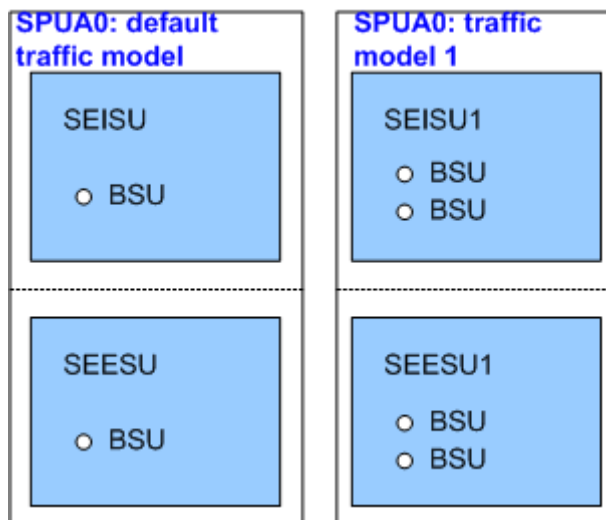


Figure 3-5 Application types of SPUA0s and BSU process layout



The SE2900's flexible resource allocation has the following advantages:

- Supports flexible resource allocation based on the traffic model.
- Supports online flexible CPU optimization without interrupting services on the live network.

- Greatly improves static link performance. The static TCP/TLS/SCTP link's CAPS performance reaches 70% of the UDP link's CAPS performance.

3.4 Efficient Platform

Advanced Hardware Platform

The SE2900 subrack (3U high) uses the OSTA5.0 hardware platform and can be installed in the standard cabinet with the depth of 800 mm. The hardware platform complies with Network Equipment Building System (NEBS) and European Telecommunications Standards Institute (ETSI) standards. Figure 3-6 shows the SE2900 hardware platform. Table 3-1 describes the hardware platform highlights.

Figure 3-6 Advanced hardware platform

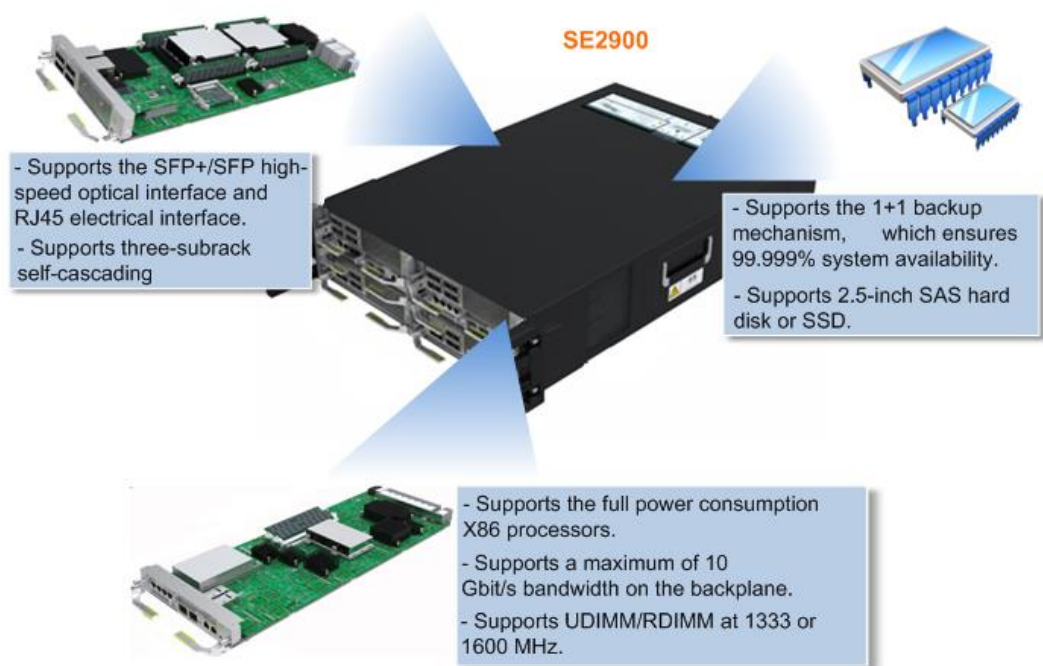


Table 3-1 Hardware platform highlights

Highlight	Description
High computing performance	Boards have the following high computing performance: <ul style="list-style-type: none"> • Supports Intel carrier-class full power consumption X86 4-core/8-core/10-core (or higher) processors. • Supports unbuffered dual in-line memory module (UDIMM) or registered dual in-line memory module (RDIMM) at 1333 or 1600 MHz. • Supports 2.5-inch serial attached SCSI (SAS) hard disk or solid-state drive (SSD) with high input output (IO) performance

Highlight	Description
	and reliability.
High switching capacity	Boards have the following high switching capacity: <ul style="list-style-type: none"> • Uses high-speed serial data links and switching structure with a maximum of 10 Gbit/s bandwidth (25 Gbit/s in later versions) on the backplane. • Uses high-performance Ethernet on management and service planes that meets the bandwidth requirements for management, control, and media.
Remarkable interface capability	Provides an independent outbound interface on each board and supports small form-factor pluggable (SFP) and enhanced SFP (SFP+) high-speed optical interfaces and RJ45 electrical interfaces.
High availability	Provides service boards, main control and switching boards, and electromechanical modules working in 1+1 backup mode, which ensures 99.999% system availability.
High scalability	Supports three-subrack self-cascading that meets the requirements for smooth capacity expansion.
Good reusability and compatibility	Allows service boards, fans, and power entry modules (PEMs) to be reused in serialized subracks.

Advanced Software Platform

The SE2900 uses the standard Distributed Object-oriented Programmable Real-time Architecture (DOPRA) platform developed by Huawei. Figure 3-7 shows the DOPRA platform. Table 3-2 describes the highlights of the DOPRA platform.

Figure 3-7 DOPRA platform

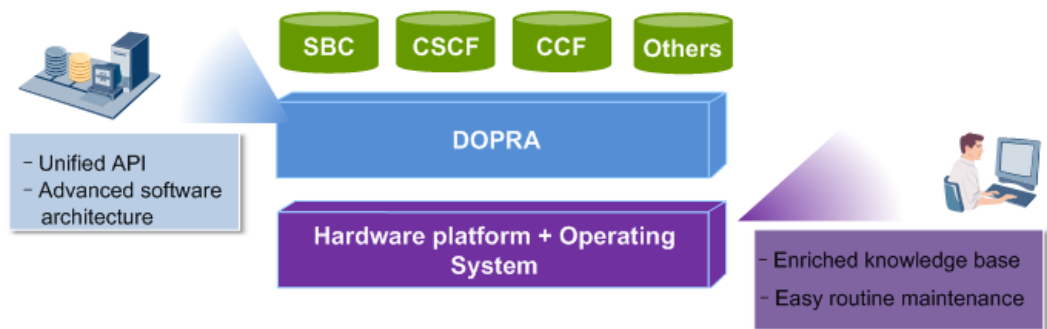


Table 3-2 DOPRA platform highlights

Highlight	Description
Wide application on commercial	DOPRA is widely used in various Huawei products on commercial networks.

Highlight	Description
networks	
Universal software application interfaces	<p>Provides a universal hardware platform interface:</p> <ul style="list-style-type: none"> • Allows upper-layer applications to run on different hardware platforms. With the universal hardware platform interface, hardware equipment management is independent of the hardware platform. • Hides the differences between operating system interfaces at the lower layer, provides a universal Virtual Operating System Application Programming Interface (VOS API) for upper-layer applications, and supports various operating systems, including Windows and UNIX/Linux.
Advanced software architecture	<p>Uses the modular architecture and provides a powerful dispatch mechanism and load-balancing mechanism.</p>
Convenient operation and maintenance	<p>Provides various mechanisms for upper-layer applications that implement various functions, including maintenance, alarm management, performance measurement, call/signaling trace, data backup, board switchover, and online loading.</p>

Flexible Networking Capabilities

The SE2900 can act as an A-BCF, IBCF, and BGF. Different function entities on one SE2900 can act as different managed elements (MEs), which can be used in different solutions, such as VoBB RCS and VoLTE, to implement access-side signaling/media processing and security defense. The SE2900 provides flexible networking capabilities at different layers. Figure 3-8 shows the SE2900 networking capabilities. Table 3-3 describes networking characteristics.

Figure 3-8 Flexible networking capabilities

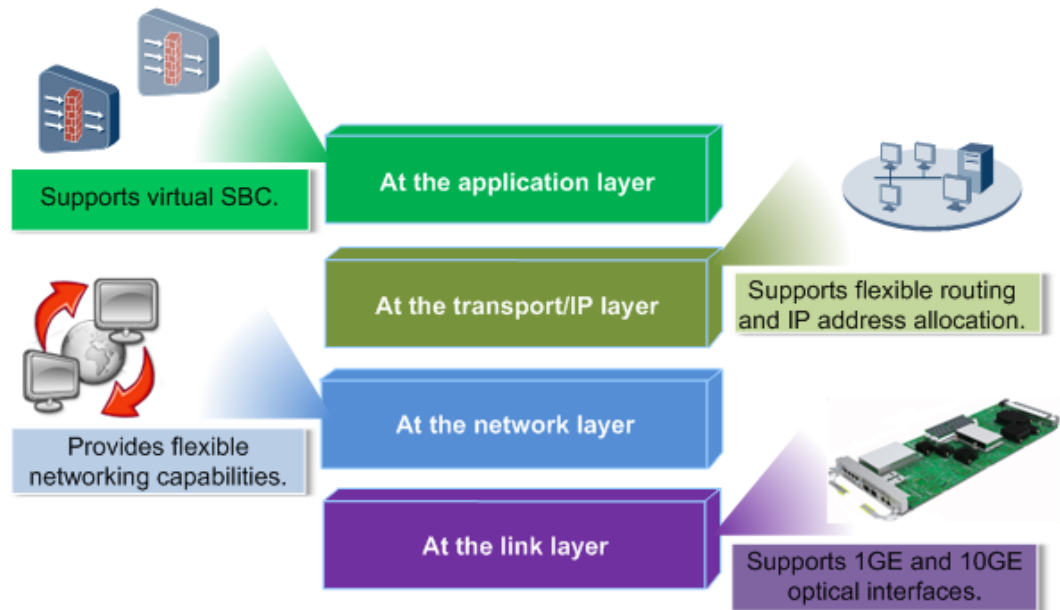


Table 3-3 Networking highlights

Layer	Highlight
Link layer	<ul style="list-style-type: none"> • Supports 1GE and 10GE optical interfaces. • Supports Eth-trunk that bundles multiple physical interfaces to a logical interface. An Eth-trunk interface has three operating modes: <ul style="list-style-type: none"> – Active/standby mode: On an Eth-trunk interface, only one member link is in the Up state, and this link is called the active link. All the other links are standby links. When the active link is Down, traffic on this link is automatically switched to other links. – Load-balancing mode: On an Eth-trunk interface, each member link is in the Up state, and traffic is load balanced among these links. – Static Link Aggregation Control Protocol (LACP) mode: On an Eth-trunk interface, M member links are primary links and N member links are backup links. When the primary links go Down, traffic on the links is switched to a backup link that has the highest priority among the N backup links.
Network layer	Supports remote redundancy networking, dual-homing networking, and P-CSCF pool networking.
Transport layer/IP layer	Supports flexible routing and IP address allocation. <ul style="list-style-type: none"> • Supports static routes. • Provides access for all users by using only one IP address.
Application layer	Supports the virtual SBC function. <ul style="list-style-type: none"> • Supports virtual SBC in physical mode (VE-PM). In VE-PM mode,

Layer	Highlight
	<p>multiple virtual SBCs operate on different boards to implement hardware resource separation. A license is required for each virtual SBC.</p> <ul style="list-style-type: none"> Supports virtual SBC in logical mode (VE-LM). In VE-LM mode, multiple virtual SBCs operate on the same board. Each virtual SBC provides independent signaling resources and media resources, implementing software resource separation. <p>NOTE A virtual SBC is a logical device. After purchasing the SE2900, you can partition one physical SBC into multiple logically independent SBCs to achieve enhanced flexibility in network deployment.</p>

3.5 Efficient Operation and Maintenance

Unified Operation and Maintenance Platform

The SE2900 uses the Huawei proprietary operation and maintenance unit (OMU), as shown in Figure 3-9. The OMU supports unified, efficient, and visible operation and maintenance.

Figure 3-9 Unified operation and maintenance platform

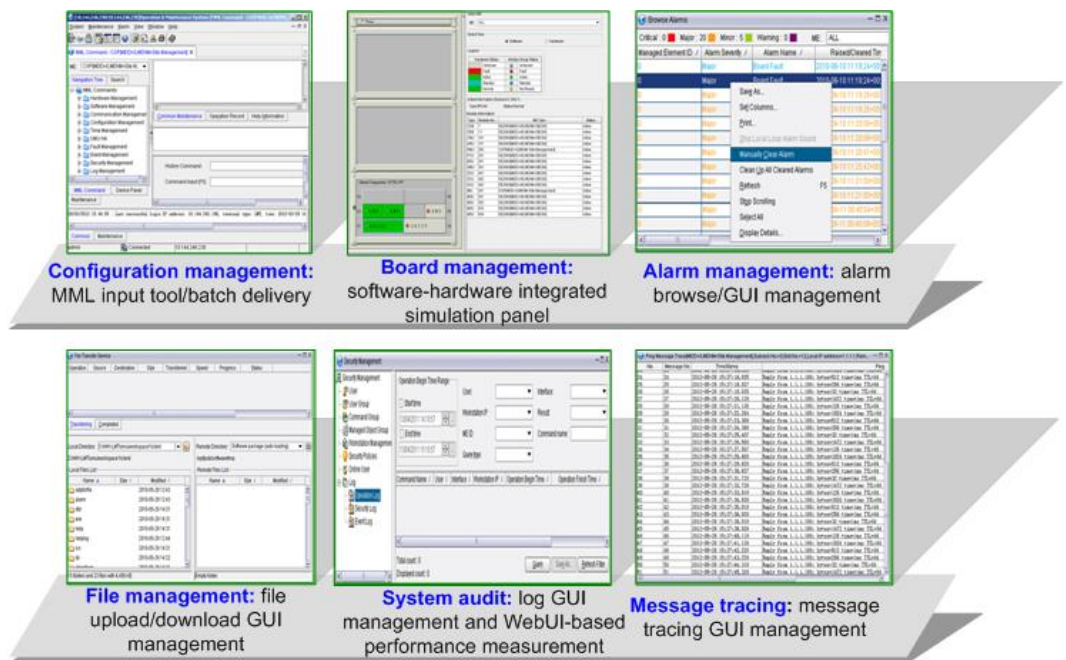


Table 3-4 Unified operation and maintenance platform

Function	Highlight

Function	Highlight
Configuration management	Provides an operation interface based on the man-machine language (MML) and graphic user interface (GUI) for local and remote maintenance.
Board management	Displays the active/standby status and operating status and board reset/switchover operation on the client.
Alarm management	Supports real-time alarm reporting when a fault occurs and marks alarm severities using different colors in the alarm browse window. This function helps facilitate immediate fault identification and rectification.
File management	Supports easy and visualized file upload/download to boards on the client.
System audit	Supports log query, alarm query, and web user interface-based (WebUI-based) performance measurement and fault diagnosis. This function facilitates fault identification and rectification, and provides a reference for network maintenance and optimization.
Message tracing	Supports the signaling tracing function. Signaling can be traced based on the IP address, port number, or signaling link. Carriers can use the signaling tracing function to trace detailed signaling messages exchanged in procedures, such as registration, call establishment and release, and subscription and notification, of a specific call. The SE2900 supports end-to-end signaling tracing tasks and displays signaling tracing results on the EMS, which improves the fault location efficiency.

GUI-based WebUI Interface

The SE2900 supports the GUI-based web user interface (WebUI), as shown in Figure 3-10. The WebUI integrates performance management and patch and upgrade tools.

Figure 3-10 GUI-based WebUI



The WebUI enables web-based GUI operations in routine maintenance. You can use the GUI for performance management (for example, creating a traffic measurement task), patch installation, and version upgrade. GUI-based maintenance improves operability, facilitates operation and maintenance, and reduces the risks of misoperation.

Small Tools for Fault Location

In addition to operation and maintenance tools, the OMU provides some small tools that are delivered along with the software package. These small tools facilitate data configuration and fault location in routine maintenance.

Figure 3-11 Small tools helping fault location



In routine operation and maintenance, rapid fault location and rectification are expected. The OMU provides some small tools shown in Figure 3-11, which facilitate rapid fault location and rectification by collecting and displaying log information or traced messages.

Smooth Expansion

The SE2900 supports smooth expansion and self-cascading, which has a minimum impact on system operation.

- Self-cascading

Up to three SE2900 subracks can be cascaded without any switch. The deployment mode is flexible, and uses a centralized management approach that allows easy maintenance.

- Smooth expansion

When the number of users at a site exceeds the system capacity, the capacity can be expanded by adding subracks, boards, IP addresses, or links. Services are not interrupted during the capacity expansion, allowing services to load-balanced smoothly. Smooth expansion saves operational expenditure (OPEX), shortens the time to market (TTM), and improves user satisfaction. The access network is unaware of capacity expansion.

3.6 High Reliability

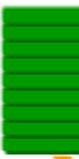

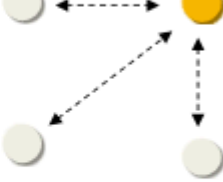
The SE2900 is designed with high hardware and software reliability that ensures 99.999% network availability.

- System reliability

- Software and hardware reliability

Table 3-5 describes the hardware and software reliability design of the SE2900.

Table 3-5 SE2900 hardware and software reliability design

Item	Measure
Hardware design	<p>The SE2900 uses SPUs and VPUs. SPUs operate in 1+1 backup mode. VPUs operate in load-balancing mode. The SE2900 optimizes fault detection at both the board and system levels and uses isolation technologies to improve the overall system maintainability.</p> <p>Figure 3-12 Hardware reliability</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="612 1256 995 1727" style="border: 1px solid gray; padding: 10px; width: 45%;"> <p style="text-align: center; background-color: #0070C0; color: white; padding: 5px;">1+1 backup</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Active</p>  </div> <div style="text-align: center;"> <p>Standby</p>  </div> </div> <p style="text-align: center; margin-top: 10px;">↔</p> <ul style="list-style-type: none"> 100% hardware redundancy <10 minutes for system restart </div> <div data-bbox="1027 1256 1410 1727" style="border: 1px solid gray; padding: 10px; width: 45%;"> <p style="text-align: center; background-color: #70AD47; color: white; padding: 5px;">N+1 backup</p>  <p style="text-align: center; margin-top: 10px;">The fans in the subrack operate in N+1 backup mode.</p> </div> </div> <ul style="list-style-type: none"> The SE2900 uses a dual power supply system, which protects the system against lightning, power outage, over-current or under-current, and over-voltage or under-voltage. The entire system can restart up within 10 minutes if a power failure occurs. The SE2900 uses centralized heat dissipation. Fans in the subrack

Item	Measure
	<p>operate in N+1 backup mode. The loss of a fan does not adversely affect the heat dissipation of the system.</p> <ul style="list-style-type: none"> Key components of the SE2900 are connected in dual-bus mode. The SE2900 uses the dual-plane and interconnection architecture for internal communication. The failure of a single node does not affect the entire system.
Software design	<ul style="list-style-type: none"> The SE2900 uses modular architecture in software design, and different functions are implemented by different modules. The software is designed with fault monitoring, fault tolerance, and protection capability. The modules on the SE2900 operate in load-balancing mode or active/standby mode to ensure high system reliability.

– Enhanced flow control

The SE2900 implements flow control using service packet type parsing, weighted queue scheduling, UDP retransmission filtering, and quick response. As long as the CPU usage remains stable, high-priority packets are given preferential treatment, and flow control is also implemented to ensure stable service processing during peak hours.

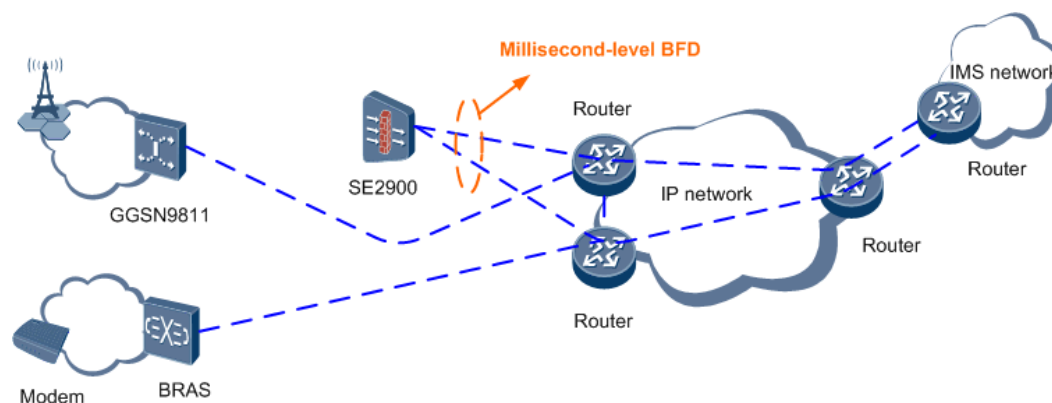
• Networking reliability

– Link detection

■ BFD

With the bidirectional forwarding detection (BFD) function, the SE2900 is able to quickly detect the status of the peer device and inform the protocol layer of the status. If a link is faulty, services can be switched to other available links within several milliseconds. See Figure 3-13.

Figure 3-13 BFD

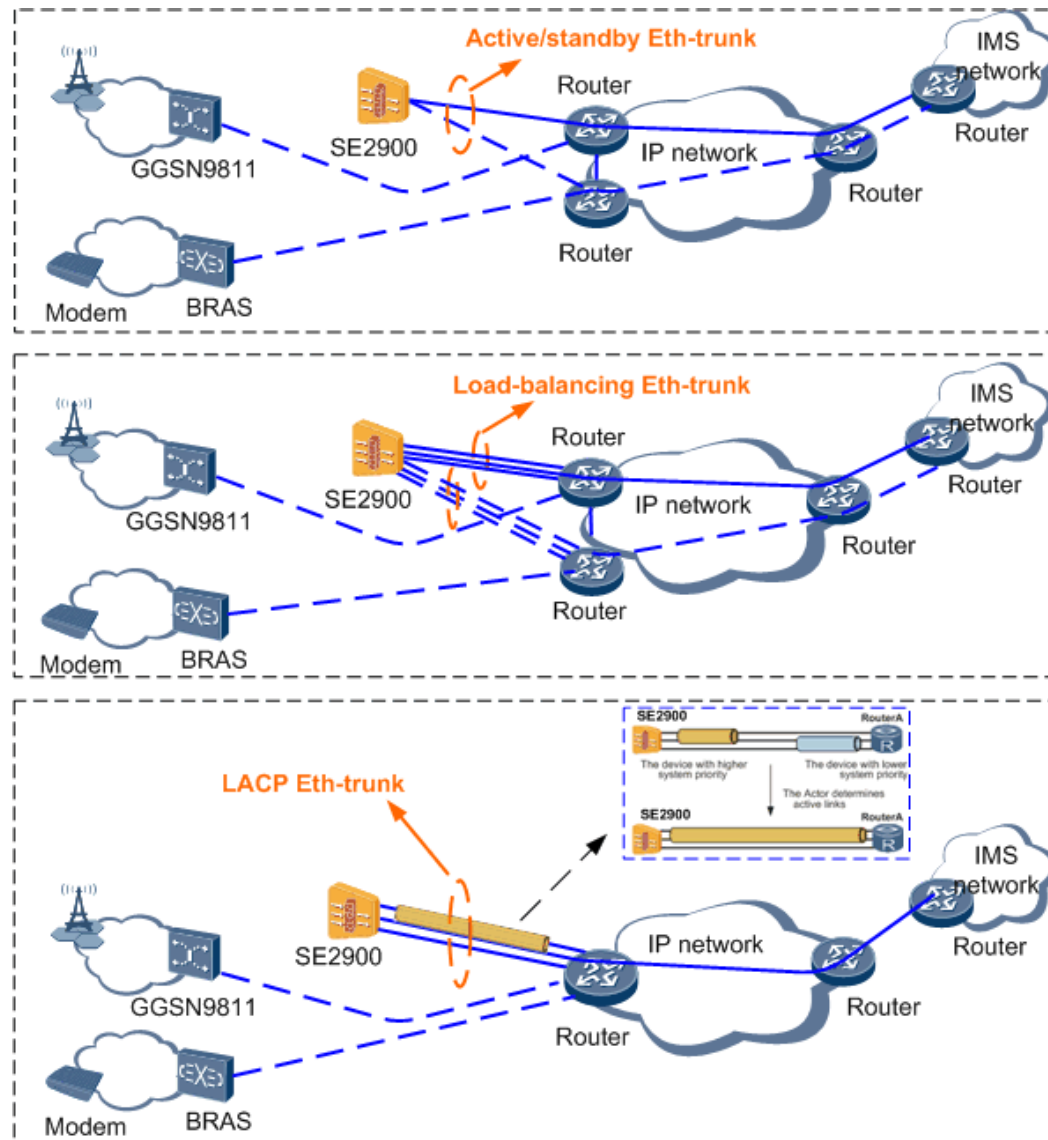


■ Eth-trunk

The SE2900 supports Eth-trunk that bundles multiple physical interfaces to a logical interface. An Eth-trunk interface can be used as one physical interface, with the bundled physical interfaces working as its member interfaces. The member interfaces operate in load-balancing mode or in active/standby mode.

If one or some of these member interfaces are faulty, services are load balanced by the other member interfaces. See Figure 3-14.

Figure 3-14 Eth-trunk



- Core network redundancy
The redundancy of core network feature enables the SE2900 to implement core network geographical redundancy. This feature ensures normal service provisioning and reduces service interruption caused by single point of failures, and improves the system reliability and network disaster tolerance capability. The SE2900 supports two networking schemes for core network redundancy: dual-homing and P-CSCF pool. See Figure 3-15 and Figure 3-16.

Figure 3-15 Core network redundancy networking schemes(With P-CSCF Not Embedded)

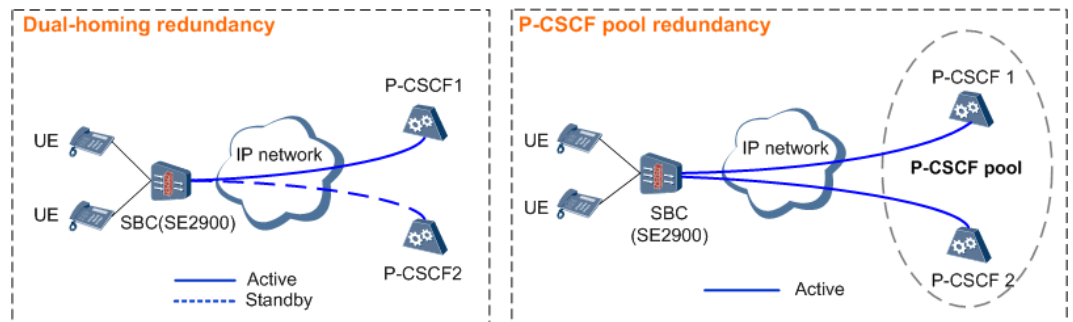
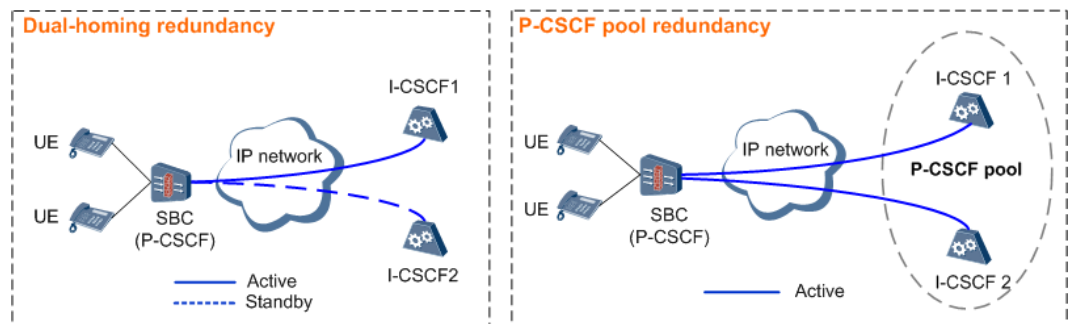


Figure 3-16 Core network redundancy networking schemes(With P-CSCF Embedded)



- In the dual-homing networking scheme, one SE2900 is homed to two P-CSCFs (with P-CSCF not embedded) or I-CSCFs (with P-CSCF Embedded). One P-CSCF or I-CSCF functions as the master device, and the other as the slave device. If the master P-CSCF is faulty, services are automatically switched to the slave P-CSCF to ensure service continuity.
- In the P-CSCF pool networking scheme, one SE2900 is homed to a P-CSCF or I-CSCF pool comprising multiple P-CSCFs or I-CSCFs that work in load-balancing mode. If one P-CSCF or I-CSCF is faulty, services are automatically switched to another P-CSCF or I-CSCF in the P-CSCF or I-CSCF pool to ensure service continuity.

– Dual-system hot backup

The SE2900 is deployed between the access network and core network, or between two different core networks. In the presence of a single SE2900, if it is faulty, the services on the entire network will be interrupted. To resolve this issue, two SE2900s, one acting as the master and the other as the backup, can be deployed in the same equipment room or different equipment rooms to ensure service reliability and provide a geographic redundancy (GR) solution for carriers. Figure 3-17 shows remote dual-system hot backup networking (GR groups in different equipment rooms); Figure 3-18 shows local dual-system hot backup networking (GR groups in the same equipment room).

Figure 3-17 Remote dual-system hot backup networking

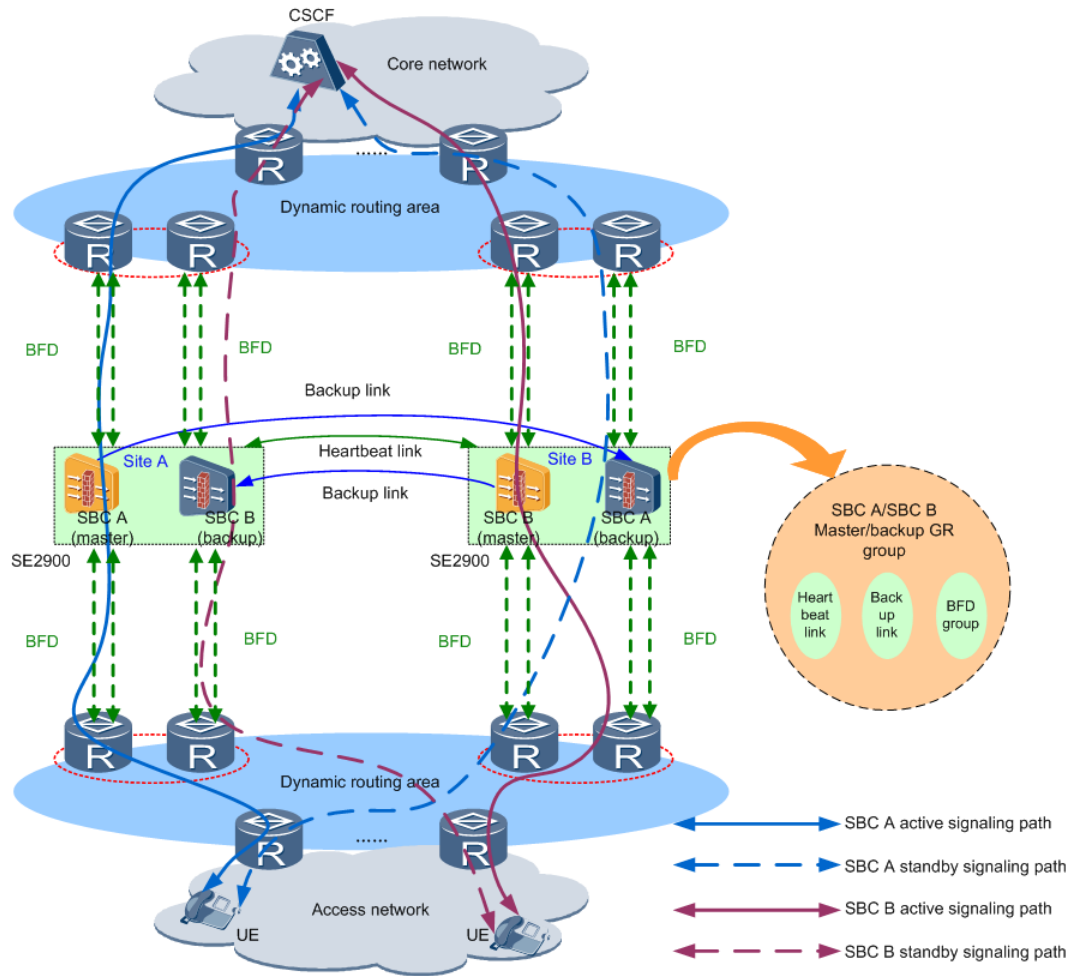
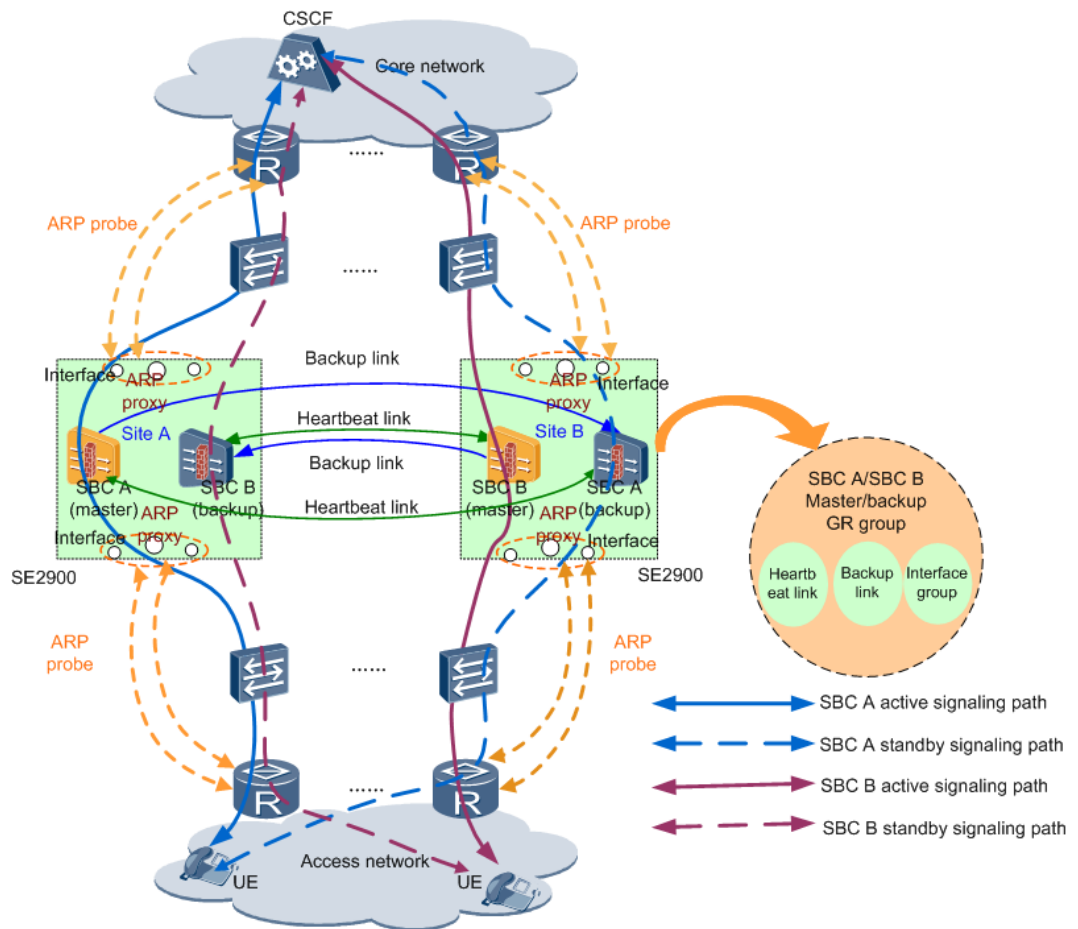


Figure 3-18 Local dual-system hot backup networking



Dual-system hot backup is implemented by configuring GR between MEs. GR groups, which are the smallest units in dual-system hot backup, operate in master/backup mode to provide services. Under normal circumstances, in remote dual-system hot backup, the master SE2900 processes services, and the backup SE2900 stays in the listening state and backs up registration data from the master SE2900; in local dual-system hot backup, the master SE2900 processes services, and the backup SE2900 stays in the listening state and backs up registration and call data from the master SE2900. If the master GR group does not function properly, the backup GR group automatically takes over as the master GR group, ensuring non-stop services.

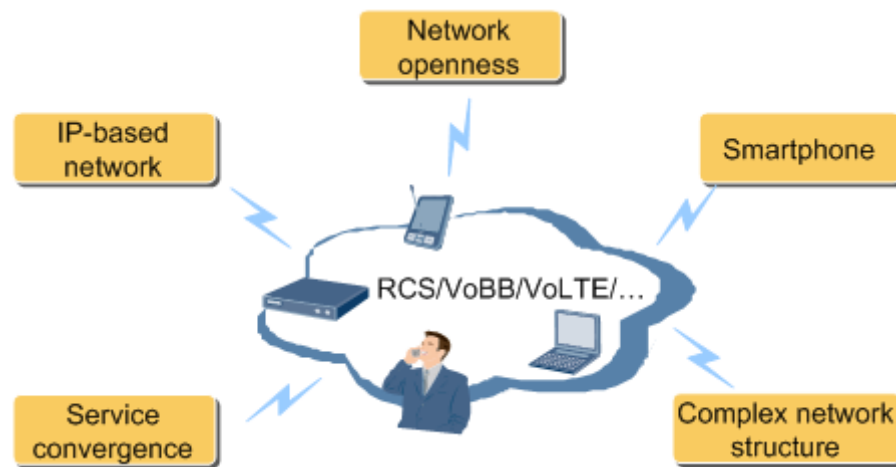
Dual-system hot backup helps improve reliability. It enables carriers to prevent service interruption due to single points of failure that are caused by such factors as the earthquake or fire, thereby providing non-stop high-quality services for users and improving user satisfaction.

3.7 Industry-leading Security Defense Capability

Powerful Security Mechanism

In the RCS, VoLTE, or VoBB solution, the core network to which the SE2900 is homed might adopt the all-IP network architecture and use SIP as its session control mechanism. Due to the open nature of IP, SIP scalability, and numerous access modes involved in the RCS, VoLTE, and VoBB solutions, the core network is vulnerable to viruses and attacks from unauthorized users or hackers. Figure 3-19 shows the factors that pose security threats to the RCS, VoLTE, or VoBB solution.

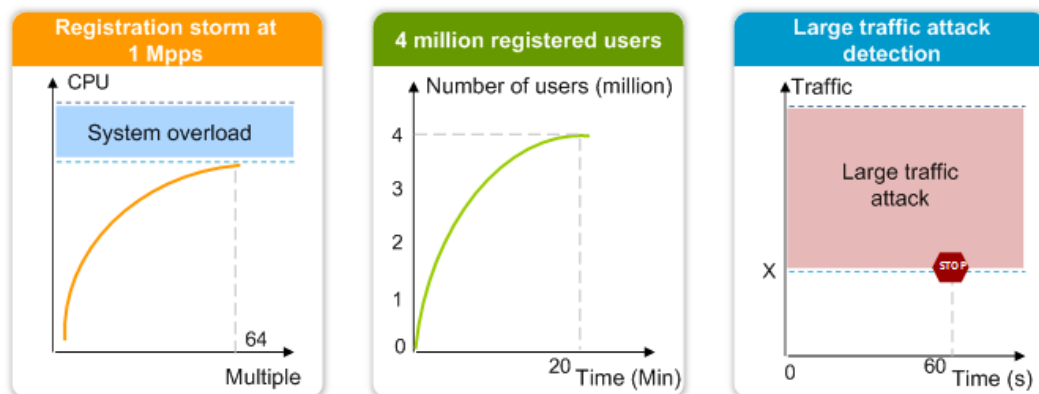
Figure 3-19 Factors that pose security threats to the RCS, VoLTE, or VoBB solution



Core servers (for example, the CSCF) are mainly responsible for signaling and media processing and do not have strong attack defense capability. An ordinary firewall can defend against the attacks composed of common IP data packets of specific types but cannot distinguish application services. Therefore, it cannot identify signaling and media attacks. To defend against the security threats, the SE2900 uses an open, transparent, and visualized architecture, which adopts effective measures to enhance network and service security, enabling carriers or enterprises to construct a hierarchical security defense mechanism for the entire network.

The SE2900 provides a powerful security architecture to guarantee the confidentiality and privacy of itself, core servers, and services. The SE2900 supports hierarchical security defense at the IP layer, signaling plane, and media plane. Figure 3-20 shows the hierarchical security defense of the SE2900.

Figure 3-20 Hierarchical security defense



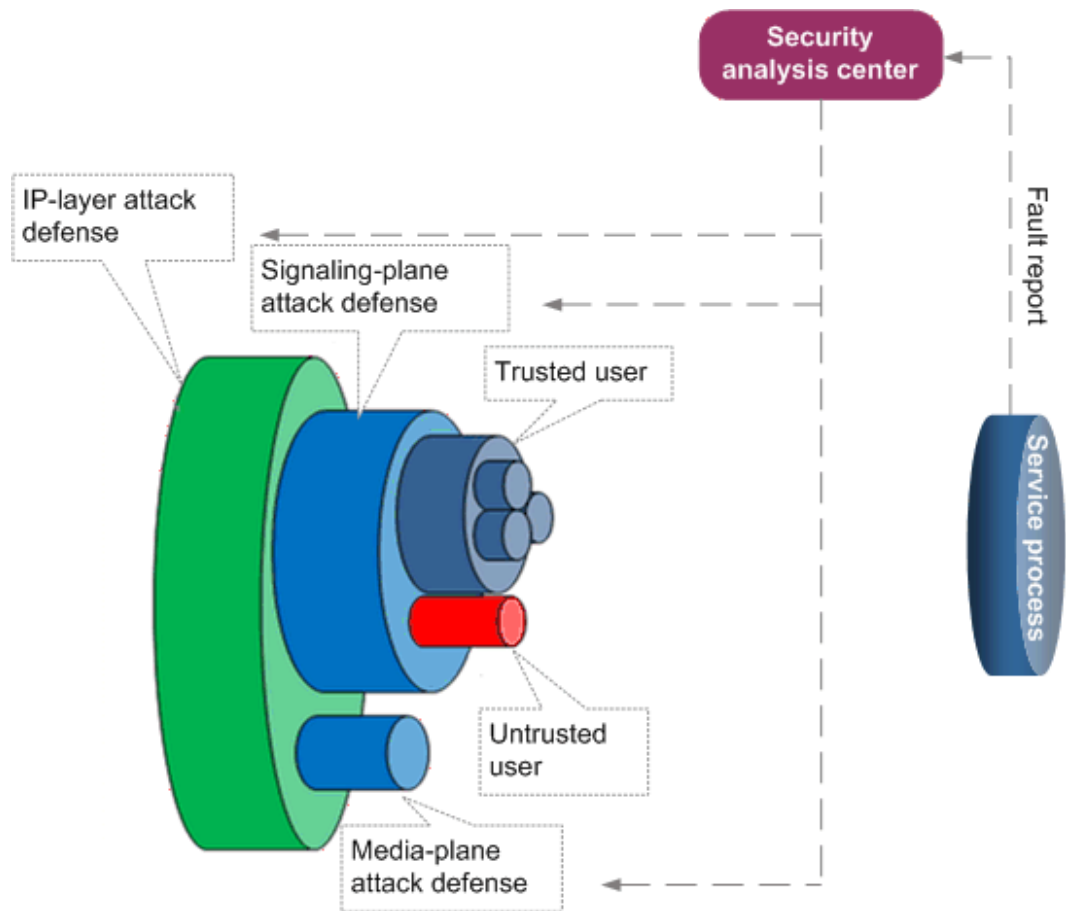
The SE2900 security highlights are as follows:

- Deep content parsing: The SE2900 supports deep content parsing using the latest local or external security policies.
- Large-traffic attack defense: The SE2900 can defend against register storms at 1 Mpps. A maximum of 4 million users can be registered with the SE2900 within 20 minutes.
- Rapid attack source identification: The SE2900 proactively identifies potential risks and takes actions. It can locate the source of a large-traffic attack within 60 seconds.

Proactive Security Defense

The SE2900 has an embedded security analysis center, which collects fault information from service processes and classifies the collected fault information by type. See Figure 3-21. The security analysis center collects fault information by IMPU, source IP address, or source IP address + port. Statistics about fault information are cleared every 5 minutes by default. If the fault information collected within a statistical period exceeds the threshold, the security analysis center blacklists the corresponding IMPU, source IP address, or source IP address + port.

Figure 3-21 Security analysis center



When a user performs an action, the security analysis center checks the action against the user's historical behaviors. Once an intrusion is detected or the user is considered to be wasting the system resources, the security analysis center immediately disconnects the user from the SE2900. Using this proactive defense procedure, the security analysis center continuously detects threats on the IP layer, signaling plane, and media plane, which ensures that the SE2900 permits packets only from trusted users and discards packets from untrusted users.

Security Service

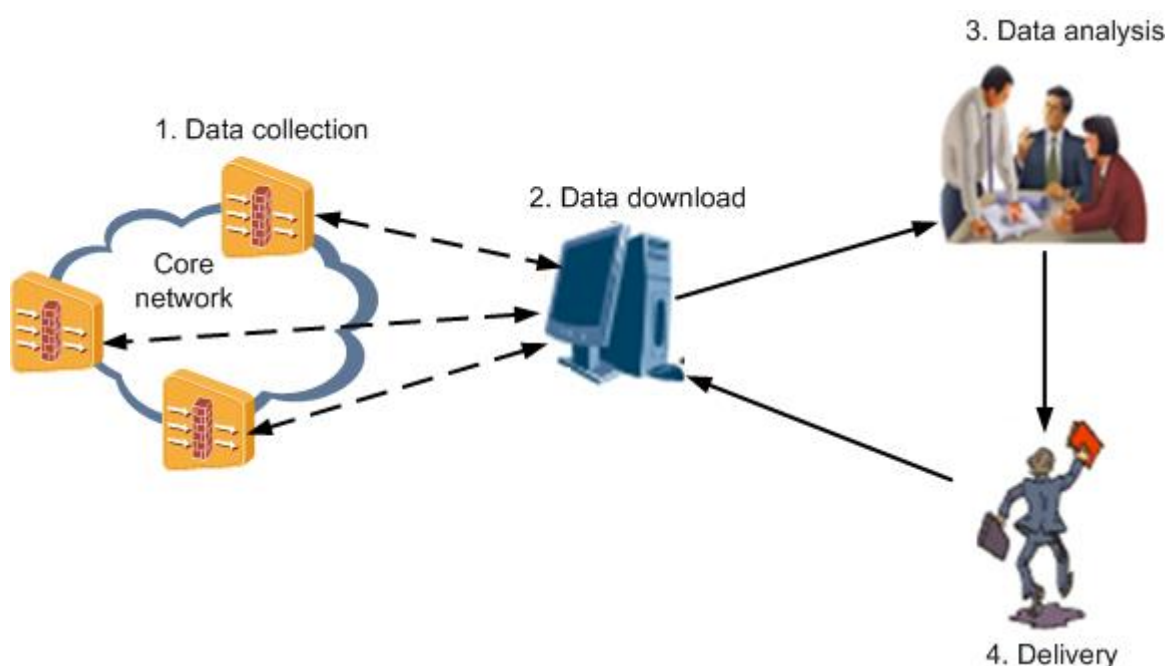
Security services refer to the services provided by Huawei technical support engineers to secure the network by optimizing attack defense parameters according to live network situations. The SE2900 periodically records users' traffic and misbehavior information. The carrier obtains the data at least once each week. Huawei technical support engineers use security service software to analyze the data within a period (from one month to half a year). Specifically, the engineers analyze the gaps between maximum transmission rates and thresholds of each user, offer optimization suggestions, and evaluate network security, helping carriers implement their security strategies and plans.

The security service is sold independently. After the purchase of the security service, Huawei technical support engineers periodically collect information from the SE2900, analyze the collected information, and provide optimization suggestions based on the analysis.

- Carriers are required to know the functions of the security service software, which helps to ensure the integrity of collected information.
- Taking the data collected using the security service software away from the carriers' networks is strictly forbidden without carriers' consent.
- The suggested optimization can be implemented on live networks only with carriers' consent.
- After security service is enabled, the performance deteriorates by 3%.

Figure 1 shows the security service procedure.

Figure 3-22 Security service procedure



1. Data collection: The SE2900 collects information about traffic peaks and anomalies of each user once a day. No communication content is involved during data collection. The procedure for collecting data is as follows:
 - Data to be analyzed on live networks
 - i. Log in to the OMU client.
 - ii. Enable the security service function.
In the **MML Command - SE2900** window, run **SET SSECPARA** with **Enable Security service** set to **Y(Yes)**.
 - Live network diagrams
Provide the network diagram files of A-SBC and I-SBC scenarios. The file name extensions must be **.png** or **.jpg**. Network diagram names, for example, **asbc.png**, must be easy to recognize.
2. Data download: The carrier downloads the collected data from the SE2900 once a day. The procedure for downloading the data is as follows:



NOTICE

The security service tool helps the SE2900 analyze the data collected within 90 days. After the security service function is enabled, the SE2900 collects and saves data at an interval of 7 days. If it takes more than seven days to analyze collected data, you must save the data in the same period to the same directory of drive D on which the security service tool is installed. No requirements are imposed on the directory name.

- a. Log in to the OMU client and choose **Maintenance > File Transfer Service**. Select **ME file** from the **Remote Directory** drop-down list box.
- b. In the **Remote Files List** area, select **ME files**. On the SE2900 on which the security service function is enabled, double-click the directory named **neXX_service** (**XX** specifies the ME ID) in **/opt/HUAWEI/cgp/workshop/omu/share/nefile**.
- c. Copy the files in the **neXX_service** directory to drive D.



NOTE

The files in **neXX_service** are the live network data to be analyzed.

- d. Run the following commands in the **MML Command - SE2900** window to save the command output to a specified file and the live network data directory in 2.c:
 - Run **LST IDXNAME** with **Index type** set to **IDX_SIPAN_INDEXID(SIP Access Net Record of ABCF: SIPAN Index)** to save the SIP AN ID and name in a new file.



NOTE

The new file must be named **SIPAN-INDEX.csv**. The file includes a table of two columns with table headings **ID** and **Name** respectively. Fill in the SIP AN ID in the **ID** column and SIP AN name in the **Name** column.

- Run **LST IDXNAME** with **Index type** set to **IDX_ISIPTG_INDEXID(SIP Trunk Group Table of IBCF: Tg Index)** to save the SIP trunk group ID and name in a new file.



NOTE

The new file must be named **SIPTG-INDEX.csv**. The file includes a table of two columns with table headings **ID** and **Name** respectively. Fill in the SIP trunk group ID in the **ID** column and SIP trunk group name in the **Name** column.

3. Data analysis: Huawei security service engineers periodically use the security service software to analyze the collected data on premise. Based on the analysis, a service model is constructed, and optimizations for security defense settings are formed. During this phase, a security service report is to be delivered after data analysis.
4. Delivery: Implements the optimization on the live network with the carrier's consent.

Table 1 lists the KPIs within the service scope.

Table 3-6 KPIs in the security service scope

KPI	Description
Threshold for the average rate of packets from trusted users (A-SBC)	Threshold for the average rate of packets from each trusted user (A-SBC)
Average rate threshold of packets sent from a non-trusted user with every source IP	Threshold for the average rate of packets from an untrusted user specified by the

KPI	Description
address (A-SBC)	source IP address
Threshold for the number of connections originated from each IP address (A-SBC)	Threshold for the number of connections originating from each IP address (A-SBC)
Threshold for the number of abnormal ports at each IP address (A-SBC)	Threshold for the number of abnormal ports associated with each source IP address (A-SBC)
Threshold for the number of registration failures per user (A-SBC)	Threshold for the number of registration failures per user in an intrusion prevention system (IPS) period (A-SBC)
Threshold for the number of incomplete emergency calls originating from each unregistered user (A-SBC)	Threshold for the number of incomplete emergency calls originating from each unregistered user in an IPS period (A-SBC)
Threshold for the number of incomplete calls per user	Threshold for the number of incomplete calls per user in an IPS period (Incomplete calls refer to calls that are proactively released by the callers before being established.)
Threshold for the number of malformed packet attacks per user	Threshold for the number of malformed packets per user in an IPS period
Threshold for the number of invalid requests per user	Threshold for the number of invalid requests per user in an IPS period (Invalid requests refer to requests that cannot match any session, transaction response, or registered user.)
Threshold for the number of ultra-short calls per user	Threshold for the number of ultra-short calls per user in an IPS period
Threshold for the packet transmission rate per SIP trunk group (I-SBC)	Threshold for the packet transmission rate per SIP trunk group (I-SBC)
Threshold for UDP flood attacks	Threshold for the non-signaling and non-media UDP packet transmission rate
Threshold for TCP flood attacks	Threshold for the non-media TCP SYN packet transmission rate

Offline Fraud Prevention

Offline fraud prevention enables the SE2900 to send CDRs to the CCF so that the fraud prevention platform can obtain the CDRs for fraud analysis and generate alarms when any fraud behavior is detected. After being informed of any such alarms, carrier's maintenance engineers can manually block the service of alarmed users to prevent fraud behavior and reduce the losses caused by such behavior. This function is supported no matter whether the CCF is built inside the SE2900 or deployed independently.

4 Services and Functions

About This Chapter

- 4.1 Feature Matrix
- 4.2 A-SBC Basic SW
- 4.3 I-SBC Basic SW
- 4.4 Optional Features

4.1 Feature Matrix

The SE2900 product package includes basic features and optional features:

- Basic feature: No license is required for a basic feature. See Table 4-1.
- Optional feature: A license is required for an optional feature. See Table 4-3.

Table 4-1 Basic features

Feature ID	Feature Name	Overview		Remarks
SE9S00ABSW01	A-SBC Basic SW	SIP Registration	SIP registration is a procedure in which SIP UEs initiate requests to the subscription network for service authorization. Registered SIP UEs can use the services provided by the home network. In the A-SBC scenario, the SE2900, which is deployed at the edge of the IMS network, forwards REGISTER requests from SIP UEs to the IMS network or forwards responses from the IMS network to SIP UEs.	This feature applies to both the IMS network and NGN.
		SIP Call	The SIP call feature enables the SE2900 to create, modify, or terminate multi-media sessions involving one or more participants and uses SDP to dynamically modify session attributes, such as required session bandwidths, media types (audio,	This feature applies to both the IMS

Feature ID	Feature Name	Overview		Remarks
			<p>video, or data), and media codec types.</p> <p>In the A-SBC scenario, the SE2900, which is deployed at the edge of the IMS network, forwards call messages from SIP UEs to the IMS network or from the IMS network to SIP UEs. For details, see 4.2.1 SIP Call.</p>	network and NGN.
		SIP Emergency Call	<p>The SIP emergency call feature enables the IMS network to identify and give special treatment to emergency calls. When a subscriber dials an emergency call number (such as 911) or an SOS uniform resource name (URN), the IMS network identifies this call as an emergency call and forwards the call request to the nearest emergency center (EC) for special treatment.</p> <p>In the A-SBC scenario, the SE2900, which is deployed at the edge of the IMS network, identifies a call as an emergency call and then forwards the call to a device on the IMS network for subsequent processing.</p>	This feature applies to both the IMS network and NGN.
		SIP Subscription	<p>The SIP subscription feature enables subscribers to subscribe to resource status from the system. When resource status changes, the system sends NOTIFY messages to subscribers.</p> <p>In the A-SBC scenario, the SE2900 is deployed at the edge of the IMS network, forwards SUBSCRIBE requests from SIP UEs to the IMS network, or forwards NOTIFY messages from the IMS network to SIP UEs.</p>	This feature applies to both the IMS network and NGN.
		SIP Fax	<p>SIP fax is a telecommunications service in which data is transmitted between two fax machines. It provides complete service functions, including fax data bearer and fax service management, from the fax machine on the one side of the network to the fax machine on the other side of the network.</p> <p>In the A-SBC scenario, the SE2900, which is deployed at the edge of the IMS network, forwards fax data from SIP UEs to the IMS network or from the IMS network to SIP UEs.</p>	This feature applies to both the IMS network and NGN.
		Media Policy	<p>The media policy feature enables the SE2900 to flexibly control media capabilities, such as early media, media types, media codecs, and bandwidth, ensuring proper communication between the caller and callee based on the same media type and codec. For details, see 4.2.2 Media Policy.</p>	This feature applies to both the IMS network and NGN.

Feature ID	Feature Name	Overview		Remarks
		MSRP Proxy	Rich Communication Suite (RCS) defines Message Session Relay Protocol (MSRP)-based picture sharing, file transmission, and chat services. The SE2900 serves as an MSRP proxy and forwards MSRP media streams between a UE and an AS or between UEs. For details, see 4.2.3 MSRP Proxy.	This feature applies only to the IMS network.
		DNS Function	The SE2900 supports DNS-query-based routing for SIP registration or calls based on the configuration of the connection between the SE2900 and an external DNS server or the configuration of the embedded DNS server. For details, see 4.2.4 DNS Query.	This feature applies to both the IMS network and NGN.
		Virtual SBC	One physical SE2900 can be divided into several virtual SBCs. Each virtual SBC provides a separate access address (and port) for a user and distinguishes user groups based on the source IP address (address segment) or the IP address (and port) accessible to the SBC. For details, see 4.2.5 Virtual SBC.	This feature applies to both the IMS network and NGN.
		SIP Keep-Alive and NAT Traversal	By re-specifying the receive address + port for signaling or RTP streams of intranet or extranet users, the SE2900 implements NAT traversal and address translation (including public or private network address translation) between different network domains. If a NAT device is deployed between a UE and the SE2900, the SE2900 supports NAT traversal by sending Simple Traversal of UDP through NAT (STUN), CLRF, or Hello packets. For details, see 4.2.6 SIP Keepalive and NAT Traversal.	This feature applies to both the IMS network and NGN.
		No Media Stream Detection	The SE2900 sends a BYE message to the UE and the core server after detecting that no media stream is available in one direction or both directions of a session for a period which is longer than the maximum allowable period. The core server tears down the session upon receiving the BYE message. The SE2900 then releases relevant media session entries and resources.	This feature applies to both the IMS network and NGN.
		Address Overlapping	The SE2900 isolates Ethernet interfaces or sub-interfaces to different virtual routing and forwarding (VRF) instances to identify users with overlapping addresses. The IP addresses in different VRF instances can be the same. The SE2900 allows overlapping access network addresses, overlapping core network addresses, and	This feature applies to both the IMS network and

Feature ID	Feature Name	Overview		Remarks
			overlapping access and core network addresses. For details, see 4.2.7 Address Overlapping.	NGN.
		Flow Control	The SE2900 supports flow control by means of service packet type parsing, weighted queue scheduling, UDP retransmission filtering, and quick response. High-priority packets are processed promptly when the CPU usage is stable to ensure satisfactory service processing during peak hours.	This feature applies to both the IMS network and NGN.
		Topology Hiding	The SE2900 can be deployed as a proxy between a UE and the core network to provide security guarantee for real-time sessions. The UE on the private network can access the core network through the SE2900, but the topology of the core network is not exposed to the UE. The UE can also access the private network through the SE2900. With the topology hiding feature, the topologies of core and private networks are both hidden, protecting the core and private networks from attacks and enhancing network architecture security.	This feature applies to both the IMS network and NGN.
		IP Layer Security	Packet filtering based on the ACL and IP denial of service (DoS)/distributed denial of service (DDoS) attack defense are two major means for ensuring IP layer security. In VoIP services, all signaling and media messages are carried in IP packets. Therefore, the core network must defend itself against various attacks from the IP layer. The SE2900 can function as a firewall to identify, classify, and handle attacks from the IP layer, thereby defending the core network against IP layer attacks.	This feature applies to both the IMS network and NGN.
		Signaling Plane Security	Signaling DoS/DDoS attack defense is a major means for ensuring signaling plane security. Common firewalls can only prevent common IP data packet attacks, and are unable to distinguish between application services. This means that common firewalls cannot protect core servers from signaling attacks. The SE2900 uses the back-to-back user agent (B2BUA) mechanism to maintain the status of each user who is using services and to check the status of each message, thereby defending the core network against various signaling attacks.	This feature applies to both the IMS network and NGN.
		Media Plane Security	Media pinholing firewall is a major means for ensuring media plane security. The SE2900 dynamically creates media session entries (IP 5-tuple) based on signaling negotiation results. The	This feature applies to both

Feature ID	Feature Name	Overview		Remarks
		ty	IP 5-tuple consists of the source IP address + port, destination IP address + port, and protocol type. All media streams pass through the SE2900. The SE2900 forwards matched media packets and discards unmatched media packets, implementing media attack defense.	the IMS network and NGN.
		SIP over TCP	SIP over TCP applies to the IMS network in the A-SBC scenario. SIP messages are transmitted over TCP between a UE and the SE2900 to enhance the reliability of SIP message transmission. For details, see 4.2.12 SIP over TCP.	This feature applies to both the IMS network and NGN.
		DSCP Remark	The SE2900 assigns different DSCP values to signaling and media packets. After receiving data packets, a router preferentially forwards packets with higher DSCP priorities to ensure QoS on the VoIP network. For details, see 4.2.13 DSCP Remarking.	This feature applies to both the IMS network and NGN.
		H.248 Proxy	H.248 proxy enables the SE2900 to allow H.248 users to access IMS networks/NGNs by means of signaling and media proxy. With this function, the SE2900 can ensure IMS network/NGN security and achieve media. The SE2900 is deployed at the edge of an IP network or deployed at the convergence layer and acts as a convergence point for signaling and media streams. For details, see 4.2.14 H.248 Proxy.	This feature applies to both the IMS network and NGN.
		Offline Fraud Prevention	Offline fraud prevention enables the SE2900 to send CDRs to the CCF so that the fraud prevention platform can obtain the CDRs for fraud analysis and generate alarms when any fraud behavior is detected. After being informed of any such alarms, carrier's maintenance engineers can manually block the service of alarmed users to prevent fraud behavior and reduce the losses caused by such behavior. This function is supported no matter whether the CCF is built inside the SE2900 or deployed independently. For details, see 3.7 Industry-leading Security Defense Capability.	This feature applies to both the IMS network and NGN.
		Security Service	Security service refers to the optimization of security defense settings by Huawei technical support engineers based on the actual situations on live networks. Specifically, Huawei technical support engineers periodically use the security	This feature applies to both the IMS

Feature ID	Feature Name	Overview		Remarks
			service software to download the statistics about the traffic and anomalous behaviors of each user from the SE2900, analyze the gaps between the thresholds and actual situations for three to six months, evaluate network security, and provide suggestions on the optimization of security defense settings. The security service is sold independently. For details, see 3.7 Industry-leading Security Defense Capability.	network and NGN.

Table 4-2 Basic features

Feature ID	Feature Name	Overview		Remarks
SE9S00IBSW01	I-SBC Basic SW	SIP Subscription	<p>The SIP subscription feature enables subscribers to subscribe to resource status from the system. When resource status changes, the system sends NOTIFY messages to subscribers.</p> <p>In the I-SBC scenario, the SE2900 is deployed between two IMS networks or between one IMS network and another type of network and forwards subscription messages between the two networks.</p>	This feature applies to both the IMS network and NGN.
		SIP Call	<p>The SIP call feature enables the SE2900 to create, modify, or terminate multi-media sessions and uses SDP to dynamically modify session attributes, such as required session bandwidths, media types (voice, video, or data), and media codec formats.</p> <p>In the I-SBC scenario, the SE2900 is deployed between two IMS networks or between one IMS network and another network and forwards call messages between the networks. For details, see 4.3.1 SIP Call.</p>	This feature applies to both the IMS network and NGN.
		SIP Fax	<p>SIP fax is a telecommunications service in which data is transmitted between two fax machines. It provides a complete set of service functions, including fax data bearer and fax service management, for fax machines on both sides of the network.</p> <p>In the I-SBC scenario, the SE2900 is deployed between two IMS networks or between one IMS network and another network and forwards fax data between the networks.</p>	This feature applies to both the IMS network and NGN.
		SIP Emer	The SIP emergency call feature enables the IMS network to identify and give special treatment to	This feature

Feature ID	Feature Name	Overview		Remarks
		Emergency Call	<p>emergency calls. When a subscriber dials an emergency call number (such as 911) or an SOS URN, the IMS network identifies this call as an emergency call and forwards the call request to the nearest EC for special treatment.</p> <p>In the I-SBC scenario, the SE2900 is deployed between two IMS networks or between one IMS network and another network and identifies a call as an emergency call and then forwards the call to a device on another network for subsequent operations.</p>	applies to both the IMS network and NGN.
		Media Policy	<p>The media policy feature enables the SE2900 to flexibly control media capabilities, such as early media, media types, media codecs, and bandwidth, ensuring proper communication between the caller and callee based on the same media type and codec. For details, see 4.3.2 Media Policy.</p>	This feature applies to both the IMS network and NGN.
		MSRP Proxy	<p>RCS defines MSRP-based picture sharing, file transmission, and chat services. The SE2900 serves as an MSRP proxy and forwards MSRP media streams between a UE and an AS or between UEs. For details, see 4.3.3 MSRP Proxy.</p>	This feature applies only to the IMS network.
		DNS Function	<p>In the I-SBC scenario, the SE2900 obtains the IP addresses of peer devices based on the domain names carried in the messages so that the SE2900 forwards the messages to the specified devices. For details, see 4.2.4 DNS Query.</p>	This feature applies to both IMS and NGN networks.
		Flow Control	<p>The SE2900 supports flow control by means of service packet type parsing, weighted queue scheduling, UDP retransmission filtering, and quick response. High-priority packets are processed promptly when the CPU usage is stable to ensure satisfactory service processing during peak hours.</p>	This feature applies to both the IMS network and NGN.
		SIP over TCP	<p>SIP over TCP applies to the IMS network in the I-SBC scenario. The SE2900 supports interworking between SIP over TCP and SIP over UDP and conversion between transport layer protocols of SIP messages. For details, see 4.3.9 SIP over TCP.</p>	This feature applies to both the IMS network

Feature ID	Feature Name	Overview		Remarks
				and NGN.
	DSCP Remark		The SE2900 assigns different DSCP values to signaling and media packets. After receiving data packets, a router preferentially forwards packets with higher DSCP priorities to ensure QoS on the VoIP network. For details, see 4.3.10 DSCP Remark.	This feature applies to both the IMS network and NGN.
	REFER Proxy		The SE2900 refers a call to the call center based on the REFER message received from the interactive voice response (IVR). For details, see 4.3.11 REFER Proxy.	This feature applies to the call center system.
	Offline Fraud Prevention		Offline fraud prevention enables the SE2900 to send CDRs to the CCF so that the fraud prevention platform can obtain the CDRs for fraud analysis and generate alarms when any fraud behavior is detected. After being informed of any such alarms, carrier's maintenance engineers can manually block the service of alarmed users to prevent fraud behavior and reduce the losses caused by such behavior. This function is supported no matter whether the CCF is built inside the SE2900 or deployed independently. For details, see 3.7 Industry-leading Security Defense Capability.	This feature applies to both the IMS network and NGN.
	Security Service		Security service refers to the optimization of security defense settings by Huawei technical support engineers based on the actual situations on live networks. Specifically, Huawei technical support engineers periodically use the security service software to download the statistics about the traffic and anomalous behaviors of each user from the SE2900, analyze the gaps between the thresholds and actual situations for three to six months, evaluate network security, and provide suggestions on the optimization of security defense settings. The security service is sold independently. For details, see 3.7 Industry-leading Security Defense Capability.	This feature applies to both the IMS network and NGN.

Table 4-3 Optional features

Feature ID	Feature Name	Overview	Remarks
SE9S00SIP00	SIP over TLS	SIP over TLS enables the SE2900 to use TLS to encrypt SIP signaling messages between a UE and the SE2900 in the A-SBC scenario, implementing secure transmission of signaling messages. For details, see 4.4.1 SIP over TLS.	This feature applies to both the IMS network and NGN.
SE9S0MSRPS00	MSRP over TLS	MSRP over TLS (MSRPS) enables the SE2900 to use TLS to encrypt MSRP media packets transmitted between a UE and the SE2900, implementing secure transmission of MSRP media packets. For details, see 4.4.2 MSRP over TLS.	This feature applies only to the IMS network.
SE9S0QOS A00	RFC2198 Redundancy	RFC2198 redundancy uses RFC2198 redundant packets to compensate for packet loss on the access side and improves audio transmission quality when the SE2900 forwards media packets between the caller and callee. For details, see 4.4.3 RFC2198 Redundancy.	This feature applies to both the IMS network and NGN.
SE9S0MED BP00	Media Bypass	<ul style="list-style-type: none"> If the SE2900 serves as a proxy for all media streams, media streams consume a lot of network bandwidth, especially in video applications. Therefore, media bypass is required in some scenarios to reduce the bandwidth consumed by media streams. Media bypass enables media streams to be transmitted between UEs without passing through the SE2900. In VoLTE roaming scenarios, optimal media routing (OMR) enables media streams in the SIP call service to be transmitted between VoLTE users (at least one is a roaming user) without passing through the devices along the path between a visited public land mobile network (VPLMN) and a home public land mobile network (HPLMN). <p>For details, see 4.4.4 Media Bypass.</p>	This feature applies to both the IMS network and NGN.
SE9S0SHM R00	SIP Header Manipulation	This feature enables the SE2900 to manipulate the headers and SDP message bodies in the received SIP messages based on configured rules (regular expressions). For details, see 4.4.5 SIP Header Manipulation.	This feature applies to both the IMS network and NGN.
SE9S0SRT P00	SRTP	SRTP enables the SE2900 to encrypt RTP media packets transmitted between a UE and the SE2900, enhancing communication security. For details, see 4.4.7 SRTP.	This feature applies to both the IMS network and NGN.
SE9S0	Firewall	The SE2900 allows signaling and media packets	This feature

Feature ID	Feature Name	Overview	Remarks
FWTR S00	Traversal	originating from RCS UEs to traverse firewalls in port aggregation mode. This feature enables carriers to quickly deploy RCS services without deploying new devices. For details, see 4.4.8 Firewall Traversal.	applies only to the IMS network.
SE9S00QOSA00	QoS Assurance	QoS assurance provides expected quality for network communication services in terms of bandwidth, packet loss rate, round-trip delay, and jitter. For details, see 4.4.9 QoS Assurance.	This feature applies to both the IMS network and NGN.
SE9S00AKA00	IMS-AKA/IPSec	IMS-AKA/IPSec enables the IMS network and IMS UEs using IP multimedia services identity module (ISIM) cards to authenticate each other. This mechanism implements mutual authentication between IMS UEs and the IMS network. For details, see 4.4.10 IMS-AKA/IPSec.	This feature applies only to the IMS network.
SE9S00SRVCC00	ATCF/ATGW	Enhanced single radio voice call continuity (eSRVCC) ensures voice call continuity when an LTE UE is handed over from the evolved universal terrestrial radio access network (E-UTRAN) to the universal terrestrial radio access network (UTRAN)/GSM EDGE radio access network (GERAN). The access transfer control function (ATCF) and access transfer gateway (ATGW) are involved in the eSRVCC handover procedure. For details, see 4.4.11 ATCF/ATGW.	This feature applies only to the IMS network.
SE9S00PSCFCF00	P-CSCF	The SE2900 provides an embedded P-CSCF. The P-CSCF is the entry point of the control plane on the IMS network (visited network). It is a proxy for all SIP messages from the access network (visited network) to the S-CSCF or I-CSCF on the home network. For details, see 4.4.12 P-CSCF.	This feature applies only to the IMS network.
SE9S00EMC00	E-CSCF/EATF	The SE2900 provides an embedded E-CSCF/emergency access transfer function (EATF). E-CSCF/EATF enables the SE2900 to process and route emergency calls to an EC. For details, see 4.4.13 E-CSCF/EATF.	This feature applies only to the IMS network.
SE9S00FR00	Flexible Routing	Flexible routing enables the SE2900 to parse the initial SIP messages and select an outgoing trunk group based on the parsing result and various routing conditions. For details, see 4.4.14 Flexible Routing.	This feature applies to both the IMS network and NGN.
SE9SS0IPITIO0	SIP-I/SIP-T Interworking	The SE2900 serves as an interworking access point of an IMS network, NGN, and IP-PBX and supports SIP/SIP-I/SIP-T interworking to complete basic services and supplementary services between the networks. For details, see 4.4.15 SIP-I/SIP-T.	This feature applies to both the IMS network and

Feature ID	Feature Name	Overview	Remarks
			NGN.
SE9S0 IPITIO 0	SIP over SCTP	SIP over SCTP enables SIP messages to be transmitted over Stream Control Transmission Protocol (SCTP) between the SE2900 and core network in the I-SBC scenario, thereby enhancing the reliability of SIP message transmission. For details, see 4.4.16 SIP over SCTP.	This feature applies to both the IMS network and NGN.
SE9S0 0IPSE C00	IPSec Tunnel	In the I-SBC scenario, to ensure security for data packets, IPSec is bound to interfaces on the SE29000 and peer NE for data authentication or encryption. For details, see 4.4.17 IPSec Tunnel.	This feature applies to both the IMS network and NGN.
SE9S0 0IPV6 00 IPV6	IPv6	IPv6 is a feature that enables the SE2900 to provide network access using IPv4/IPv6 dual-stack. With this feature, IPv4/IPv6 UEs can access an IPv4/IPv6 core network and IPv4/IPv6 core networks can interwork with each other. For details, see 4.4.18 IPv6.	This feature applies to both the IMS network and NGN.
SE9S0 0PBX TRK0 0	IP-PBX Trunkin g	The SE2900 implements IP-PBX trunking to provide IP-private branch exchanges (IP-PBXs) with access to the IMS network. In IP-PBX trunking, an IP-PBX that has the registration capability accesses the IMS network through the A-BCF, and an IP-PBX that does not have the registration capability accesses the IMS network through the IBCF. For details, see 4.4.19 IP-PBX Trunking.	This feature applies only to the IMS network.
SE9S0 0ACO DEC0 0	Audio Transco ding	Audio transcoding enables the SE2900 to convert media packets from one media format to another. With this feature, the SE2900 allows UEs using different media formats to communicate with each other. For details, see 4.4.20 Audio Transcoding.	This feature applies to both the IMS network and NGN.
SE9S0 0ROC DR00	Chargin g	Charging enables the SE2900 to implement offline charging by interworking with the charging collection function (CCF) over the Rf interface. For details, see 4.4.21 Charging.	This feature applies only to the IMS network.
SE9S BSEC SW00	Security Enhanc ement Functio n	Security enhancement includes intrusion detection system (IDS), blacklist/whitelist (manually configured), media plane security, and call admission control (CAC). For details, see 4.4.22 Security Enhancement Function.	This feature applies to both the IMS network and NGN.
SE9S0 RDCC N00	Redund ancy of Core	The SE2900 supports the core network redundancy feature using the dual-homing or P-CSCF pool networking scheme. For details, see 4.4.23 Redundancy	This feature applies to both the

Feature ID	Feature Name	Overview	Remarks
	Network	of Core Network.	IMS network and NGN.
SE9S00SHIWF00	SIP-H.323 Interworking	SIP-H.323 interworking enables the SE2900 to provide basic and supplementary services between IMS/NGN and H.323 networks. For details, see 4.4.24 SIP-H.323 Interworking.	This feature applies to both the IMS network and NGN.
SSE9S00DSHB00	Dual-system Hot Backup	The SE2900 supports the dual-system hot backup feature to ensure service reliability. This feature provides a geographic redundancy solution for carriers. For details, see 4.4.26 Dual-System Hot Backup.	This feature applies to both the IMS network and NGN.
SE9S00HDV00	VoLTE High Definition Video	The SE2900 implements control over the number of concurrent video calls, ensuring experience of VIP users even in network congestion. For details, see 4.4.25 Standard Definition/High Definition Video.	This feature applies only to the IMS network.
SE9S00SDV00	VoLTE Standard Definition Video	The SE2900 implements control over the number of concurrent video calls, ensuring experience of VIP users even in network congestion. For details, see 4.4.25 Standard Definition/High Definition Video.	This feature applies only to the IMS network.
SE9S00STG A00	Security Traversal Gateway	The security traversal gateway (STG) feature enables the SE2900 to encrypt and encapsulate RCS service packets into TLS/DTLS tunnel packets and send them through TCP/UDP port 443 so that the encapsulated TCP/UDP packets can traverse the firewall or HTTP proxy. This feature mainly applies to the IMS network and enterprise network. For details, see 4.4.27 Security Traversing Gateway.	This feature applies only to the IMS network.
SE9S VOWIFI00	VoWiFi Access	VoWiFi access enables UEs to make voice calls after registering with the IMS network over Wireless Fidelity (Wi-Fi). During a UE handover between Wi-Fi and LTE, the SE2900 identifies the access network type change and notifies the change to the core network so that the core network performs distinctive charging. The SE2900 also supports the emergency call initiated over Wi-Fi. For details, see 4.4.29 VoWiFi Access.	This feature applies only to the IMS network.
SE9S VOLTER00	VoLTE Roaming	The SE2900 enables VoLTE users to use roaming services on the IMS network without having to fall back to the 2G/3G network based on 3GPP and Global System for Mobile Communications Association (GSMA)'s standards. For details, see 4.4.28 VoLTE	This feature applies only to the IMS network.

Feature ID	Feature Name	Overview	Remarks
		Roaming.	

4.2 A-SBC Basic SW

4.2.1 SIP Call

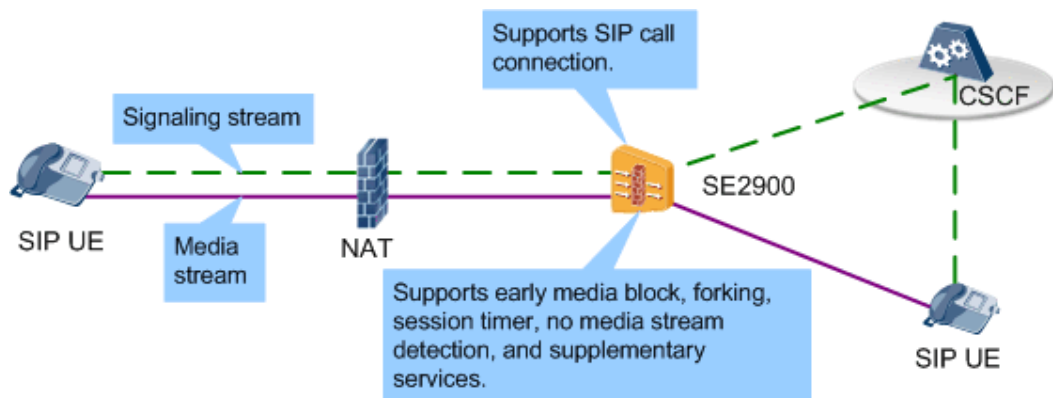
The SIP call feature enables the SE2900 to create, modify, or terminate multi-media sessions and use SDP to dynamically modify session attributes, such as required session bandwidths, media types (voice, video, or data), and media codec formats.

 **NOTE**

A SIP call is a logical connection established between two nodes, over which audio or video data is transmitted. Nodes can be UEs or network devices.

In the A-SBC scenario, the SE2900, which is deployed at the edge of the IMS network, forwards call messages from SIP UEs to the IMS network or from the IMS network to SIP UEs. Figure 4-1 shows the SIP call procedure.

Figure 4-1 SIP call procedure



Various types of SIP UEs with different media capabilities exist on the live network. The SE2900 performs media negotiation in the SIP call procedure to enable the SIP UEs with different media capabilities to exchange media packets using the same media type and codec. In the SIP call procedure, the SE2900 also supports early media block, forking, session timer, no media stream detection, and supplementary services.

- Early media block

After SDP offer/answer negotiation is complete and before the callee sends a 200 OK message, the caller and callee have known the media address of each other. At this point, the caller and callee can speak to each other. Because the SE2600 starts charging only after receiving a 200 OK message from the callee, there is a possibility that malicious users take advantage of this situation and make free calls. Early media block applies to the A-SBC scenario. With this feature, the SE2900 discards the media packets

originating from or destined for the callee before receiving a 200 OK message from the callee, preventing malicious users from making free calls.

- **Forking**

Forking enables the SE2900 to act as a proxy for a single-number multi-contact user when the core server sends a call request to the user. (The call request generates multiple session forks.) The SE2900 supports parallel search and sequential search in forking.

 - In parallel search, the core server constructs multiple requests at a time and sends the requests to all the qualified UEs (specified by the callee address) simultaneously.
 - In sequential search, the core server constructs multiple requests at a time and sends one of the requests to a qualified UE (specified by the callee address). After receiving a non-2XX or non-6XX final response to this request, the core server sends another request to next UE.
- **Session timer**

Session timer is a mechanism in which after a session is established, a UE or an NE periodically sends a session refresh request to a peer device to detect whether the peer device is in the active state. With the session timer, the SE2900 or core server can terminate sessions once the UE is not in a conversation or any involved NE fails, thereby preventing these sessions from wasting network resources. On the IMS network, service control is separate from service bearer, and signaling is separate from media. Therefore, when a fault occurs, there is a probability that media streams are unavailable but signaling is not released, resulting in an extra-long call detail record (CDR). With the session timer, abnormal sessions can be terminated in time, thereby ensuring accurate charging and avoiding unnecessary loss to users.
- **No media stream detection**

No media stream detection enables the SE2900 to send a BYE message to a UE and a core server after detecting that no media stream is available in one direction or both directions of a session for a period that is longer than the maximum allowable period. The core server tears down the session immediately after receiving the BYE message, improving the accuracy of subscriber charging.
- **Supplementary services**

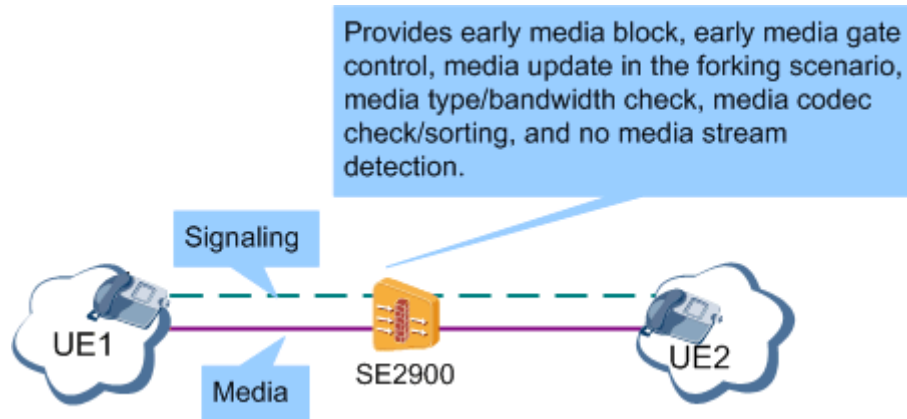
The SE2900 collaborate with the core server to implement supplementary services, including call hold, call transfer, third-party calling, conference calling, and short message receipt.

4.2.2 Media Policy

The media policy feature enables the SE2900 to flexibly control media capabilities, such as the early media, media types, media codecs, and bandwidth. This feature enables different types of UEs to communicate using the same media type and codec. This feature enables carriers to implement flexible control on media capabilities over the network, thereby ensuring proper use of network resources.

The SE2900 controls media capabilities based on media policies in the A-SBC scenario. See Figure 4-2.

Figure 4-2 Media policy



In the A-SBC scenario, the media policy feature provides the following functions:

- Early media block

Before the callee returns a 200 OK response to complete the establishment of a SIP call, the SE2900 does not forward media packets to or from the callee, preventing users from making free calls.

 **NOTE**

- The SE2900 blocks the media packets to and from the callee but it forwards the media packets to and from the caller. This is to ensure that the caller can use services such as the ring back tone (RBT), based on early media interworking.
- The SE2900 blocks only media streams transmitted over UDP. It does not block media streams transmitted over TCP.
- The SE2900 does not block Real-Time Transport Control Protocol (RTCP) packets.
- Early media gate control

After receiving a message that includes the P-Early-Media header, the SE2900 enables or disables the gate control based on the header.
- Media update in the forking scenario

In the forking scenario, after receiving responses along multiple forking paths, the SE2900 performs bearer control over the early media transferred along these forking paths and upgrades the media based on the P-Early-Media header.
- Media type check and media bandwidth check
 - Media type check: The SE2900 restricts the types of media packets transferred over the network and blocks media packets of specific media types, such as video packets.
 - Media bandwidth check: The SE2900 restricts the bandwidth for each type of media packet and prevents UEs from overusing media bandwidth.
- Media codec check and media codec sorting
 - Media codec check: The SE2900 restricts the audio and video codecs that are allowed across the network.
 - Media codec sorting: The SE2900 sorts the media codecs in the SDP offer by priority, ensuring that high-priority media codecs are used in the communication between the caller and callee.
- No media stream detection

When the signaling plane is normal but the media plane is abnormal, if the SE2900 detects no media stream within the specified time period, it sends a BYE message to both the UE and the core server. The core server then tears down the session upon receiving the BYE message, thereby improving charging accuracy.

4.2.3 MSRP Proxy

MSRP is a session-based connection-oriented protocol used to exchange Multipurpose Internet Mail Extensions (MIME) content in any format, including binary content. MSRP establishes sessions using the SDP offer/answer model. During SIP session establishment, both parties negotiate MSRP uniform resource identifiers (URIs) and MSRP extensions. After SIP session establishment is complete, MSRP messages are transmitted on the media plane to exchange MIME contents. MSRP is an application layer protocol and runs over connection-oriented protocols such as TCP. An MSRP message can be a request or a response.

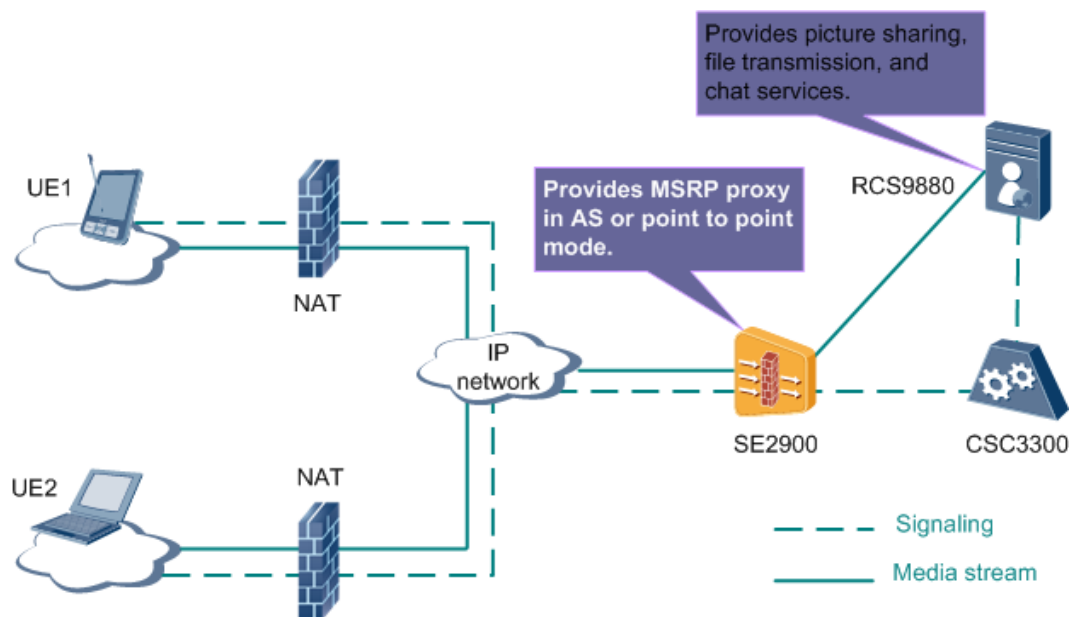
Rich Communication Suite (RCS) defines a variety of enhanced services, such as Message Session Relay Protocol-based (MSRP-based) picture sharing, file transmission, and chat services. The MSRP proxy feature enables the SE2900 to act as an MSRP session proxy and forward MSRP media streams between a UE and an AS or between UEs during RCS services. Figure 4-3 shows the MSRP proxy networking.



NOTE

MSRP proxy is a basic feature in which MSRP packets are transmitted not over TLS, while MSRP over TLS is an optional feature in which MSRP packets are transmitted over TLS. 4.4.2 MSRP over TLS shows the MSRP proxy mechanism.

Figure 4-3 MSRP proxy



RCS services use the following MSRP modes:

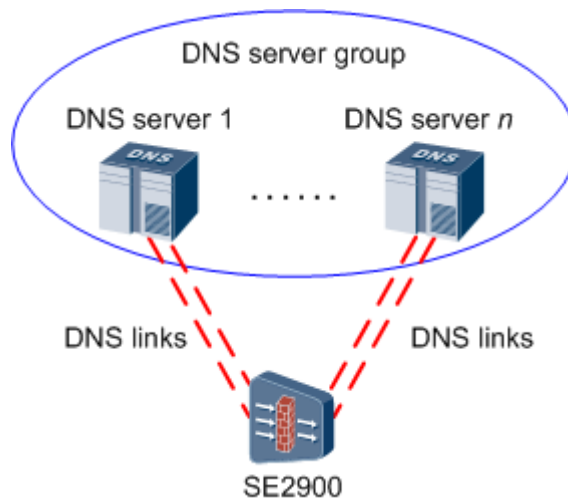
- AS mode: An MSRP session is established between a UE and the AS. This mode is used in chat and file transmission services.
- Point-to-point mode: An MSRP session is established between two UEs. This mode is used in the picture sharing service.

4.2.4 DNS Query

The domain name system (DNS) is used to route signaling messages by translating between domain names and IP addresses. In the A-SBC scenario, after receiving an initial REGISTER request, the SE2900 queries for the P-CSCF address from the embedded DNS or external DNS server based on the domain name, if the dynamic routing mode is configured on the SE2900. Then the SE2900 sends the REGISTER request to the P-CSCF. The SE2900 supports embedded DNS and external DNS.

- Embedded DNS: The SE2900 supports DNS-query-based routing based on the DNS data configuration in the database management system (DBMS).
- External DNS: The SE2900 supports DNS-query-based routing for SIP registration or calls based on the configuration of the connection between the SE2900 and DNS servers. Figure 4-4 shows the external DNS query mechanism.

Figure 4-4 External DNS query

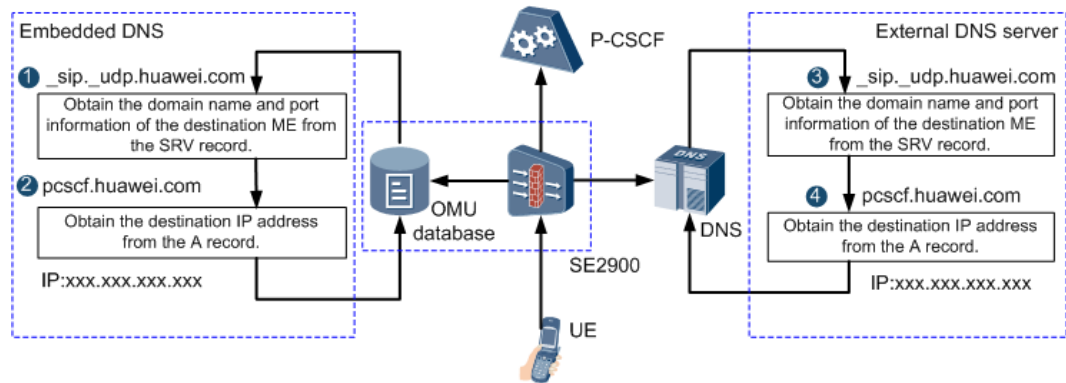


Advantages and disadvantages of embedded DNS and external DNS:

- Embedded DNS is more efficient than external DNS. In external DNS, the SE2900 obtains required information over the links to external DNS servers, and therefore a delay occurs. In embedded DNS, no DNS links are involved, and DNS query is faster.
- External DNS is more reliable than embedded DNS. One SE2900 can be connected to multiple DNS servers. These DNS servers can be deployed in different locations and configured to operate in master/backup or load-balancing mode.

Embedded DNS and external DNS can be configured separately or simultaneously. If external DNS and embedded DNS are both configured, the SE2900 performs embedded DNS query first. If the embedded DNS query fails, the SE2900 performs external DNS query. Figure 4-5 shows the DNS query sequence.

Figure 4-5 DNS query sequence



4.2.5 Virtual SBC

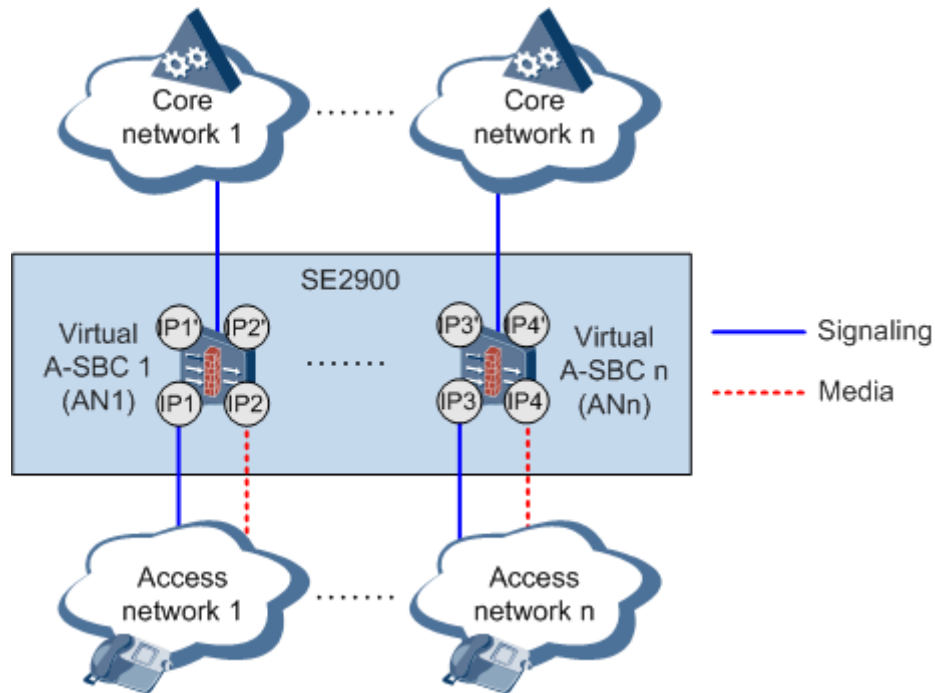
One SE2900 can be divided into several virtual A-SBCs to serve different access networks. Each virtual A-SBC separately processes signaling, media, and routing information for UEs on each access network.

The virtual A-SBC is used when multiple access networks connect to one or more core networks. This feature has the following advantages:

- Saves capital expenditure (CAPEX) and operating expense (OPEX) for carriers.
- Simplifies network architecture.
- Facilitates the delivery of universal services.
- Enables fast deployment of new services.

The A-BCF divides the UEs that access the SBC into multiple ANs based on UE addresses and access-side signaling addresses. Each AN serves as an independent virtual SBC. Figure 4-6 shows the virtual SBC networking.

Figure 4-6 Virtual SBC networking



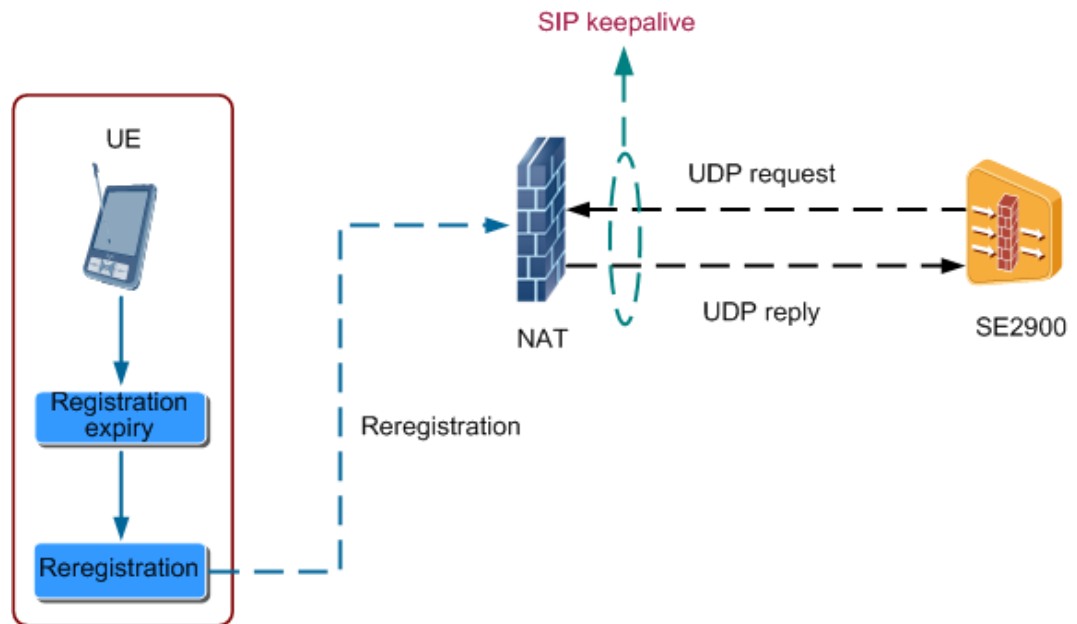
Multiple virtual SBCs are deployed on one SE2900. Each virtual SBC operates independently and has separate resources, traffic, call admission control (CAC) policies, traffic statistics, and logs. Each SE2900 can be configured with only one A-BCF. One A-BCF supports the configuration of a maximum of 6000 ANs, namely, 6000 virtual A-SBCs.

4.2.6 SIP Keepalive and NAT Traversal

SIP Keepalive

The NAT device uses a configurable aging timer for mapping entries. Generally, the reregistration time of a SIP UE is longer than the aging time of address mapping entries on the NAT device. The SE2900, being a heuristic device, can learn the addresses of UE-initiated packets after NAT. After the address mapping entry for a SIP UE on the NAT device ages out, if the NAT device receives a service packet originating from a SIP UE, the NAT device will be unable to find an address mapping entry and therefore will discard the packet. As a result, the requested service is interrupted. To avoid such service interruption, the SE2900 periodically sends UDP packets to the NAT device to refresh the aging time of address mapping entries on the NAT device and keep them alive. Figure 4-7 shows the SIP keepalive networking.

Figure 4-7 SIP keepalive networking



The SE2900 keeps NAT entries alive by sending any of the following packets:

- Hello packet
The SE2900 sends Hello packets (UDP packets) to a UE at regular intervals. Hello packets are a type of user-defined packet.
- SIP re-REGISTER packet
After receiving a registration response from the core network, the SE2900 modifies the Expire header or parameter to force the UE to immediately send a re-REGISTER request. The SE2900 updates the aging time of address mapping entries on the NAT device according to the Re-REGISTER request before the entries expire.
- STUN packet
When signaling is transmitted over UDP between a UE and the SE2900, the UE sends Simple Traversal of UDP through NAT (STUN) keepalive messages to the SE2900 at regular intervals. After receiving a STUN keepalive message, the SE2900 returns a STUN response.
- CLRf packet
When signaling is transmitted over TCP between a UE and the SE2900, the UE sends ping keepalive packets to the SE2900 at regular intervals. After receiving a ping keepalive message, the SE2900 returns a pong response.

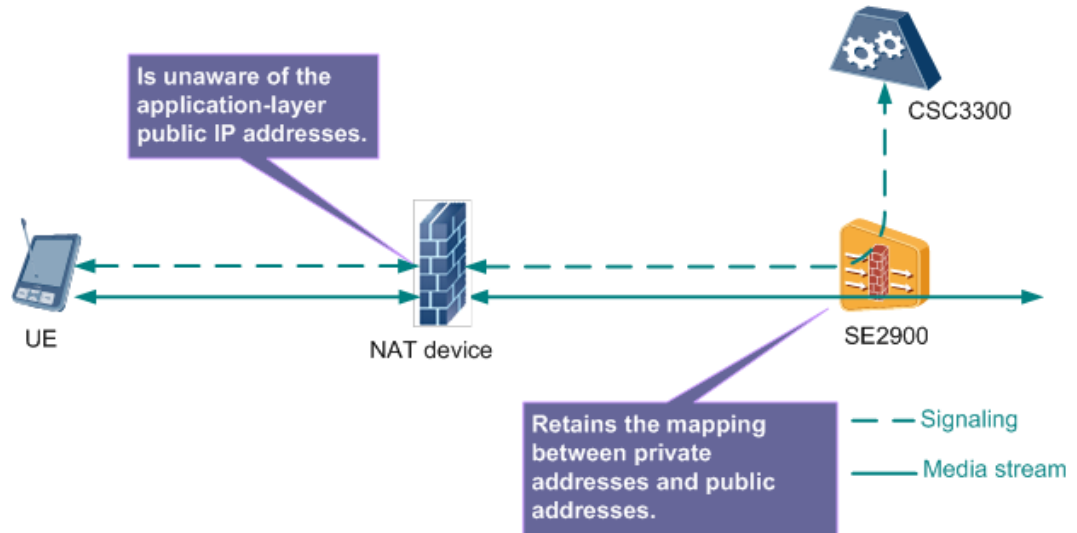
NAT Traversal

Many enterprises use private addresses for internal communications and apply for only a few public addresses from carriers for external communications. As packets with private addresses cannot be routed across the Internet, a NAT device is needed to translate between private addresses and public addresses.

NAT helps process and filter packets at layers lower than the transport and network layers. When a packet passes through the NAT device, the network layer address and transport layer address of the packet are changed but the application layer address is still a private address. If

the peer device returns a packet to the application layer address, the packet will fail to reach the destination. The SIP application address is an application layer address. To ensure the transmission of SIP signaling messages, the SE2900 implements NAT traversal by changing the receive addresses + ports UEs use to receive SIP signaling messages. Figure 4-8 shows the NAT traversal mechanism.

Figure 4-8 NAT traversal



4.2.7 Address Overlapping

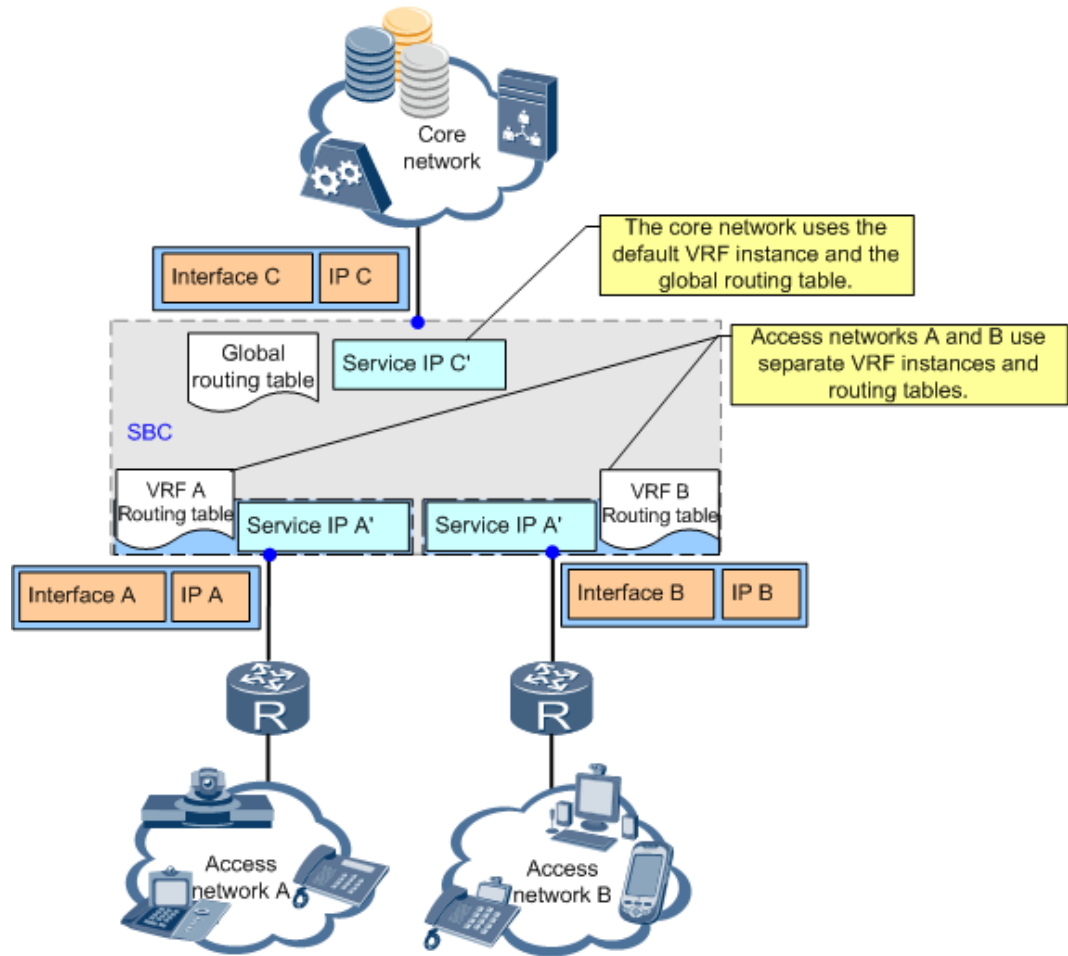
Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist on the SE2900, which is used to implement address overlapping. Packets are sent and received independently in each VRF instance. Routing instances are independent of each other, with their own routing entries, interfaces, and IP addresses. The overlapping IP addresses/segments can be used in different routing instances without conflicting with each other.

The SE2900 allows access network addresses to overlap with each other, core network addresses to overlap with each other, and access network addresses and core network addresses to overlap with each other. Address overlapping implements the sharing of IP addresses/segments and simplifies the service and application configurations on different access networks. Address overlapping saving the IP address, and much more compatible with live network.

Overlapping Between Access Network Addresses

Two access networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-9 shows the networking for overlapping between access network addresses.

Figure 4-9 Overlapping between access network addresses



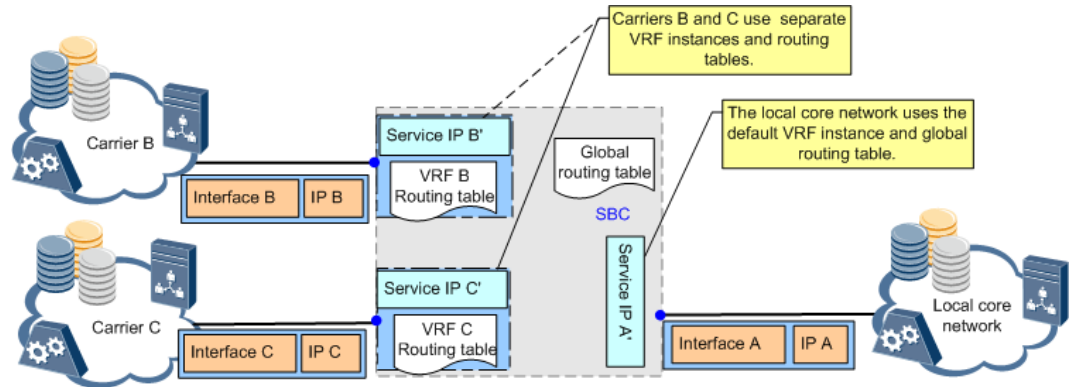
In Figure 4-9, access networks A and B connect to the SBC. Access network A is at 10.0.0.0/8, while access network B is at 10.2.0.0/16. The two network segments are overlapping. All the packets whose destination addresses belong to 10.2.0.0/16 are sent to access network B through interface B. The UEs at 10.2.0.0/16 on access network A cannot access services.

To address the issue, the SBC separates the two access networks to different VRF instances.

Overlapping Between Core Network Addresses

Two core networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-10 shows the networking for overlapping between core network addresses.

Figure 4-10 Overlapping between core network addresses



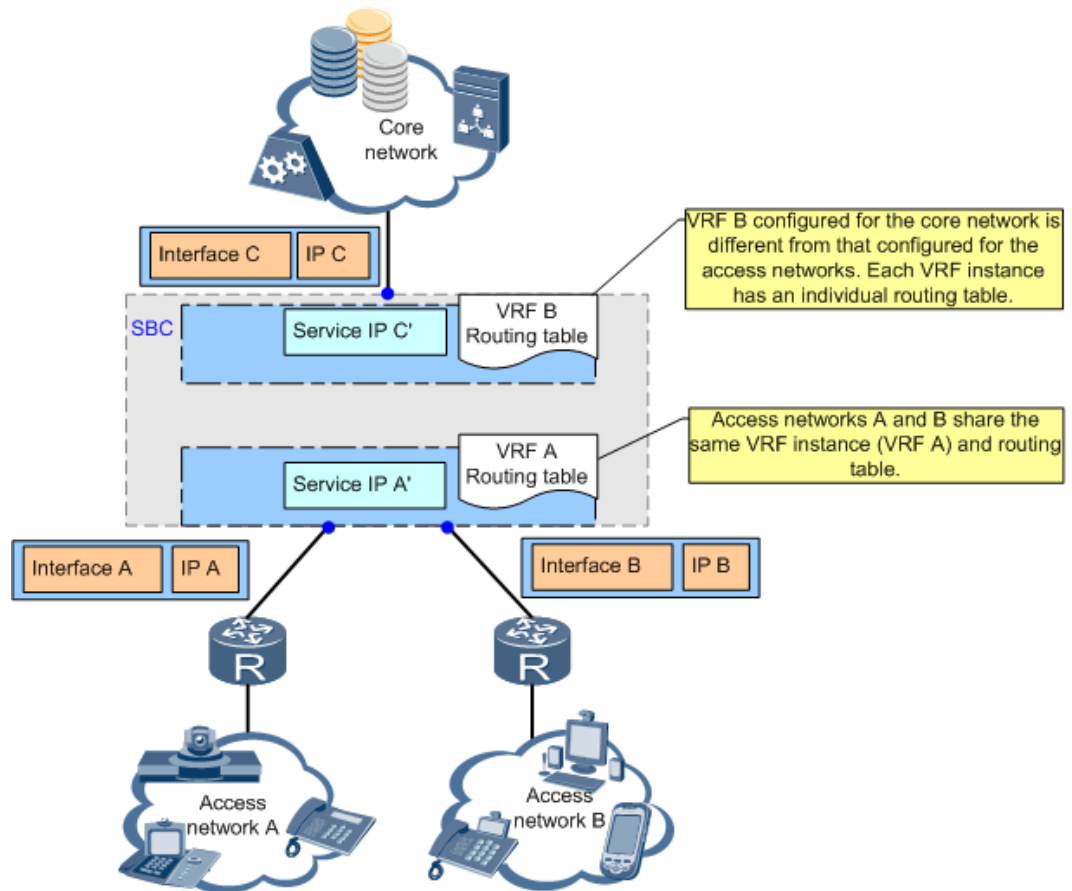
In Figure 4-10, the core network of carrier B is at 11.0.0.0/8, where the core network of carrier C is at 11.0.0.0/16. The two network segments are overlapping.

The SBC separates the two core networks to different VRF instances so that the UEs on access networks can access services.

Overlapping Between Access Network Addresses and Core Network Addresses

Access networks and core networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-11 shows the networking for overlapping between access network addresses and core network addresses.

Figure 4-11 Overlapping between access network addresses and core network addresses



In Figure 4-11, access networks A and B are at 10.0.0.0/8, where the core network is at 10.0.0.0/8. The two network segments are overlapping. The UEs on access networks A and B cannot access services.

To address the issue, the SBC separates the access networks and the core network to different VRF instances.

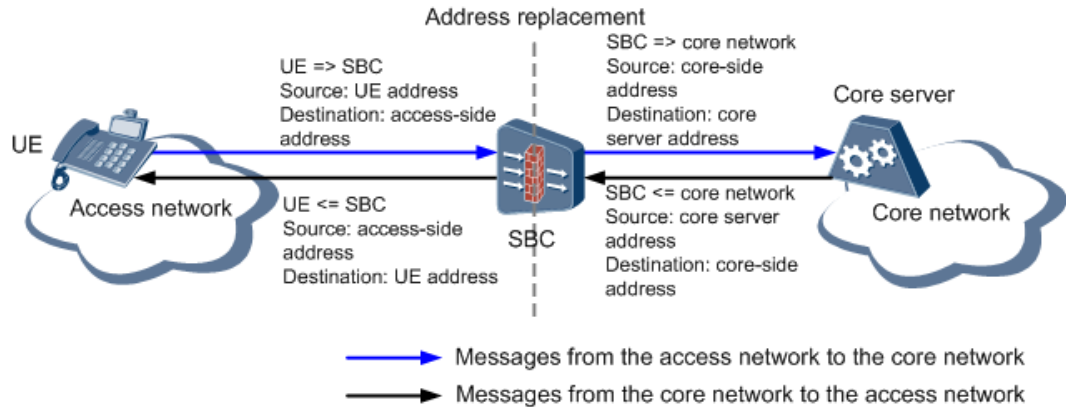
4.2.8 Topology Hiding

Network topology may be exposed because of routing information carried in SIP messages during SIP calls. Attackers may probe the network structure by obtaining network topology carried in SIP messages.

Deployed between the public network and private network, the SE2900 hides the core network topology from the access network and hides the access network topology from the core network. Topology hiding of the core network can prevent core servers from being exposed to users. It can also prevent other carriers from obtaining information about the core network topology, therefore enhancing network architecture security.

The SE2900 implements topology hiding by translating between core-side and access-side addresses during message processing at the IP, transport, and signaling layers. Figure 4-12 shows the topology hiding mechanism.

Figure 4-12 Topology hiding



- On the core network, the SE2900 implements topology hiding by using the Network Address Translation (NAT) mechanism to translate IP addresses and ports so that the access network can only obtain the IP addresses and ports of the SBC instead of core server addresses.
- On the access network, the SE2900 implements topology hiding by changing the IP address + port at the transport layer, and IP address and SIP headers (including Via and Route headers) in the SIP message so that the core network cannot obtain the actual IP addresses and ports of UEs.

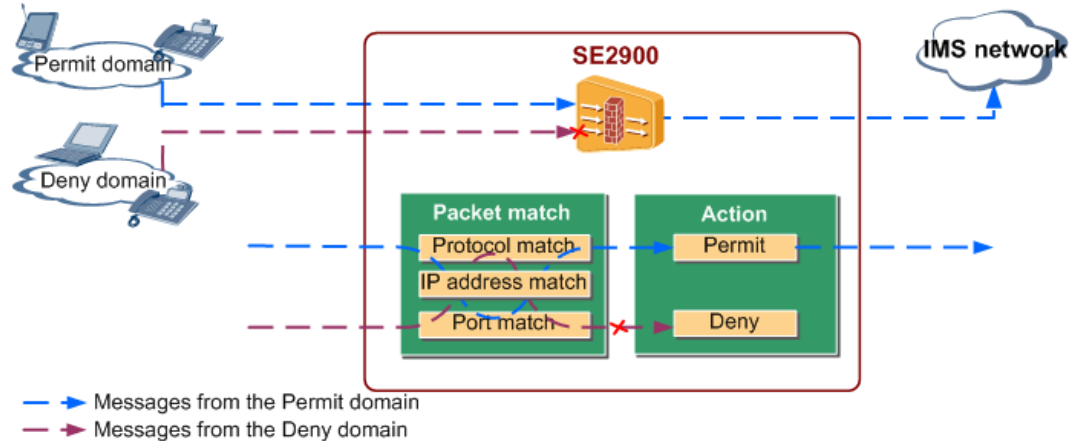
4.2.9 IP Layer Security

ACL-based Packet Filtering

An ACL defines rules that are used to filter IP packets. The SE2900 matches IP packets with the rules and discards the packets (for example, call packets initiated by unauthorized users) that do not conform to the rules.

After receiving a packet, the SE2900 performs ACL-based filtering first. The SE2900 performs subsequent operations only on conforming packets. This processing protects closed ports and services against attacks. Figure 4-13 shows the ACL-based packet filtering mechanism.

Figure 4-13 ACL-based packet filtering



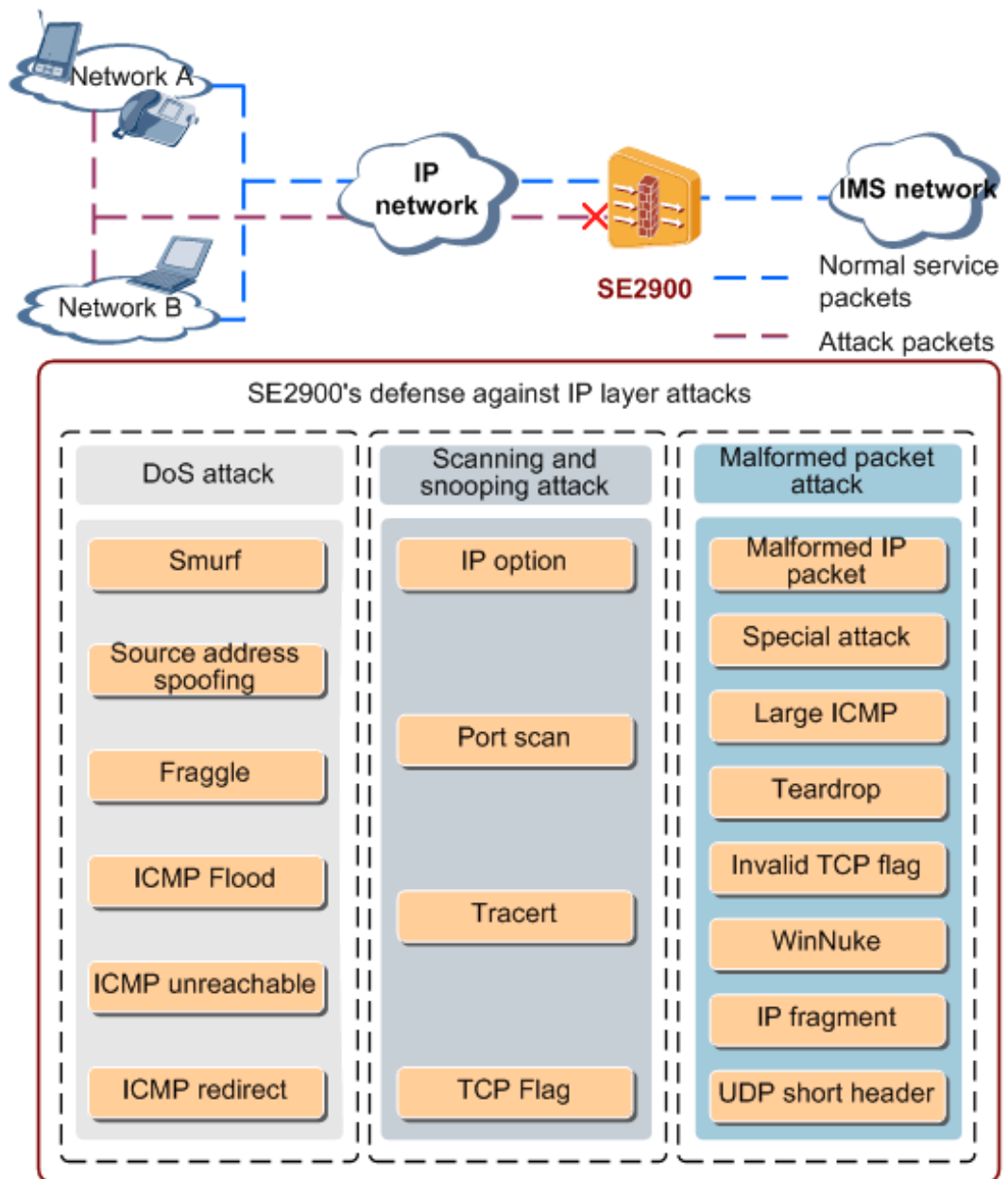
The SE2900 supports standard and advanced ACL groups.

- The standard ACL group contains basic ACL rules, which are defined based on the source IP address.
- The advanced ACL group contains advanced ACL rules, which are defined based on the source address + port, destination address + port, and protocol type. Advanced ACLs allow for more accurate, diversified, and flexible rules.

DoS/DDoS Attack Defense

Nowadays, most networks adopt the all-IP architecture and use SIP as the session control mechanism. All signaling messages and media messages are carried in IP packets. An attacker can launch an IP layer attack by sending a large number of IP packets to the target host, exhausting the host's resources; or by sending malformed IP packets to the target host, causing the host that processes the malformed packets to break down. The SE2900 identifies, classifies, and filters out IP attack packets at the edge of the core network. Figure 4-14 shows the DoS/DDoS attack defense mechanism.

Figure 4-14 DoS/DDoS attack defense



After identifying attack packets, the SE2900 discards them and counts the number of attack packets. When the number of attack packets reaches a specified threshold, the SE2900 generates an IP layer attack defense alarm.

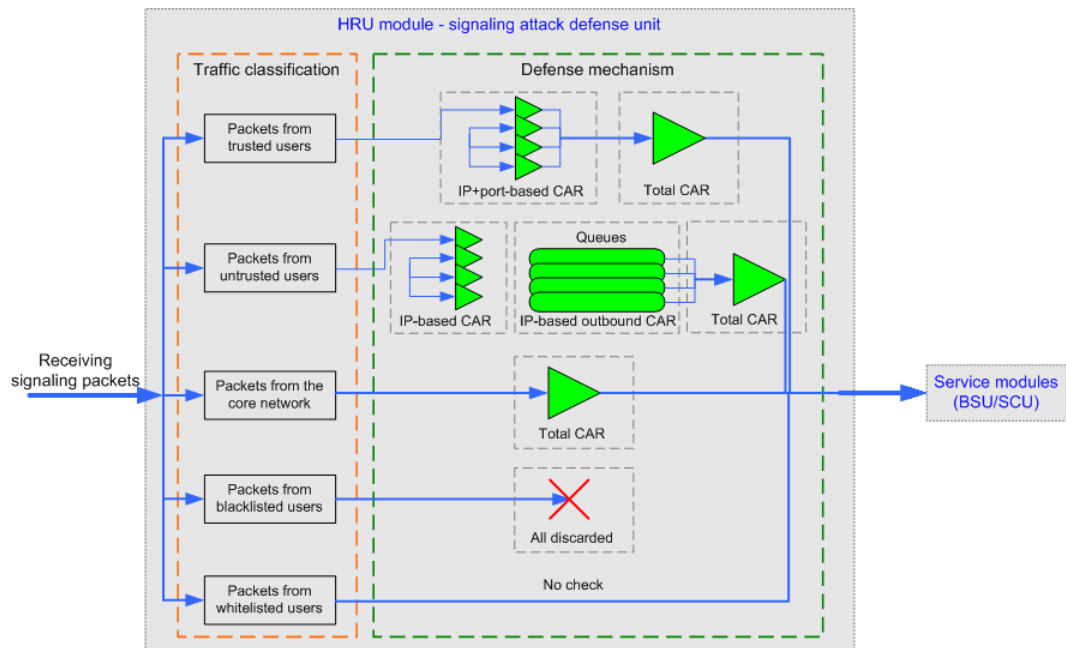
4.2.10 Signaling Plane Security

DoS/DDoS attacks are the major threats to the signaling plane. In a DoS/DDoS attack, an attacker sends a large number of data packets to the target host to exhaust system resources, causing the host unable to process valid requests from legitimate users. DoS attacks are launched by a single attacker, whereas DDoS attacks are launched by multiple attackers. In most cases, an attacker launches a DoS/DDoS attack by sending huge numbers of packets to a well-known port, such as the SIP well-known port 5060, attempting to exhaust the system

resources. An attacker may also take advantage of system vulnerabilities and send attack packets to cause system exceptions, such as memory overwriting, memory leak, and call stack overflow/reset.

The signaling attack defense module on the SE2900 performs strict flow control over received SIP messages. Different flow control policies can be applied to packets from different users. Figure 4-15 shows the DoS/DDoS attack defense mechanism.

Figure 4-15 DoS/DDoS attack defense



- Packets from trusted users: The SE2900 restricts the committed access rate (CAR) of the packets from each source IP address + port and the packets on each service processing module.
- Packets from untrusted users: The SE2900 restricts the CAR of the packets from each source IP address, places all received IP packets into 2048 queues by source IP address, and restricts the CAR of the packets on each service module.
- Packets from the core network: The SE2900 restricts the overall rate of received packets.
- Packets from blacklist users: The SE2900 discards all the packets.
- Packets from whitelist users: The SE2900 does not perform flow control on the packets.

4.2.11 Media Plane Security

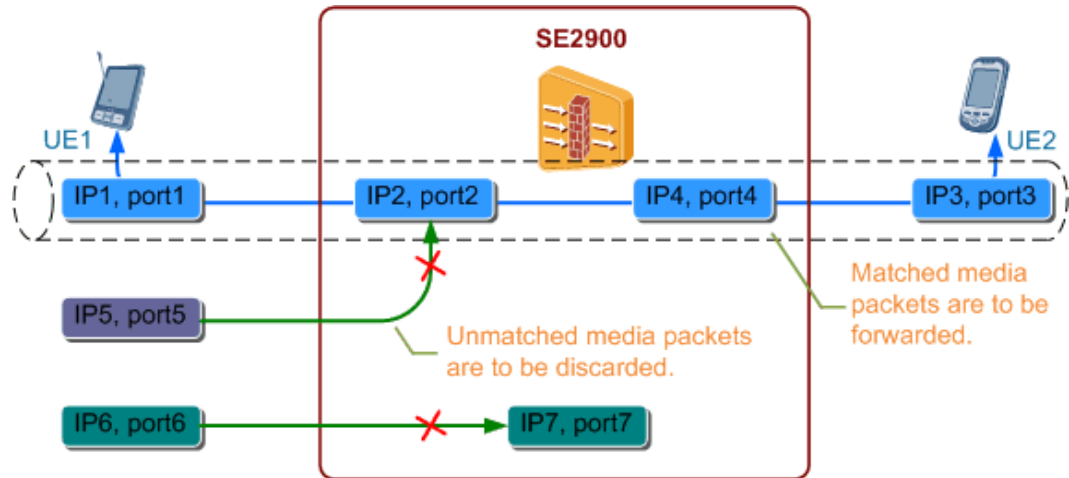
Media Pinholing Firewall

The dynamic pinholing firewall feature enables the SE2900 to dynamically create media session entries (IP 5-tuple) based on signaling negotiation results. Figure 4-16 shows the media pinholing firewall mechanism.

 **NOTE**

IP 5-tuple consists of the source IP address, source port number, destination IP address, destination port number, and protocol in use.

Figure 4-16 Media pinholing firewall



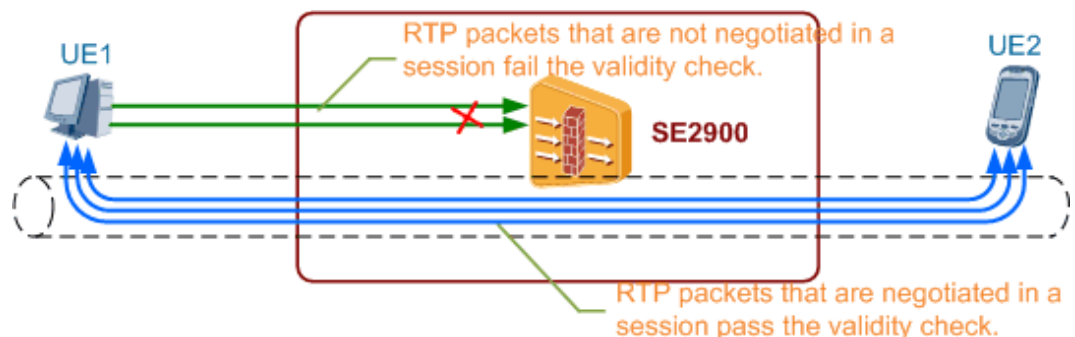
- After receiving media packets in a call procedure, the SE2900 extracts 5-tuple information. The SE2900 matches the 5-tuple information against media session entries and only forwards media packets with matching media session entries.
- When the call is over, the SE2900 deletes the media session entries of the call after receiving a BYE message.

Malformed RTP Packet Attack Defense

An attacker can send a huge number of RTP packets to attack the SE2900 or its peer media device. The SE2900 performs validity checks on RTP packets to implement malformed RTP packet attack defense.

After an RTP packet passes through the media pinholing firewall, the SE2900 checks the version number and payload type of the RTP packet header. If the version number of an RTP packet is not 2 or the payload type of the RTP packet header is different from that negotiated in the session, the RTP packet fails the validity check. The SE2900 then considers the RTP packet to be an attack packet and discards it. Figure 4-17 shows the malformed RTP packet attack defense mechanism.

Figure 4-17 Malformed RTP packet attack defense

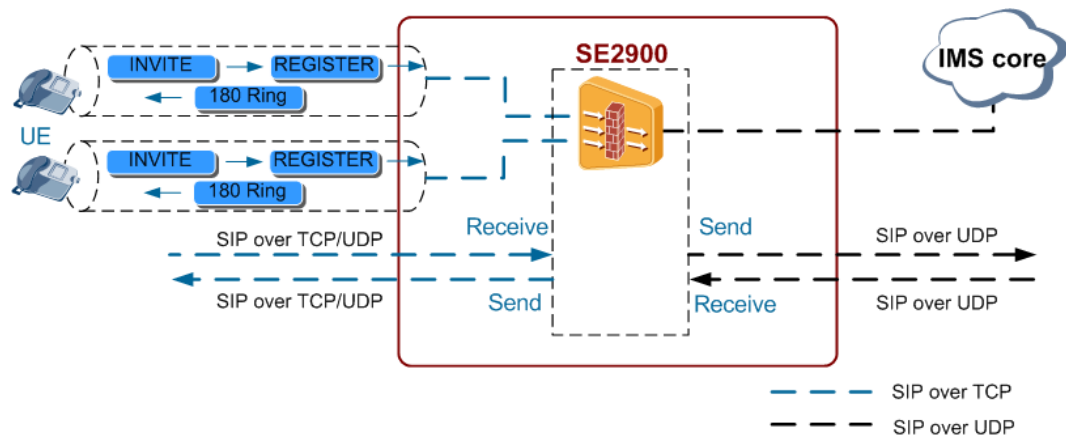


4.2.12 SIP over TCP

TCP is connection-oriented and provides reliable data transmission. TCP achieves reliable end-to-end transmission using a series of measures, including retransmission, duplicate data discarding, checksums, and traffic control.

In the A-SBC scenario, when the MTU value of packets transmitted between the SE2900 and UEs is 1300 bytes or greater, the SE2900 uses TCP to transmit SIP messages; when the MTU value of packets transmitted between the SE2900 and UEs is less than 1300 bytes, the SE2900 uses UDP to transmit SIP messages. See Figure 4-18.

Figure 4-18 SIP over TCP



The SE2900 supports the processing of SIP messages over TCP and UDP.

- Before forwarding a UE-originated message to the core network, the SE2900 changes the transport layer protocol from TCP to UDP.
- Before forwarding a core-network-originated message to the UE, the SE2900 changes the transport layer protocol from UDP to TCP.

As the transmission network between UEs and the SE2900 is unstable, SIP over TCP is used to enhance the reliability of data transmission.

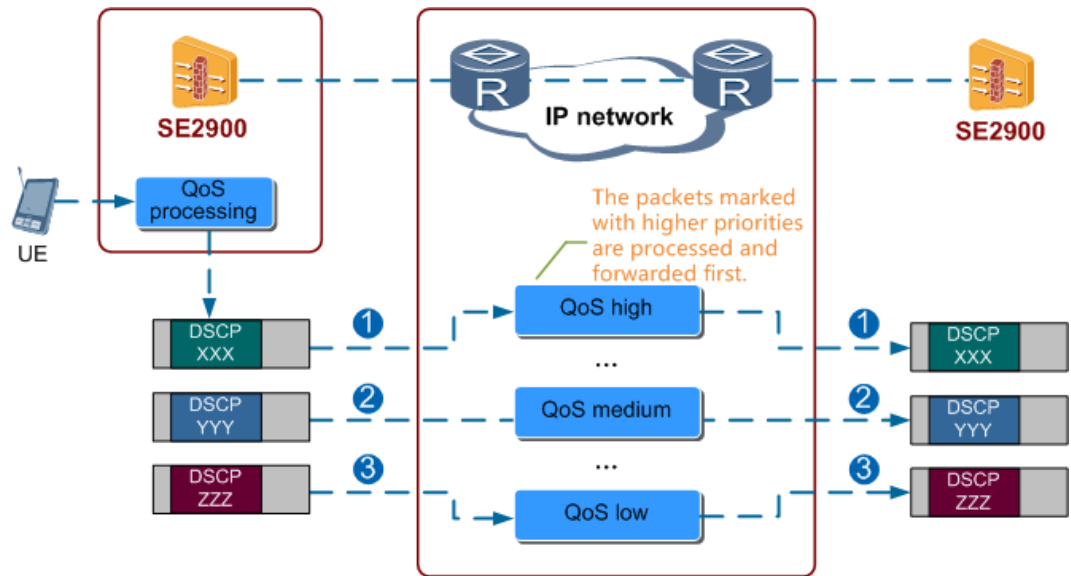
By comparison, UDP provides connectionless and unreliable data transmission. UDP does not set up a dedicated end-to-end connection for before starting traffic transmission. The destination device does not confirm whether the correct data packet has been received. Therefore, UDP messages may be lost, duplicated, delayed, or delivered out of order. However, UDP has a higher transmission efficiency than TCP. SIP over UDP can be used between the SE2900 and IMS core servers, which are both located in carriers' central equipment room and have reliable transmission conditions.

4.2.13 DSCP Remarking

DSCP remarking: The SE2900 assigns different DSCP values to signaling and media packets. After receiving data packets, a router preferentially forwards packets with higher DSCP priorities to ensure QoS on the voice over Internet Protocol (VoIP) network.

DSCP remarking enables carriers to prioritize the services of high-priority subscribers by allocating resources and implementing charging based on the service priorities of subscribers stored on the HSS. Figure 4-19 shows DSCP remarking.

Figure 4-19 DSCP remarking



DSCP remarking can be performed on both signaling packets and media packets.

- DSCP remarking on signaling packets: **ADD AADDR** can be used to set DSCP values for SIP signaling packets. When sending a SIP signaling packet, the SE2900 searches for a corresponding DSCP value based on the source IP address of the SIP signaling packet.
- DSCP remarking for media packets: The SE2900 supports AN-specific DSCP values for various media types. When an AN record is added for a specified A-BCF, the system automatically adds the default media QoS record that corresponds to the AN to the A-BCF default QoS information table.

4.2.14 H.248 Proxy

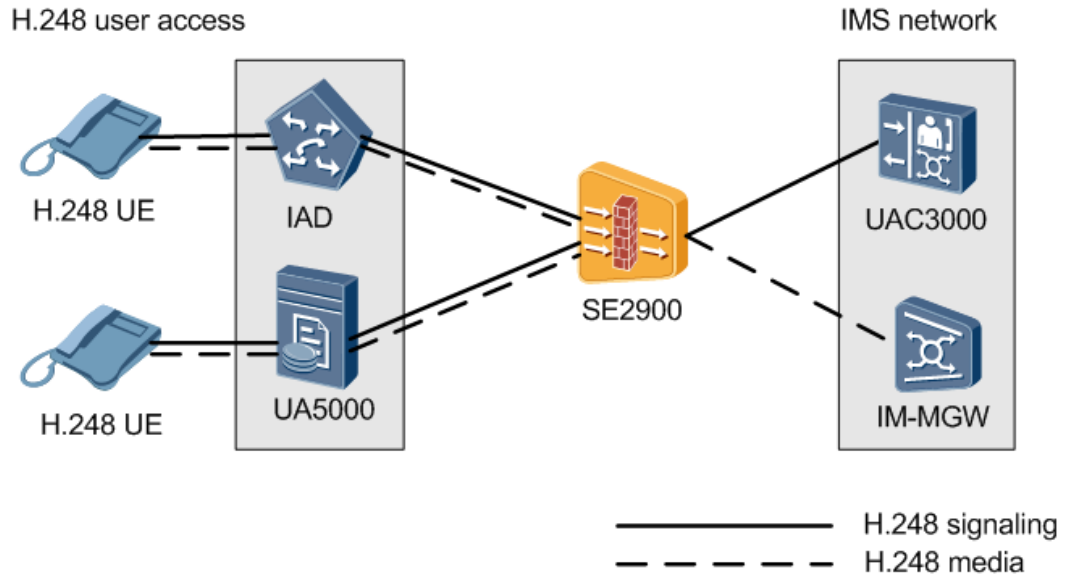
H.248 proxy enables the SE2900 to allow H.248 users to access IMS networks/NGNs by means of signaling and media proxy. With this function, the SE2900 can ensure IMS network/NGN security and achieve QoS, media, and nomadic management. The SE2900 is deployed at the edge of an IP network or deployed at the convergence layer and acts as a convergence point for signaling and media streams.

H.248 proxy includes signaling proxy and media proxy.

- Signaling proxy: The SE2900 parses, processes, and forwards H.248 signaling packets.
- Media proxy: The SE2900 processes and forwards audio and video streams.

Figure 4-20 shows H.248 proxy on the IMS network, and Figure 4-21 shows H.248 proxy on the NGN.

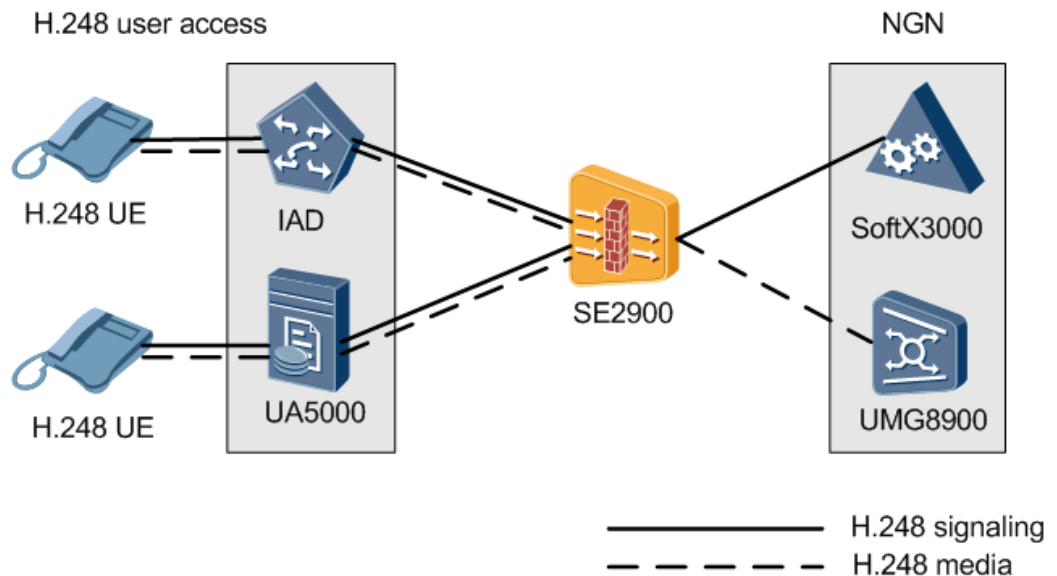
Figure 4-20 H.248 proxy on the IMS network



In the IMS networking as shown in Figure 4-20, H.248 UEs send signaling and media packets to the SE2900 through the H.248 gateway (IAD or UA5000).

- Acting as a signaling proxy, the SE2900 sends H.248 signaling packets to the UAC3000 on the IMS network.
- Acting as a media proxy, the SE2900 sends H.248 media packets to the IM-MGW on the IMS network.

Figure 4-21 H.248 proxy on the NGN



In the NGN networking as shown in Figure 4-21, H.248 UEs send signaling and media packets to the SE2900 through the H.248 gateway (IAD or UA5000).

- Acting as a signaling proxy, the SE2900 sends H.248 signaling packets to the SoftX3000 on the NGN.
- Acting as a media proxy, the SE2900 sends H.248 media packets to the UMG8900 on the NGN.

4.3 I-SBC Basic SW

4.3.1 SIP Call

The SIP call feature enables the SE2900 to create, modify, or terminate multi-media sessions and use SDP to dynamically modify session attributes, such as required session bandwidths, media types (voice, video, or data), and media codec formats.

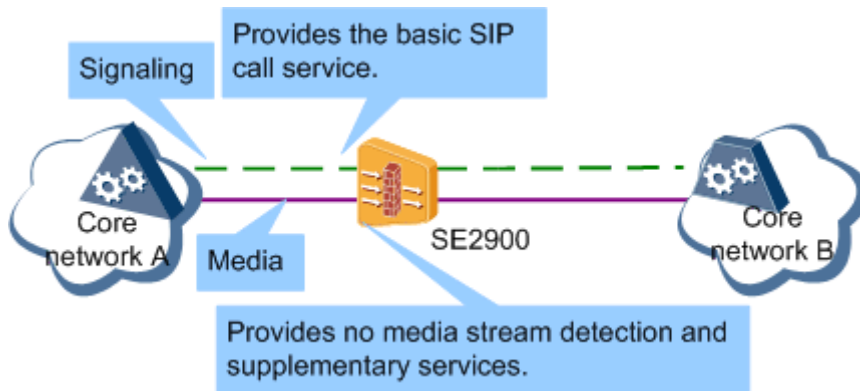


NOTE

A SIP call is a logical connection established between two nodes, over which audio or video data is transmitted. Nodes can be UEs or network devices.

In the I-SBC scenario, the SE2900 is deployed between two IMS networks or between one IMS network and another network and forwards call messages between the networks. See Figure 4-22.

Figure 4-22 SIP call



After core network A initiates a call, the SE2900 receives and processes the call request as a user agent server (UAS). The SE2900 also acts as a user agent client (UAC) and generates requests and sends them to core network B. Besides performing media negotiation to implement the basic call service, the SE2900 also supports no media stream detection and supplementary services.

- No media stream detection
No media stream detection enables the SE2900 to send a BYE message to a UE and a core server after detecting that no media stream is available in one direction or both directions of a session for a period that is longer than the maximum allowable period. The core server tears down the session immediately after receiving the BYE message, improving the accuracy of subscriber charging.
- Supplementary services

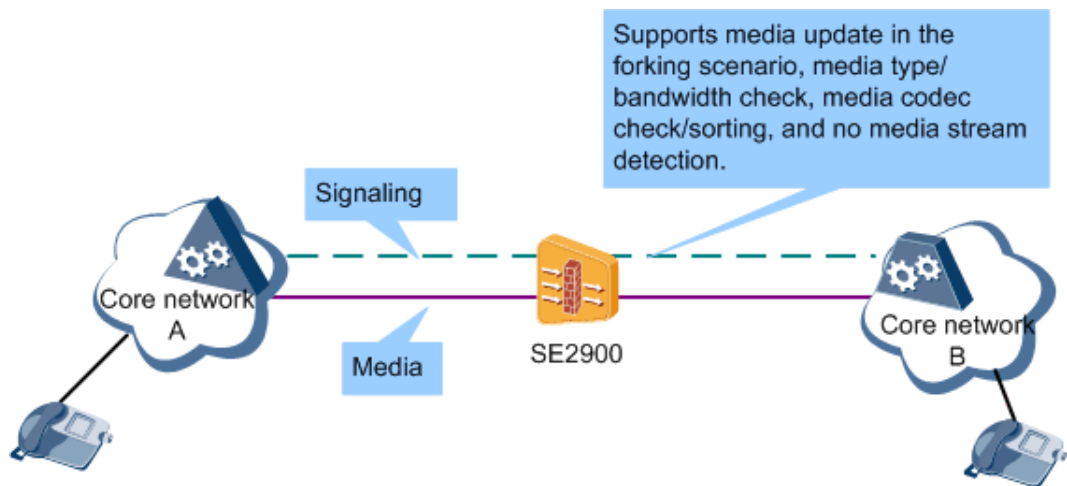
The SE2900 collaborates with the core server to implement supplementary services, including call hold, Forking, Forking Masquerading, call transfer, third-party calling, conference calling, and short message receipt.

4.3.2 Media Policy

The media policy feature enables the SE2900 to flexibly control media capabilities, such as the early media, media types, media codecs, and bandwidth. This feature enables different types of UEs to communicate using the same media type and codec. This feature enables carriers to implement flexible control on media capabilities over the network, thereby ensuring proper use of network resources.

The SE2900 controls media capabilities based on media policies in the I-SBC scenario. See Figure 4-23.

Figure 4-23 Media policy



In the I-SBC scenario, the media policy feature provides the following functions:

- Media update in the forking scenario: After receiving responses along multiple forking paths, the SE2900 performs bearer control over the early media transferred along these forking paths and upgrades the media based on the P-Early-Media header.
- Media type check and media bandwidth check
 - Media type check: The SE2900 restricts the types of media packets transferred over the network and blocks media packets of specific media types, such as video packets.
 - Media bandwidth check: The SE2900 restricts the bandwidth for each type of media packet and prevents UEs from overusing media bandwidth.
- Media codec check and media codec sorting
 - Media codec check: The SE2900 restricts the audio and video codecs that are allowed across the network.
 - Media codec sorting: The SE2900 sorts the media codecs in the SDP offer by priority, ensuring that high-priority media codecs are used in the communication between the caller and callee.
- No media stream detection: When the signaling plane is normal but the media plane is abnormal, the SE2900 sends a BYE message to the UE and the core server after

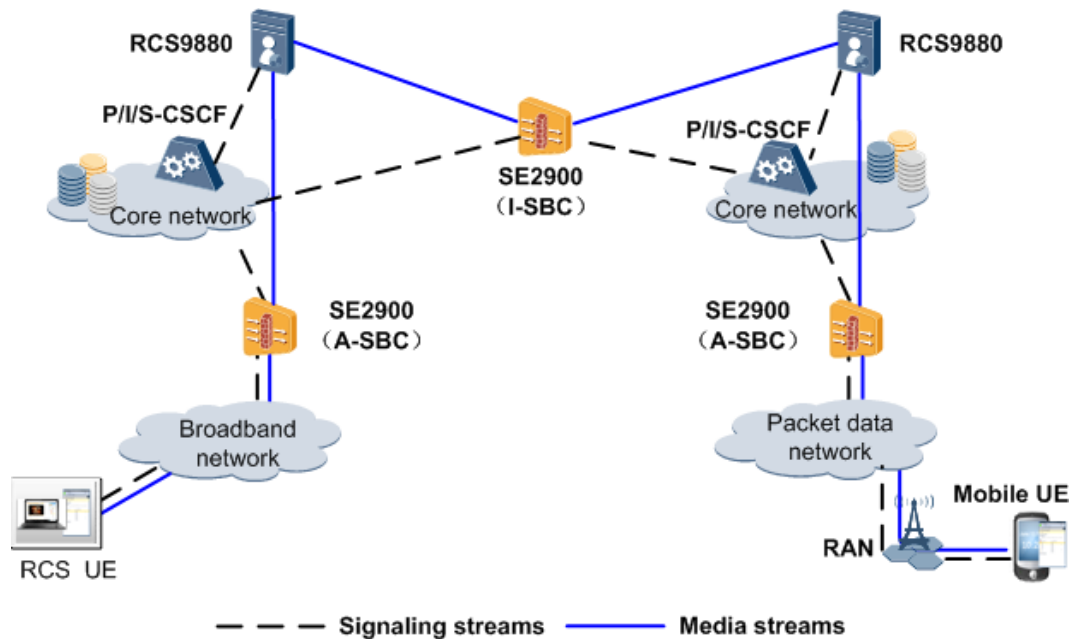
detecting no media streams within the specified period. Upon receipt of the BYE message, the core server tears down the session, improving the charging accuracy.

4.3.3 MSRP Proxy

MSRP is a session-based connection-oriented protocol used to exchange Multipurpose Internet Mail Extensions (MIME) content in any format, including binary content. MSRP establishes sessions using the SDP offer/answer model. During SIP session establishment, both parties negotiate MSRP uniform resource identifiers (URIs) and MSRP extensions. After SIP session establishment is complete, MSRP messages are transmitted on the media plane to exchange MIME contents. MSRP is an application layer protocol and runs over connection-oriented protocols such as TCP. An MSRP message can be a request or a response.

Rich Communication Suite (RCS) defines a variety of enhanced services, such as Message Session Relay Protocol-based (MSRP-based) picture sharing, file transmission, and chat services. The MSRP proxy feature enables the SE2900 to act as an MSRP session proxy and forward MSRP media streams between a UE and an AS or between UEs during RCS services. See Figure 4-24.

Figure 4-24 MSRP proxy



RCS services involve the following MSRP modes:

- AS mode: An MSRP session is established between a UE and the AS. This mode is used in chat and file transmission services.
- Point-to-point (P2P) mode: An MSRP session is established between an RCS UE and a UE of another type through the SE2900. This mode is used in the picture sharing service.

4.3.4 Address Overlapping

Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist on the SE2900, which is used to implement address overlapping. Packets are sent and received independently in each VRF instance. Routing instances are

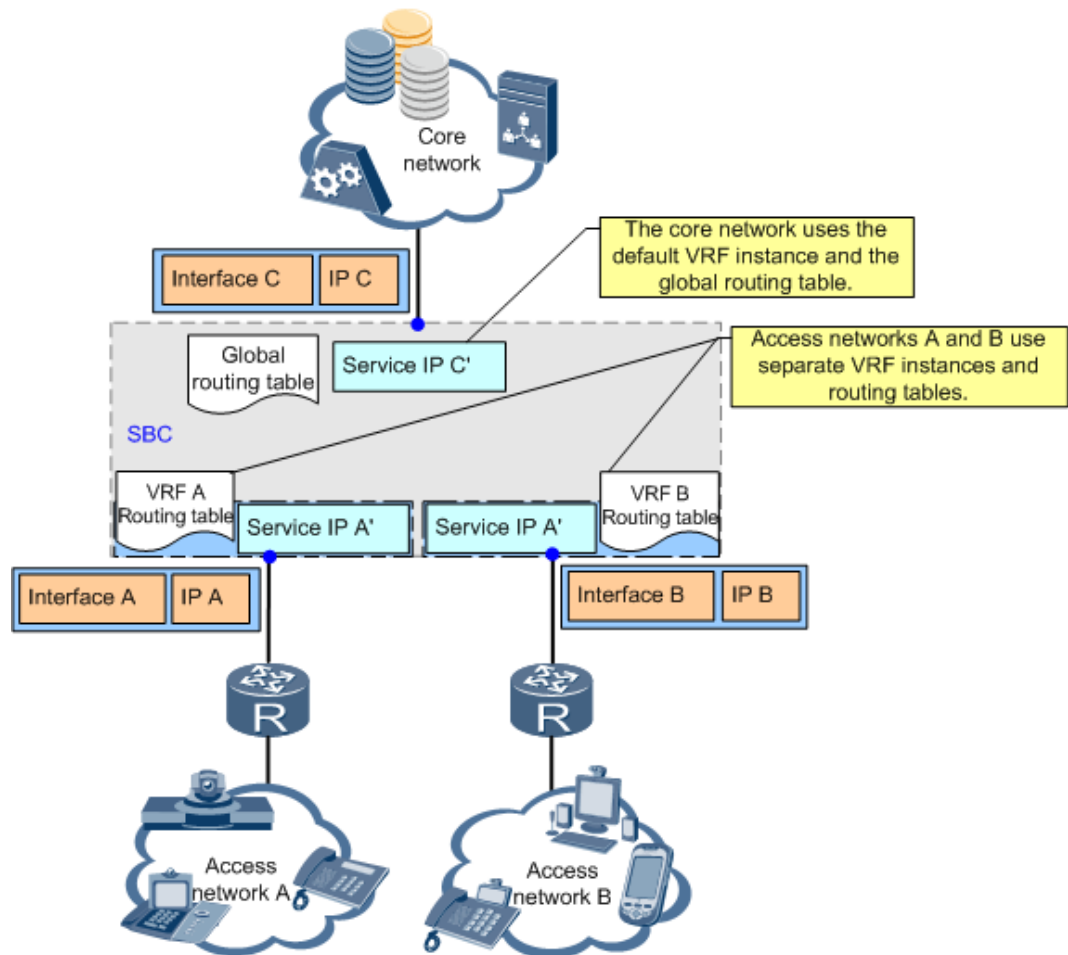
independent of each other, with their own routing entries, interfaces, and IP addresses. The overlapping IP addresses/segments can be used in different routing instances without conflicting with each other.

The SE2900 allows access network addresses to overlap with each other, core network addresses to overlap with each other, and access network addresses and core network addresses to overlap with each other. Address overlapping implements the sharing of IP addresses/segments and simplifies the service and application configurations on different access networks. Address overlapping saving the IP address, and much more compatible with live network.

Overlapping Between Access Network Addresses

Two access networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-25 shows the networking for overlapping between access network addresses.

Figure 4-25 Overlapping between access network addresses



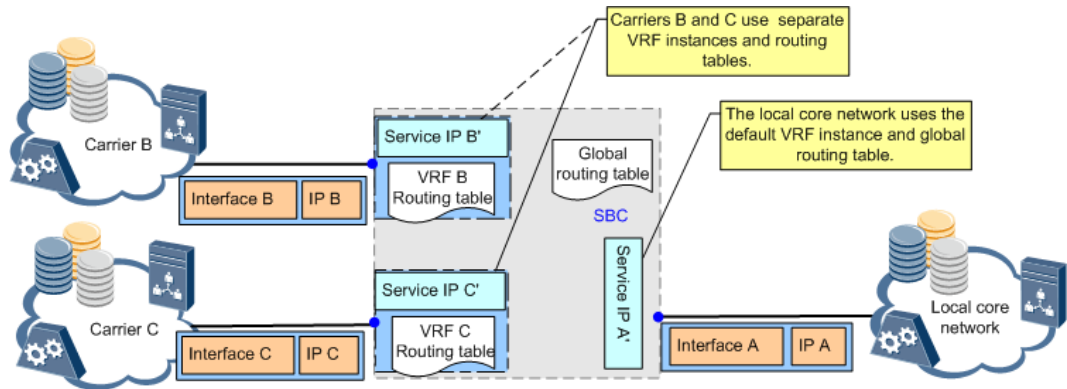
In Figure 4-25, access networks A and B connect to the SBC. Access network A is at 10.0.0.0/8, while access network B is at 10.2.0.0/16. The two network segments are overlapping. All the packets whose destination addresses belong to 10.2.0.0/16 are sent to access network B through interface B. The UEs at 10.2.0.0/16 on access network A cannot access services.

To address the issue, the SBC separates the two access networks to different VRF instances.

Overlapping Between Core Network Addresses

Two core networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-26 shows the networking for overlapping between core network addresses.

Figure 4-26 Overlapping between core network addresses



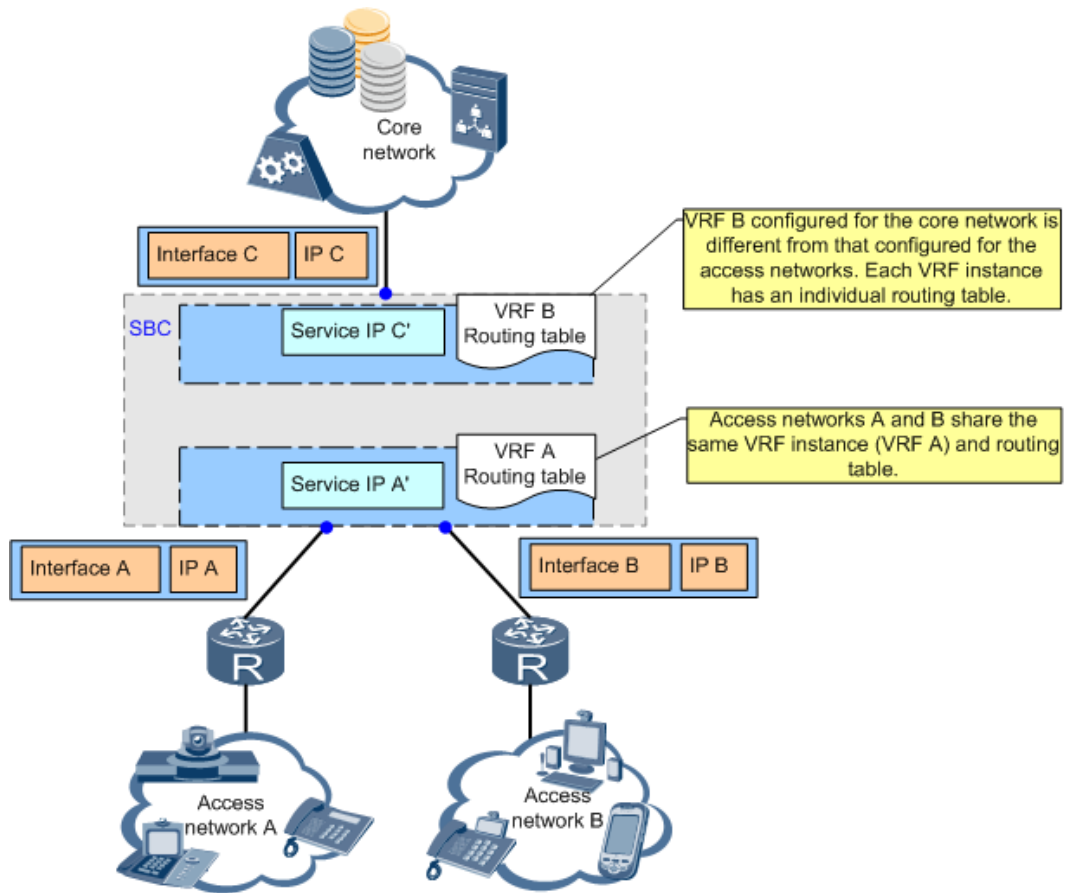
In Figure 4-26, the core network of carrier B is at 11.0.0.0/8, where the core network of carrier C is at 11.0.0.0/16. The two network segments are overlapping.

The SBC separates the two core networks to different VRF instances so that the UEs on access networks can access services.

Overlapping Between Access Network Addresses and Core Network Addresses

Access networks and core networks with overlapping IP addresses/segments connect to the same SE2900. Figure 4-27 shows the networking for overlapping between access network addresses and core network addresses.

Figure 4-27 Overlapping between access network addresses and core network addresses



In Figure 4-27, access networks A and B are at 10.0.0.0/8, where the core network is at 10.0.0.0/8. The two network segments are overlapping. The UEs on access networks A and B cannot access services.

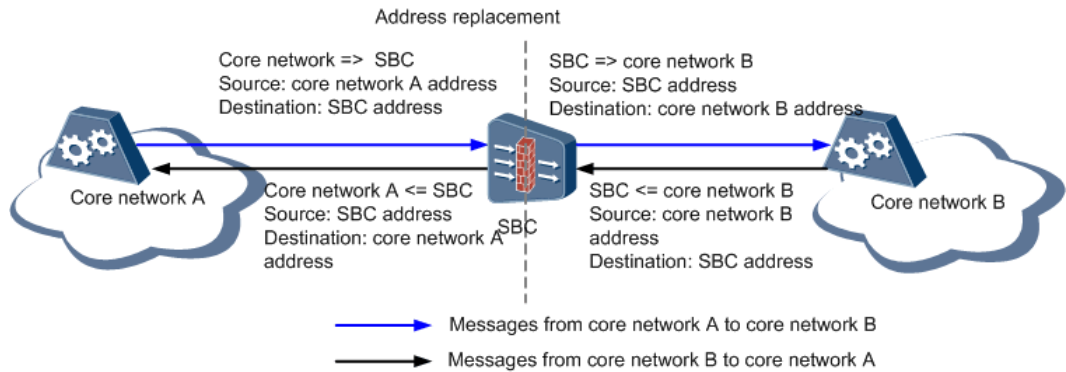
To address the issue, the SBC separates the access networks and the core network to different VRF instances.

4.3.5 Topology Hiding

Network topology may be exposed because of routing information carried in SIP messages during SIP calls. Attackers may probe the network structure by obtaining network topology carried in SIP messages.

When deployed between two networks, the SE2900 hides the topology of each network from the other. The SE2900 implements topology hiding by changing the source IP address to the SE2900's address during message processing at the IP, transport, and signaling layers, enhancing network security. See Figure 4-28.

Figure 4-28 Topology hiding



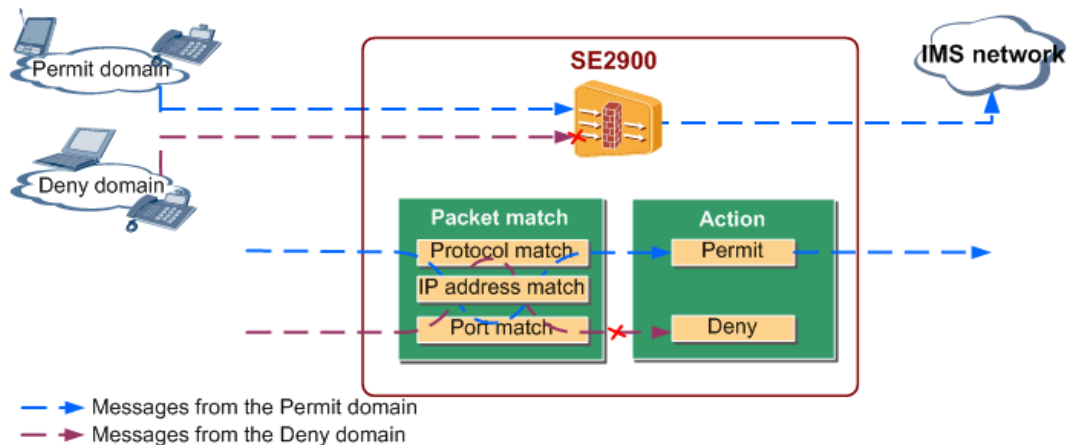
4.3.6 IP Layer Security

ACL-based Packet Filtering

An ACL defines rules that are used to filter IP packets. The SE2900 matches IP packets with the rules and discards the packets (for example, call packets initiated by unauthorized users) that do not conform to the rules.

After receiving a packet, the SE2900 performs ACL-based filtering first. The SE2900 performs subsequent operations only on conforming packets. This processing protects closed ports and services against attacks. Figure 4-29 shows the ACL-based packet filtering mechanism.

Figure 4-29 ACL-based packet filtering



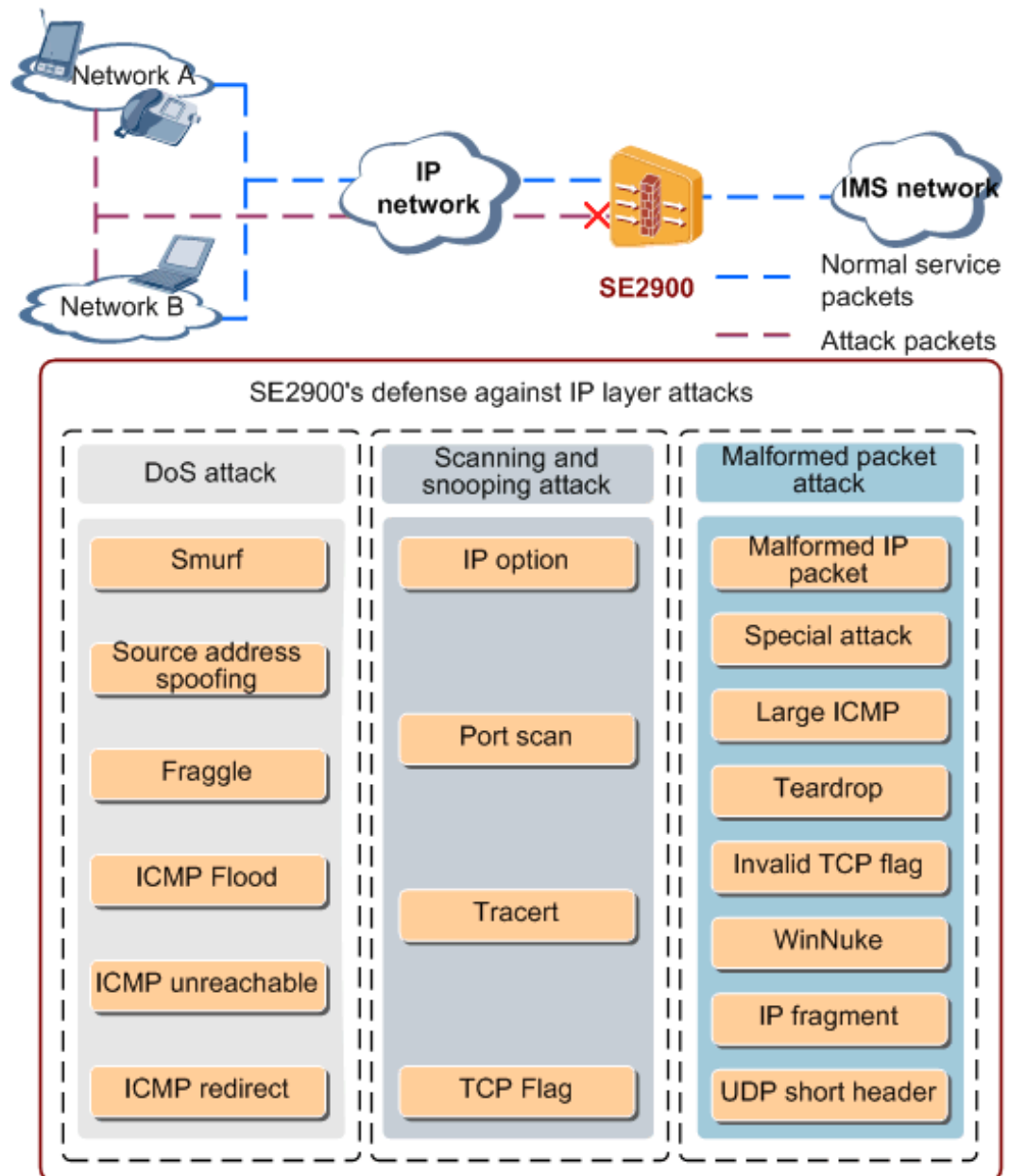
The SE2900 supports standard and advanced ACL groups.

- The standard ACL group contains basic ACL rules, which are defined based on the source IP address.
- The advanced ACL group contains advanced ACL rules, which are defined based on the source address + port, destination address + port, and protocol type. Advanced ACLs allow for more accurate, diversified, and flexible rules.

DoS/DDoS Attack Defense

Nowadays, most networks adopt the all-IP architecture and use SIP as the session control mechanism. All signaling messages and media messages are carried in IP packets. An attacker can launch an IP layer attack by sending a large number of IP packets to the target host, exhausting the host's resources; or by sending malformed IP packets to the target host, causing the host that processes the malformed packets to break down. The SE2900 identifies, classifies, and filters out IP attack packets at the edge of the core network. Figure 4-30 shows the DoS/DDoS attack defense mechanism.

Figure 4-30 DoS/DDoS attack defense



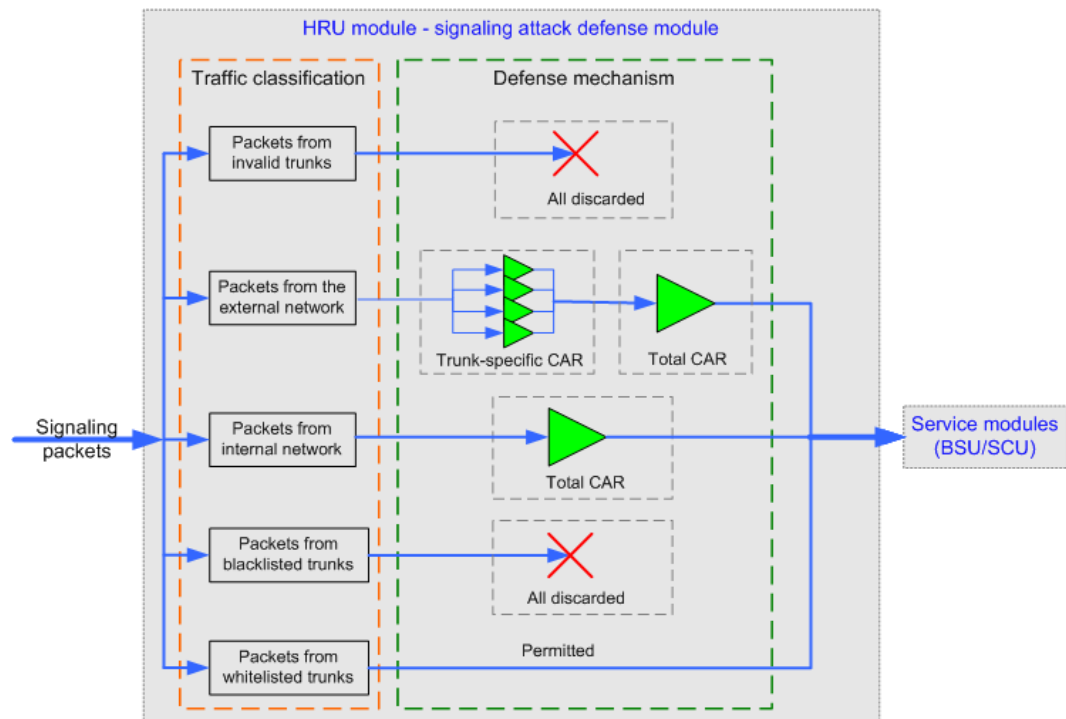
After identifying attack packets, the SE2900 discards them and counts the number of attack packets. When the number of attack packets reaches a specified threshold, the SE2900 generates an IP layer attack defense alarm.

4.3.7 Signaling Plane Security

DoS/DDoS attacks are the major threats to the signaling plane. In a DoS/DDoS attack, an attacker sends a large number of data packets to the target host to exhaust system resources, causing the host unable to process valid requests from legitimate users. DoS attacks are launched by a single attacker, whereas DDoS attacks are launched by multiple attackers. In most cases, an attacker launches a DoS/DDoS attack by sending huge numbers of packets to a well-known port, such as the SIP well-known port 5060, attempting to exhaust the system resources. An attacker may also take advantage of system vulnerabilities and send attack packets to cause system exceptions, such as memory overwriting, memory leak, and call stack overflow/reset.

The signaling attack defense module on the SE2900 performs strict flow control over received SIP messages. Different flow control policies can be applied to packets from different users. Figure 4-31 shows the DoS/DDoS attack defense mechanism.

Figure 4-31 DoS/DDoS attack defense



- Packets from an unauthorized trunk group: The SE2900 searches for a SIP trunk group based on the source IP address, virtual routing and forwarding (VRF) instance ID, and destination IP address + port of the received signaling packet. If no trunk group matches the signaling packet, the SE2900 discards the signaling packet and increments the statistics by source IP address.
- Packets from a trunk group in the external domain: The SE2900 calculates the average packet rate and processes the packets according to the relationship between the average packet rate and committed access rate (CAR) threshold.

- If the average packet rate is less than the CAR threshold, the SE2900 parses and forwards the packets.
- If the average packet rate is between the CAR threshold and the blacklist threshold, the SE2900 discards only the initial packet.
- If the average packet rate is greater than the blacklist threshold, the SE2900 blacklists the trunk group that sends the packets so that physical interfaces on the SE2900 are used to discard subsequent packets.
- Packets from the internal domain: The SE2900 restricts the overall rate of received packets.
- Packets from blacklisted users: The SE2900 discards all the packets.
- Packets from whitelisted users: The SE2900 does not perform flow control over the packets.

4.3.8 Media Plane Security

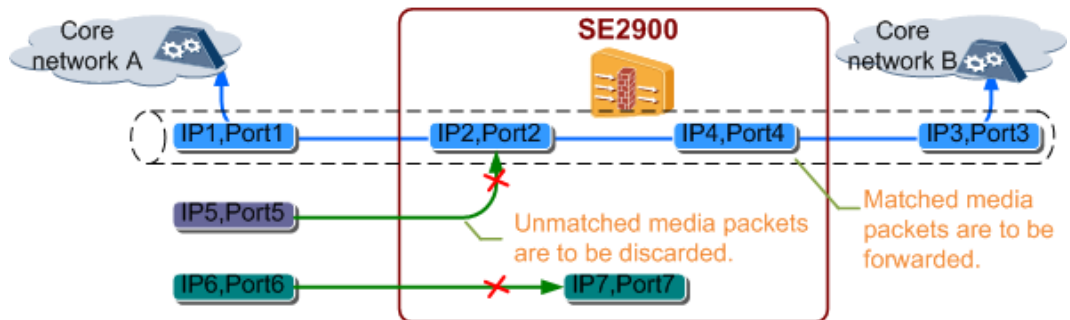
The dynamic pinholing firewall feature enables the SE2900 to dynamically create media session entries (IP 5-tuple) based on signaling negotiation results. Figure 4-32 shows the media pinholing firewall mechanism.



NOTE

IP 5-tuple consists of the source IP address, source port number, destination IP address, destination port number, and protocol in use.

Figure 4-32 Media pinholing firewall

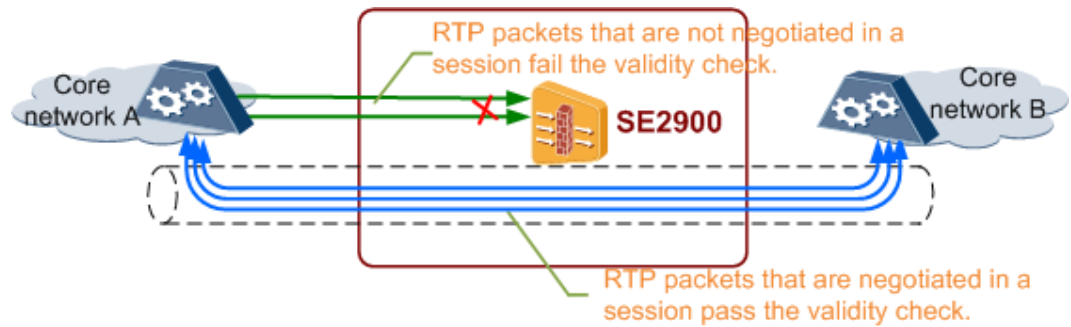


- After receiving media packets in a call procedure, the SE2900 extracts 5-tuple information. The SE2900 matches the 5-tuple information against media session entries and only forwards media packets with matching media session entries.
- When the call is over, the SE2900 deletes the media session entries of the call after receiving a BYE message.

An attacker can send a huge number of RTP packets to attack the SE2900 or its peer media device. The SE2900 performs validity checks on RTP packets to implement malformed RTP packet attack defense.

After a Real-Time Transport Protocol (RTP) packet passes through the media pinholing firewall, the SE2900 checks the version number and payload type of the RTP packet header. If the version number of an RTP packet is not 2 or the payload type of the RTP packet header is different from the payload type negotiated in the session, the RTP packet fails the validity check. The SE2900 then considers the RTP packet to be an attack packet and discards it. Figure 4-33 shows the malformed RTP packet attack defense mechanism.

Figure 4-33 Malformed RTP packet attack defense

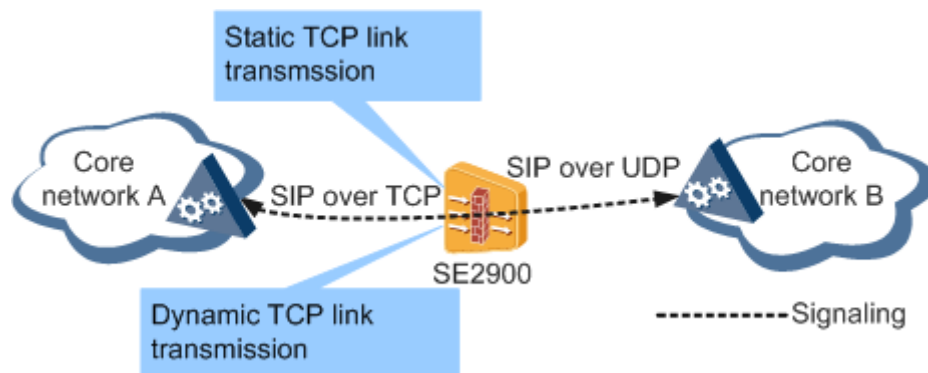


4.3.9 SIP over TCP

TCP is connection-oriented and provides reliable data transmission. TCP achieves reliable end-to-end transmission using a series of measures, including retransmission, duplicate data discarding, checksums, and traffic control.

In the I-SBC scenario, the SE2900 supports interworking between SIP over TCP and SIP over UDP, and transmits SIP messages over static or dynamic TCP links. When SIP messages are transmitted over dynamic TCP links, the SE2900 supports dynamic conversion between SIP over TCP and SIP over UDP. If the SIP message length is greater than or equal to the MTU value (1300 bytes by default), a TCP link is established, and SIP messages are switched to the TCP link for transmission. If the SIP message length is less than the MTU value, the SE2900 sends the SIP messages using the transport protocol specified in the initial INVITE message. See Figure 4-34.

Figure 4-34 SIP over TCP



The SE2900 supports the processing of SIP messages over TCP and UDP.

- Before forwarding a message from core network A to core network B, the SE2900 changes the transport-layer protocol from TCP to UDP.
- Before forwarding a message from core network B to core network A, the SE2900 changes the transport-layer protocol from UDP to TCP.

The SE2900 transmits SIP messages over static or dynamic TCP links during interworking between SIP over TCP and SIP over UDP.

- SIP transmission over static TCP links: One static TCP link can bear multiple SIP calls.

The SE2900 establishes a TCP link based on the local TCP link configuration specified by **ADD SIPSLNK**.

Acting as a TCP client, the SE2900 uses the specified address + port to initiate a link establishment request and completes the TCP link establishment. Subsequent SIP messages between the SE2900 and core network A are all transmitted over the TCP link.

- SIP transmission over dynamic TCP links: One dynamic TCP link can bear only one SIP call.

Core network B initiates a SIP call. The SE2900 decides on an IBCF SIP trunk group based on a routing policy. Then the SE2900 selects TCP as the transport-layer protocol based on the bearer protocol specified by **Link information** in **ADD ISIPTG** and establishes a TCP link.

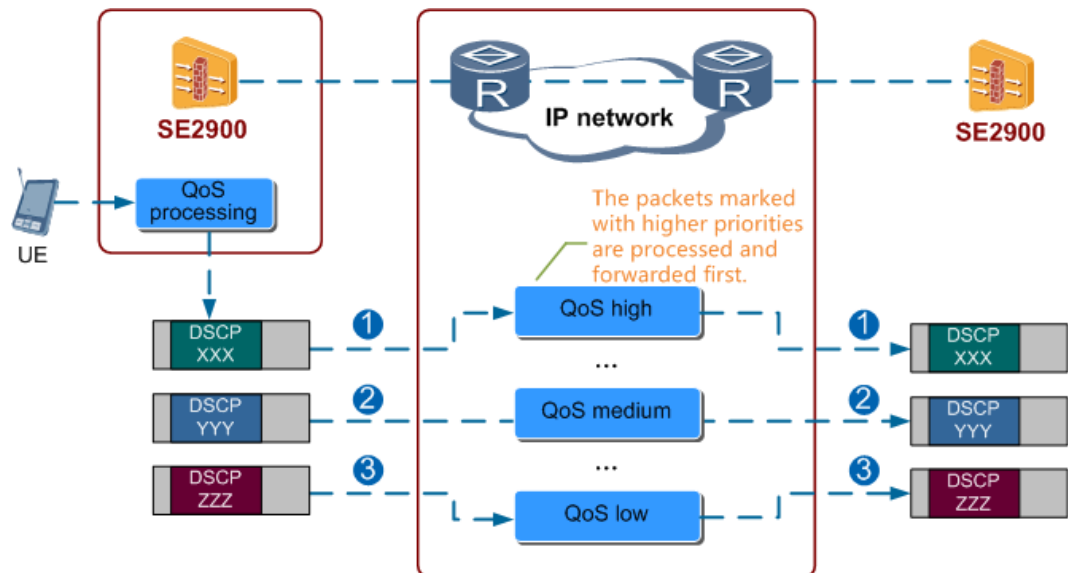
Acting as a TCP client, the SE2900 uses the local address, peer address, and peer port configured for the IBCF SIP trunk group to initiate a link establishment request and completes the TCP link establishment. Subsequent SIP messages between the SE2900 and core network B are all transmitted over the TCP link.

4.3.10 DSCP Remark

DSCP remarking: The SE2900 assigns different DSCP values to signaling and media packets. After receiving data packets, a router preferentially forwards packets with higher DSCP priorities to ensure QoS on the voice over Internet Protocol (VoIP) network.

DSCP remarking enables carriers to prioritize the services of high-priority subscribers by allocating resources and implementing charging based on the service priorities of subscribers stored on the HSS. Figure 4-35 shows DSCP remarking.

Figure 4-35 DSCP remarking



DSCP remarking can be performed on both signaling packets and media packets.

- DSCP remarking for signaling packets: **ADD IADDR** can be used to set DSCP values for SIP signaling packets. When sending a SIP signaling packet, the SE2900 searches for a corresponding DSCP value based on the source IP address of the SIP signaling packet.

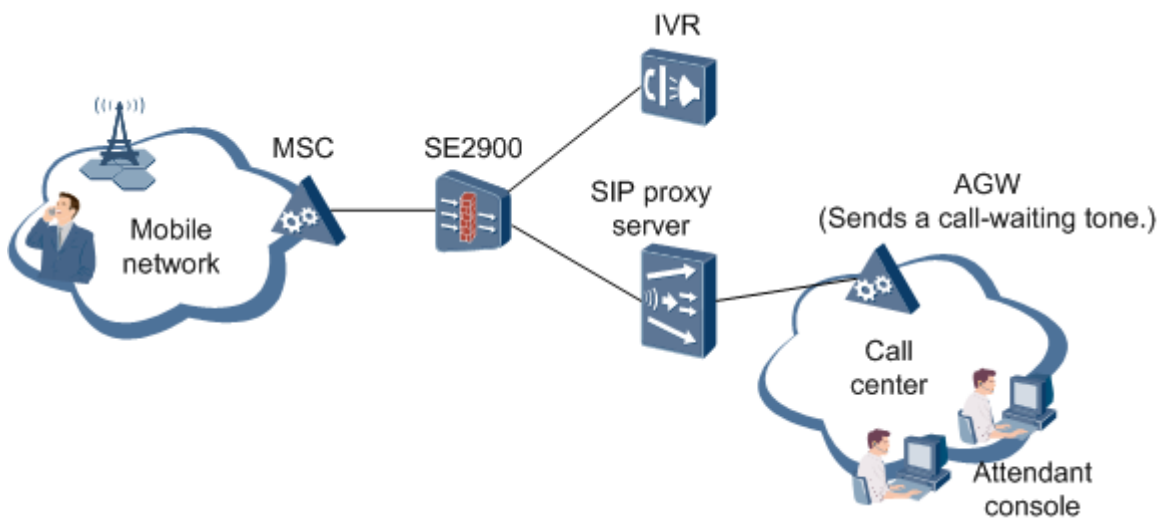
- DSCP remarking for media packets: The SE2900 supports core-network-specific DSCP values for various media types. When an IBCF record is added, the system automatically adds the default media QoS record that corresponds to the IBCF to the IBCF default QoS information table.

4.3.11 REFER Proxy

This feature enables the SE2900 to refer a call to the call center based on the REFER message received from the interactive voice response (IVR).

The REFER proxy feature applies to the I-SBC scenario. Figure 4-36 shows the typical REFER proxy networking.

Figure 4-36 Typical REFER proxy networking



The service procedure is as follows:

1. A user dials an IVR number.
2. After the call is connected, the user selects the attendant service based on the voice prompt sent by the IVR.
3. The SIP proxy server selects an attendant.
 - If no attendant is available, the SIP proxy server instructs the announcement gateway (AGW) to send a call-waiting tone to the UE.
 - If an attendant is available, the SIP proxy server connects the call between the UE and attendant.

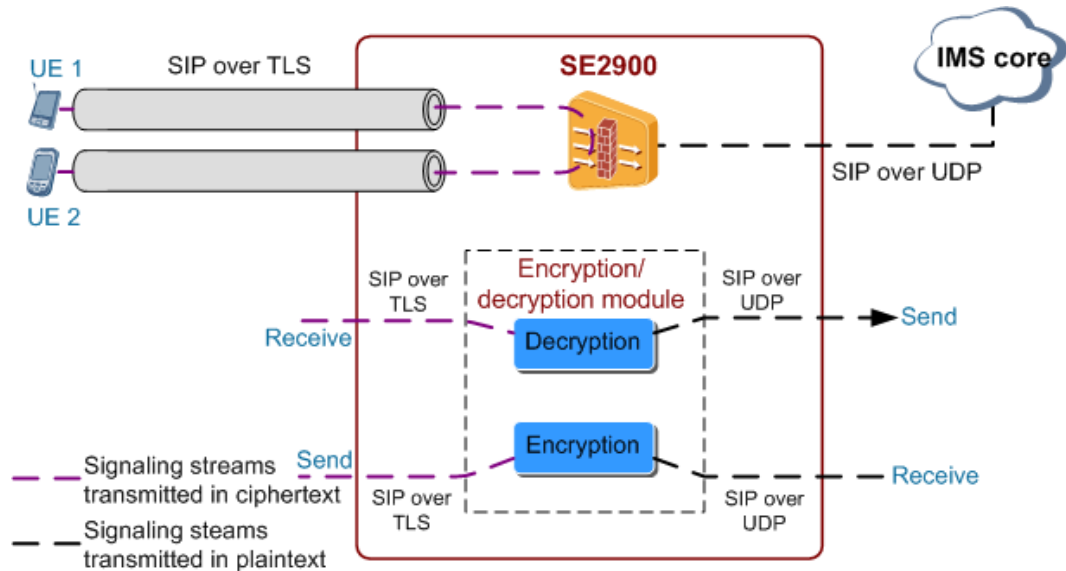
4.4 Optional Features

4.4.1 SIP over TLS

SIP over Transport Layer Security (TLS) enables the SE2900 to use TLS to encrypt SIP signaling messages between UEs and the SE2900 in the A-SBC scenario. SIP over TLS prevents SIP signaling packets from being tampered with and intercepted and protects the

SE2900 against forged SIP packet attacks. Figure 4-37 shows the networking for SIP over TLS.

Figure 4-37 SIP over TLS



- Upon receiving a SIP message from a UE, the SE2900 performs decryption and changes TCP to UDP. Then the SE2900 sends the SIP message to the core network.
- Upon receiving a SIP message from the core network, the SE2900 performs encryption and changes UDP to TCP. Then the SE2900 sends the SIP message to the UE.

TLS is an IETF-defined protocol intended to provide communications security at the transport layer. Based on TCP, TLS uses certificate validation, key negotiation, and data encryption to implement secure connections between two devices and encrypt the sessions between them. TLS is independent of protocols at the application layer and can work with various application protocols, for example, HTTP and SIP.

In the A-SBC scenario, the SE2900 uses SIP over TLS to encrypt SIP signaling messages and uses SRTP to encrypt SIP media messages, between UEs and the SE2900.

4.4.2 MSRP over TLS

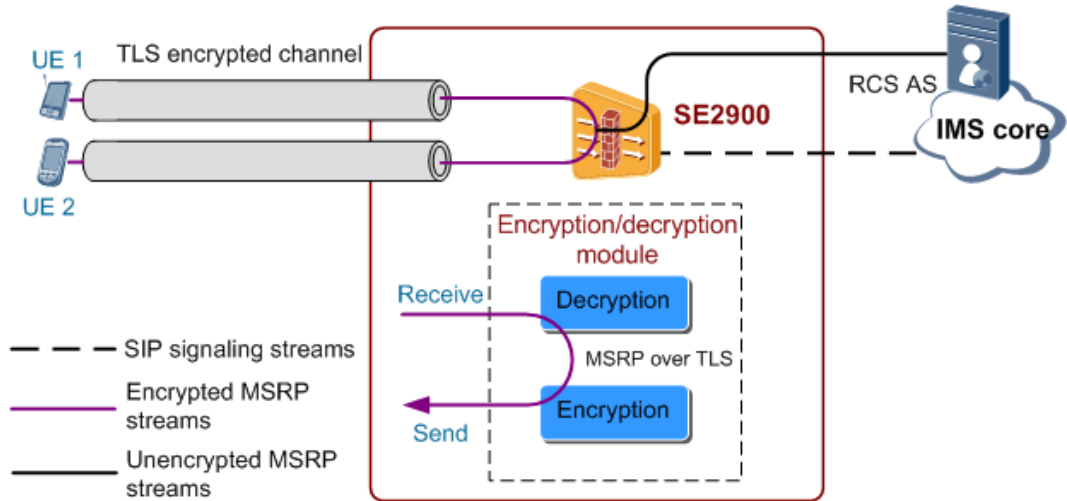
MSRP is a session-based connection-oriented protocol used to exchange Multipurpose Internet Mail Extensions (MIME) content in any format, including binary content. MSRP establishes sessions using the SDP offer/answer model. During SIP session establishment, both parties negotiate MSRP uniform resource identifiers (URIs) and MSRP extensions. After SIP session establishment is complete, MSRP messages are transmitted on the media plane to exchange MIME contents. MSRP is an application layer protocol and runs over connection-oriented protocols such as TCP. An MSRP message can be a request or a response.

TLS is an IETF-defined protocol intended to provide communications security at the transport layer. Based on TCP, TLS uses certificate validation, key negotiation, and data encryption to implement secure connections between two devices and encrypt the sessions between them.

Rich Communication Suite (RCS) defines Message Session Relay Protocol-based (MSRP-based) picture sharing, file transmission, and chat services. The SE2900 acts as an MSRP session proxy and forwards MSRP media streams between a UE and an application

server (AS) or between UEs. MSRP over TLS enables the SE2900 to use TLS to transmit MSRP data streams between UEs and the SE2900, which ensures communication data security. Figure 4-38 shows the networking for MSRP over TLS.

Figure 4-38 MSRP over TLS



RCS services use the following MSRP modes:

- AS mode: An MSRP session is established between a UE and the AS. This mode is used in chat and file transmission services.
- Point-to-point mode: An MSRP session is established between two UEs. This mode is used in the picture sharing service.

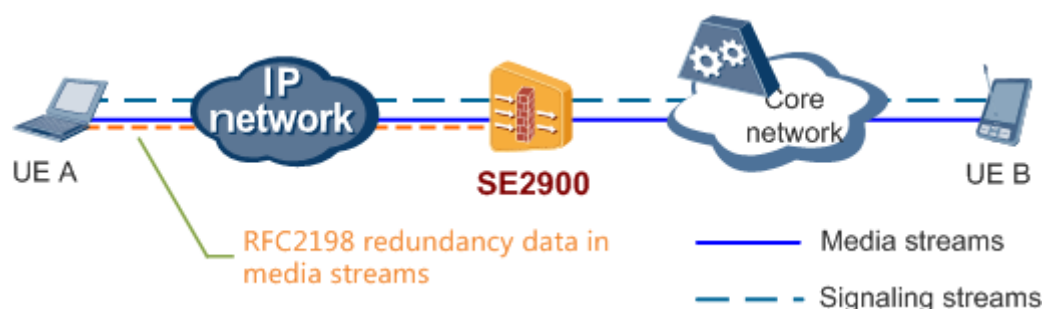
The SBC uses MSRP over TLS in AS mode or point-to-point mode to ensure enhanced data security in picture sharing, file transmission, and chat services.

4.4.3 RFC2198 Redundancy

RFC2198 redundancy: The SE2900 uses RFC2198 redundant packets to compensate for packet loss on the access side and improves audio transmission quality when forwarding media packets between the caller and callee.

RFC2198 redundancy compensates for packet loss on the IP network and ensures reliable audio transmission. This feature is used when soft clients access the SBC over the Internet. RFC2198 redundant transmission of media packets is implemented between the SBC and soft clients to compensate for packet loss on the IP network and ensure call quality for soft clients. Figure 4-39 shows the RFC2198 redundancy networking.

Figure 4-39 RFC2198 redundancy



The audio codecs of the supported audio packets in RFC2198 redundancy are as follows:

- On the fixed-line phone network: G.711 (including G.711 a-law and G.711 μ -law), G.722, G.723, G.726, G.728, G.729, and G.729E
- On the mobile network: GSM (including EFR, FR, and HR), AMR, AMR-WB, AMR-WB+, Q8, Q13, EVRC, and 4GV-NB
- On the Internet: iLBC

4.4.4 Media Bypass

Media bypass includes:

- Media bypass: enables media streams in the 4.2.1 SIP Call service to be transmitted between UEs without passing through the SE2900.
- Optimal media routing (OMR): enables media streams in the SIP call service to be transmitted between VoLTE UEs (at least one is the roaming UE) without passing through the devices along the path between a visited public land mobile network (VPLMN) and a home public land mobile network (HPLMN).

Basic Media Bypass (Referred to as Media Bypass)

If the SE2900 serves as a proxy for all media streams, media streams consume a lot of network bandwidth, especially in video applications. Therefore, media bypass is required in some scenarios to reduce the bandwidth consumed by media streams. Media bypass enables media streams to be transmitted between UEs without passing through the SE2900.

- In the A-SBC scenario, media bypass has four modes: automatic media bypass, intra-AN automatic media bypass, forced media bypass, and same-IP automatic media bypass.
- In the I-SBC scenario, media bypass has two modes: automatic media bypass and forced media bypass.

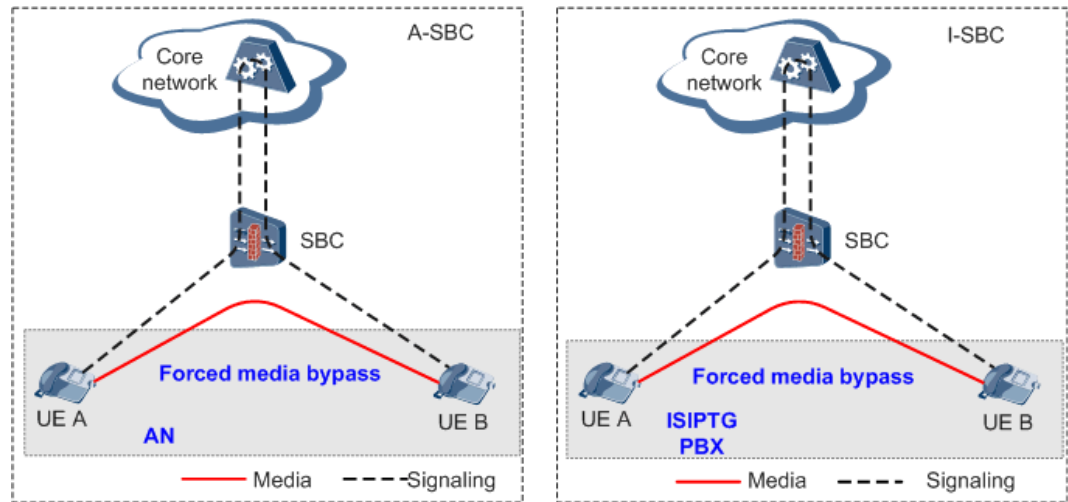
When media bypass is implemented on the IMS network, such as in the VoBB solution, an appropriate media bypass mode can be selected based on live network conditions. Media bypass saves bandwidth, improves the SE2900's performance, and reduces operating expenditure. Media bypass also shortens media stream transmission delay and improves call quality.

Forced Media Bypass

If forced media bypass is enabled, the SE2900 processes signaling packets only and does not process SDP information. All media-related services cease to be effective. Therefore, forced

media bypass applies only to networks on which the SE2900 processes only signaling packets. See Figure 4-40.

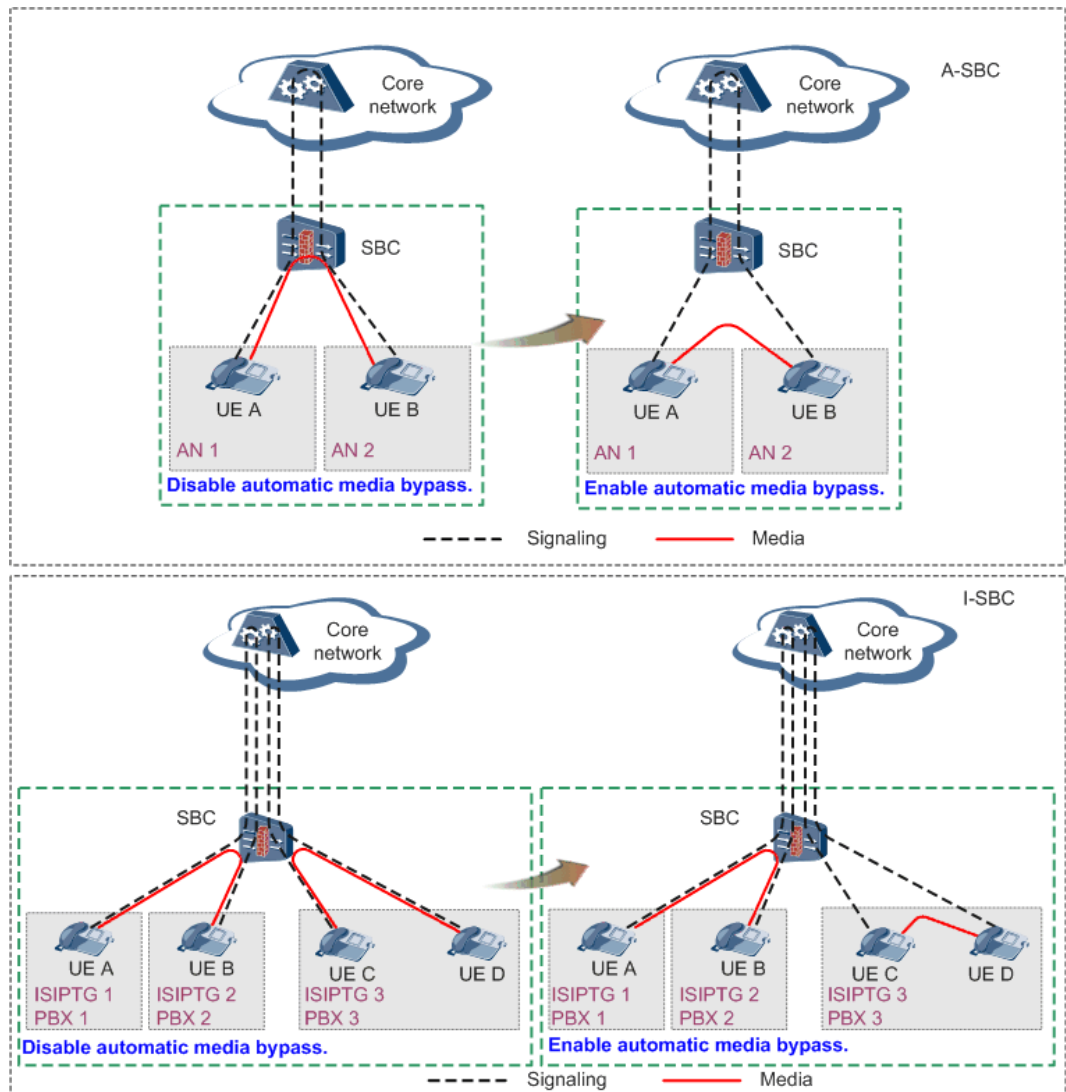
Figure 4-40 Forced media bypass



Automatic Media Bypass

When the caller and callee are connected to the same SE2900 and SDP negotiation is performed to set up a session between the caller and callee, the SE2900 determines whether to perform media bypass between the caller and callee based on the network conditions and service requirements. If the caller and callee cannot communicate with each other without the proxy of the SE2900 or the SE2900 needs to process media-related services, automatic media bypass is not performed so as to guarantee proper call service. See Figure 4-41.

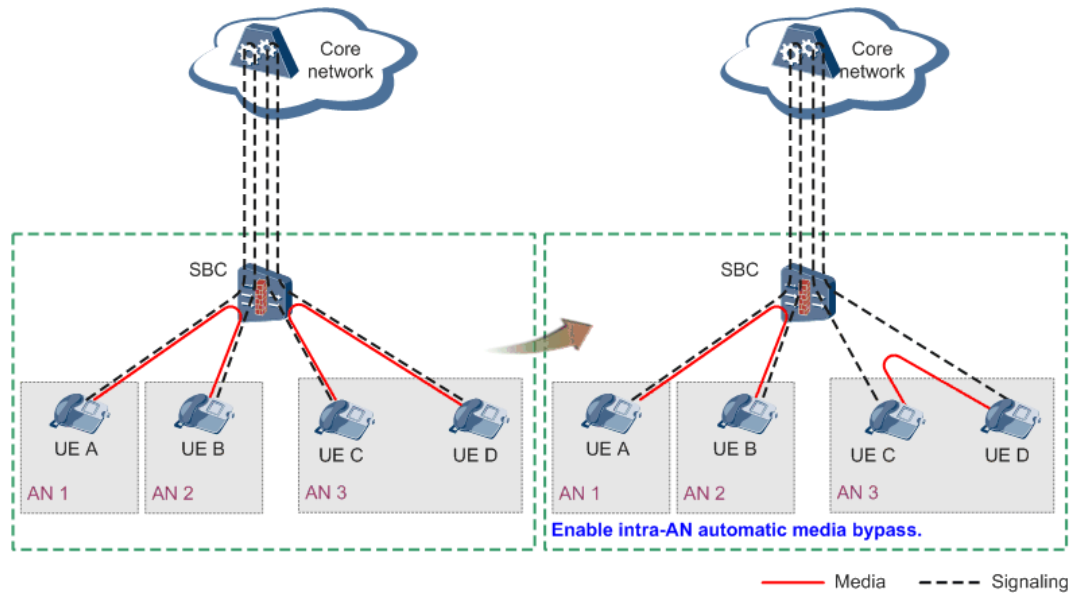
Figure 4-41 Automatic media bypass



Intra-AN Automatic Media Bypass

Intra-AN automatic media bypass is similar to automatic media bypass. The difference is that in intra-AN automatic media bypass, the calling UE and called UE between which media bypass is performed must be in the same AN. See Figure 4-42.

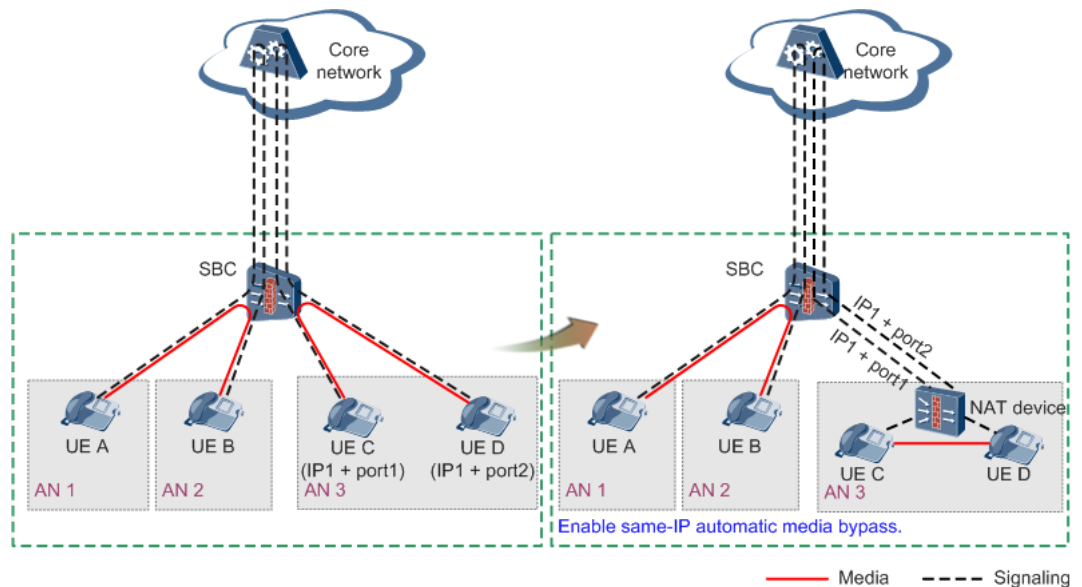
Figure 4-42 Intra-AN automatic media bypass



Same-IP Automatic Media Bypass

Same-IP automatic media bypass is similar to automatic media bypass. The difference is that in same-IP automatic media bypass, the calling UE and called UE between which media bypass is performed must use the same IP address.

Figure 4-43 Same-IP automatic media bypass



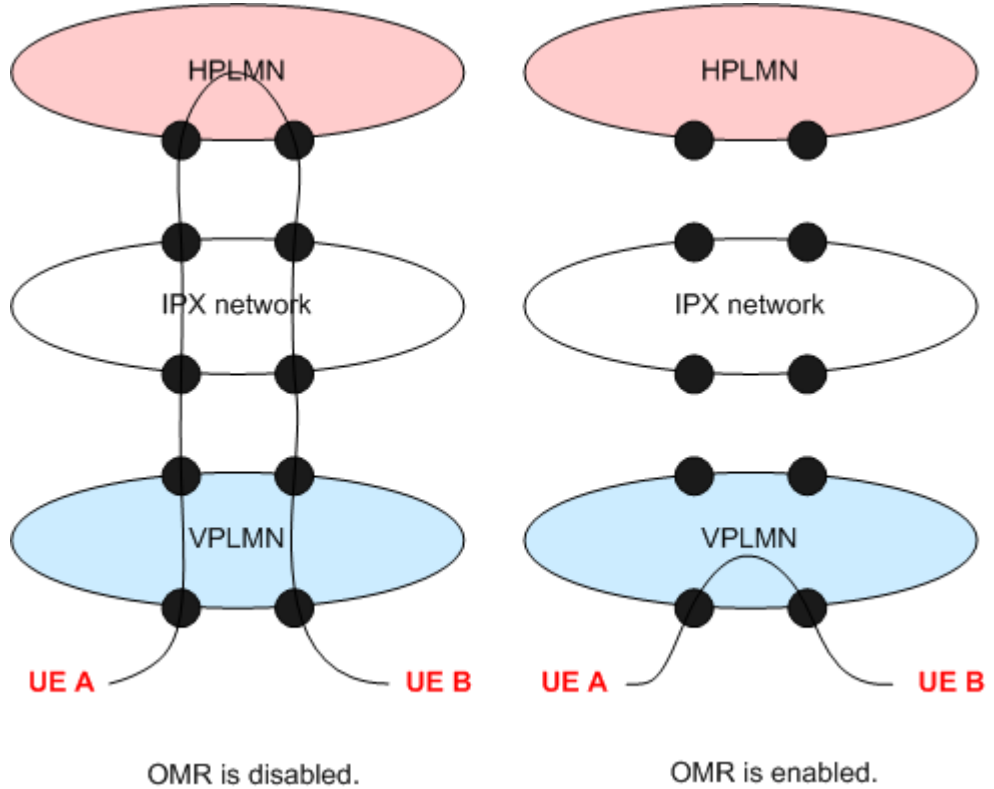
OMR

Four typical application scenarios are as follows:

- Scenario 1:

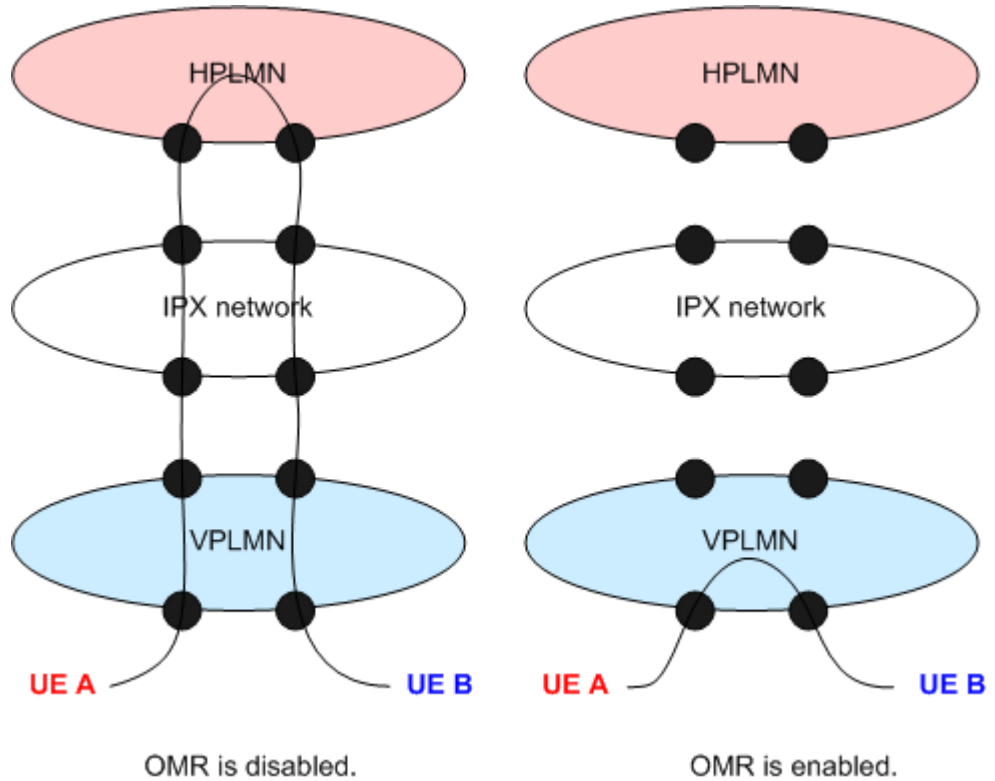
- UEs A and B belong to the HPLMN.
- UEs A and UE B roam to the VPLMN.
- UE A calls UE B.

The following figure shows media stream routing when OMR is enabled and disabled.



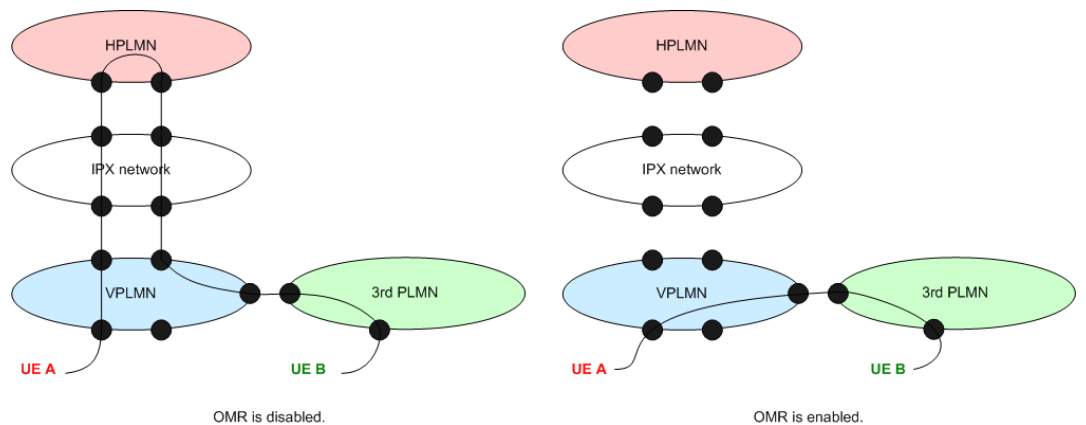
- Scenario 2:
 - UE A belongs to the HPLMN.
 - UE A roams to the VPLMN.
 - UE B belongs to the VPLMN.
 - UE A calls UE B.

The following figure shows media stream routing when OMR is enabled and disabled.



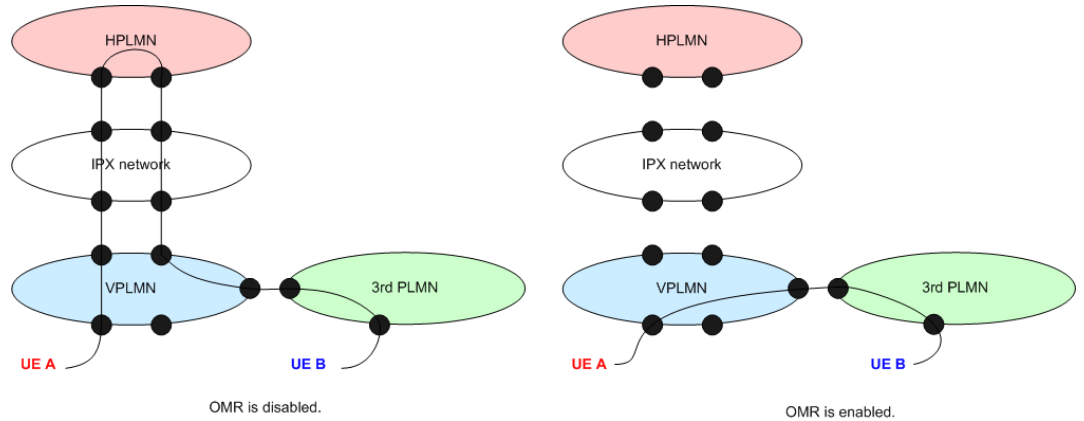
- Scenario 3:
 - UE A belongs to the HPLMN.
 - UE A roams to the VPLMN.
 - UE B belongs to the 3rd PLMN, which is close to the VPLMN.
 - UE A calls UE B.

The following figure shows media stream routing when OMR is enabled and disabled.



- Scenario 4:
 - UE A belongs to the HPLMN.
 - UE A roams to the VPLMN.
 - UE B belongs to the VPLMN.
 - UE B roams to the 3rd PLMN, which is close to the VPLMN.
 - UE A calls UE B.

The following figure shows media stream routing when OMR is enabled and disabled.



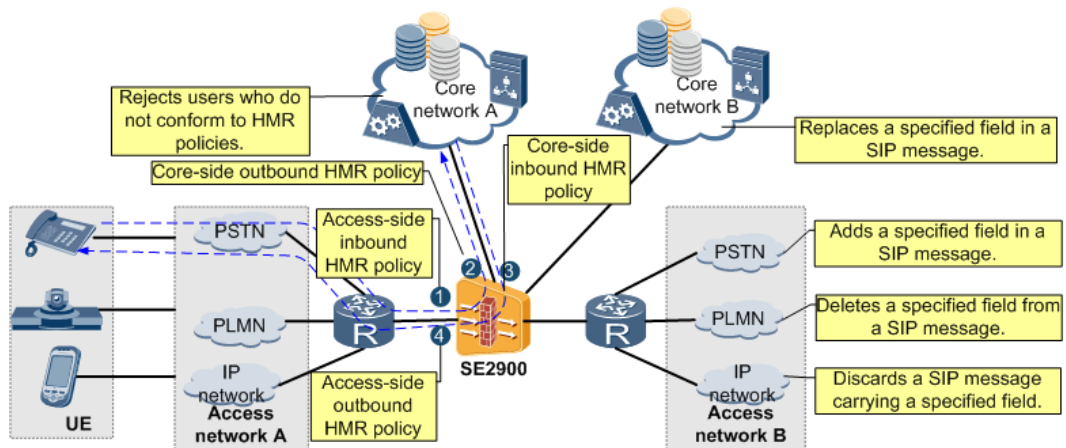
4.4.5 SIP Header Manipulation

SIP header manipulation is a feature in which the SE2900 performs insert, discard, reject, delete, replace, or save actions on matched first lines, headers, or message bodies in SIP messages based on the regular expression match result.

NOTE

A regular expression is a formula for matching character strings that have a certain pattern. It is used to express a type of filtering logic for character strings.

Figure 4-44 SIP header manipulation



SIP header manipulation provides a mechanism to flexibly control SIP messages and enables a network to have better SIP application-layer attack defense capability. Furthermore, this mechanism helps quickly solve interworking problems related to protocol use. The SE2900 can perform SIP header manipulation using user-defined mechanisms:

- **Rule:** A user-defined rule consists of match conditions and a manipulation action. The SE2900 uses the match conditions to perform regular expression matching for SIP messages and performs manipulation actions on matching SIP messages.
- **Policy:** User-defined policies include SIP request HMR policies and SIP response HMR policies. After receiving a SIP message, the SE2900 determines whether it is a request or response and executes the rules by priority in the corresponding SIP request HMR policy or SIP response HMR policy.

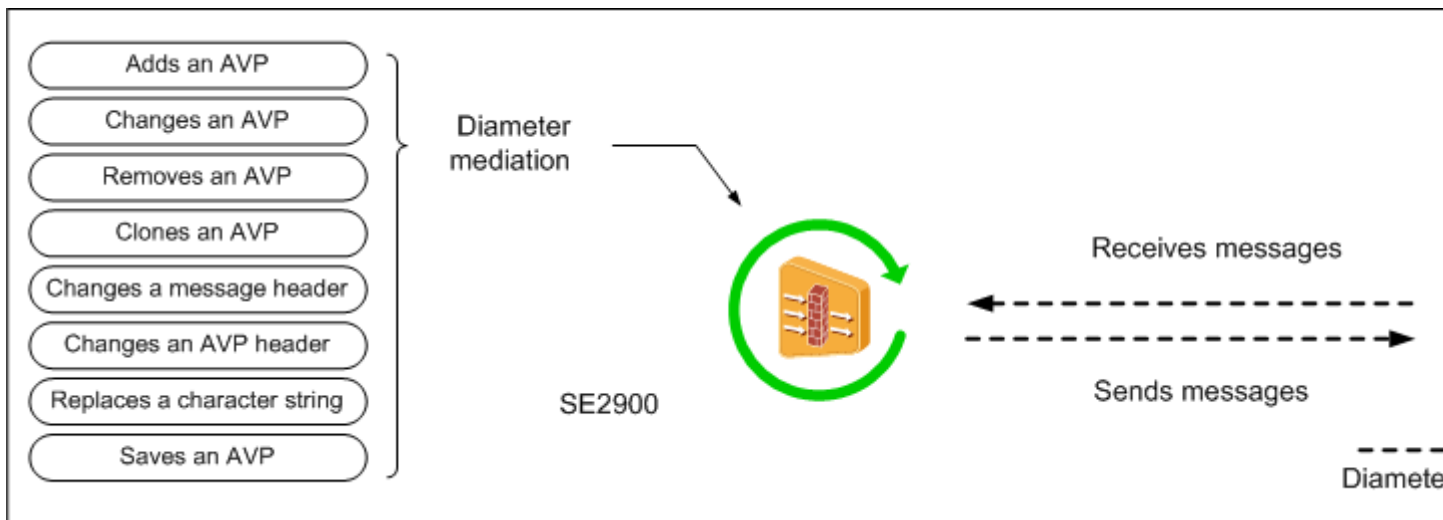
- Policy set: A user-defined policy set can associate multiple policies with an AN, a trunk group, a routing table, or an HMRIP. Then the SE2900 performs SIP header manipulation for the SIP messages in the AN, group, routing table, or HMRIP based on the policies in the set. An AN, a trunk group, a routing table, or an HMRIP can be associated with policies in different directions.

4.4.6 Diameter Mediation

Products of different vendors may use different Diameter protocol versions or implementation mechanisms, causing Diameter signaling transmission failures between such products and the SE2900. To address this problem, the SE2900 introduces the Diameter mediation feature. With this feature, the SE2900 can add, modify, delete, clone, or save AVPs, modify message headers or AVP headers, or replace character strings so that Diameter signaling can be transmitted properly.

Figure 4-45 shows how the SE2900 mediates Diameter signaling.

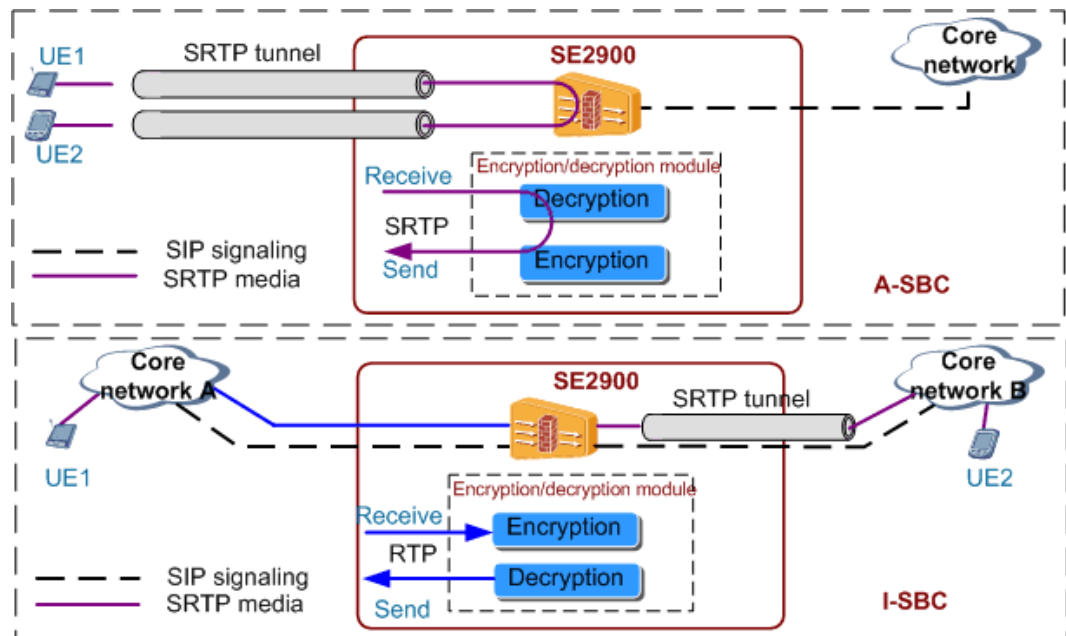
Figure 4-45 Diameter mediation



4.4.7 SRTP

Secure Real-time Transport Protocol (SRTP) enables the SE2900 to encrypt Real-Time Transport Protocol (RTP) packets transmitted between the SE2900 and UEs/SIP trunks, enhancing communication security between the SE2900 and UEs/SIP trunks. See Figure 4-46.

Figure 4-46 SRTP



Data verification and encryption are not performed during the packetization of RTP packets. Therefore, security and integrity cannot be ensured during data transmission using RTP or RTCP. To address this issue, SRTP is introduced to implement encryption, verification, integrity, and anti-playback protection for media packets transmitted between VoIP users.

Compared with common RTP packets, SRTP packets carry encrypted RTP payloads and two additional fields: Master Key Identifier (MKI) and authentication tag. The MKI field is optional and used to identify the master key in SRTP cryptographic contexts. The authentication tag field value is the hash-based message authentication code (HMAC) used for verifying packet headers and encrypted payloads.

In the A-SBC scenario, the SE2900 uses SRTP to encrypt media packets and uses SIP over TLS to encrypt signaling packets, ensuring secure data transmission between the SE2900 and UEs/SIP trunks.

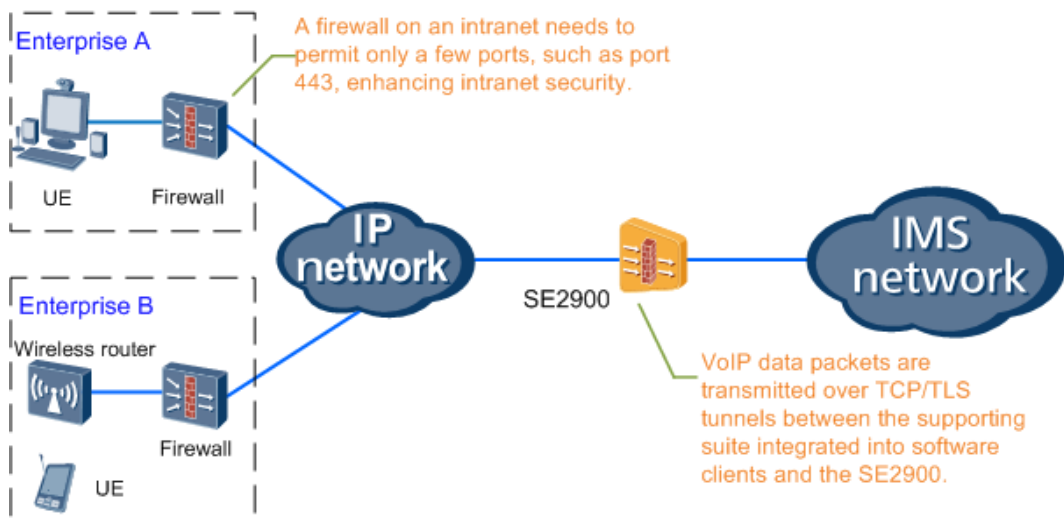
4.4.8 Firewall Traversal

More and more enterprises are deploying VoIP services on their intranets. Enterprises that deploy VoIP services must address the following problems:

- If an HTTP or socket proxy server is used to connect to the public network, the proxy server only forwards HTTP/HTTPS service streams. VoIP data packets are discarded, which renders the VoIP service unavailable.
- If a firewall is deployed at the border between the intranet and public network, and the firewall permits port 443 (HTTPS) or 80 (HTTP), VoIP data packets cannot traverse the firewall, causing VoIP service failures.

The firewall traversal feature can be configured on the SE2900, with supporting suite integrated into software clients, to address the preceding problems. Figure 4-47 shows the firewall traversal networking.

Figure 4-47 Firewall traversal



When firewall traversal is used, a firewall on an intranet needs to permit only a few ports, such as port 443, for RTP packets to ensure that VoIP data packets traverse the firewall or HTTP proxy server. Meanwhile, the supporting suite is integrated into software clients to encapsulate SIP/RTP packets. Then packets are transmitted over TCP/TLS tunnels and can traverse the firewall.

NOTE

To minimize the risks of attacks, enterprises usually permit only port 443 (HTTPS) or 80 (HTTP).

4.4.9 QoS Assurance

Quality of service (QoS) assurance provides expected quality for network communication services in terms of bandwidth, packet loss rate, round-trip delay, and jitter. QoS provides network services of differentiated quality based on service requirements. It focuses on user experience rather than on the techniques that are involved in services, network design, or QoS degradation causes.

QoS enables carriers to monitor the status of the media plane and the operating status of the network, based on which the carriers can adjust and optimize their networks and improve service quality. In addition, the reported QoS data also can be used in network planning and troubleshooting. QoS assurance involves the following functions: voice quality reporting, policy control support (Rx), multimedia priority service (MPS), and rate adjustment. Figure 4-48, Figure 4-49, and Figure 4-50 show the corresponding networking diagrams.

Figure 4-48 Voice quality reporting

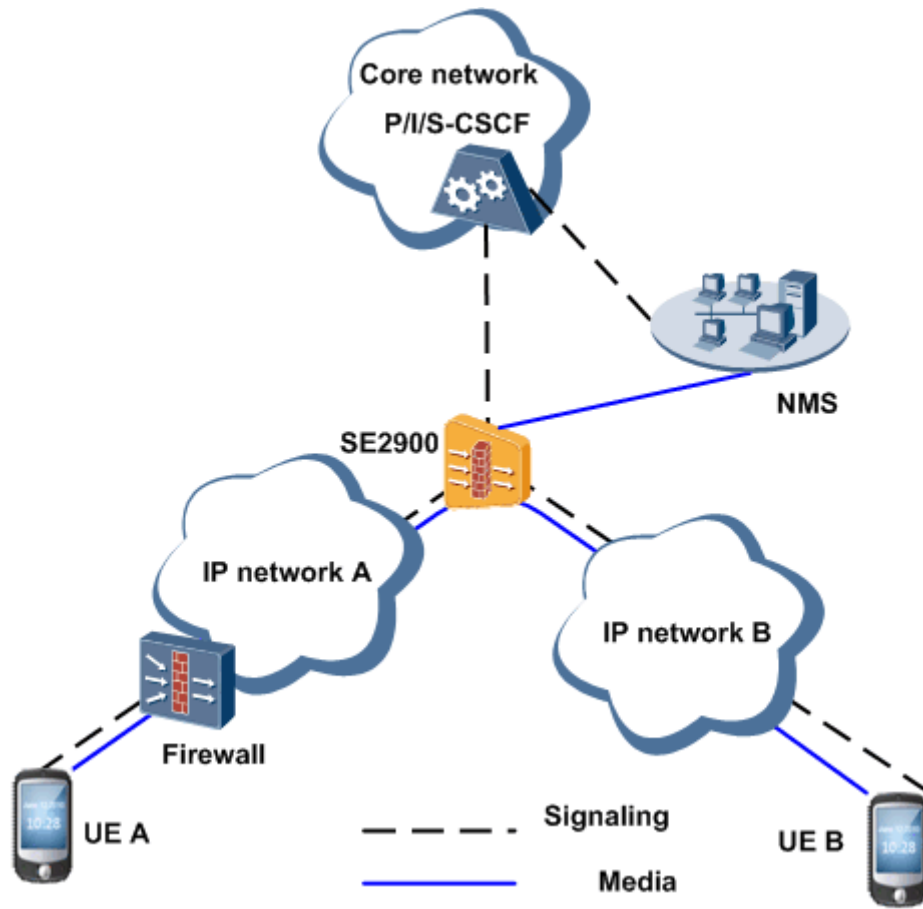


Figure 4-49 Policy control support (Rx)

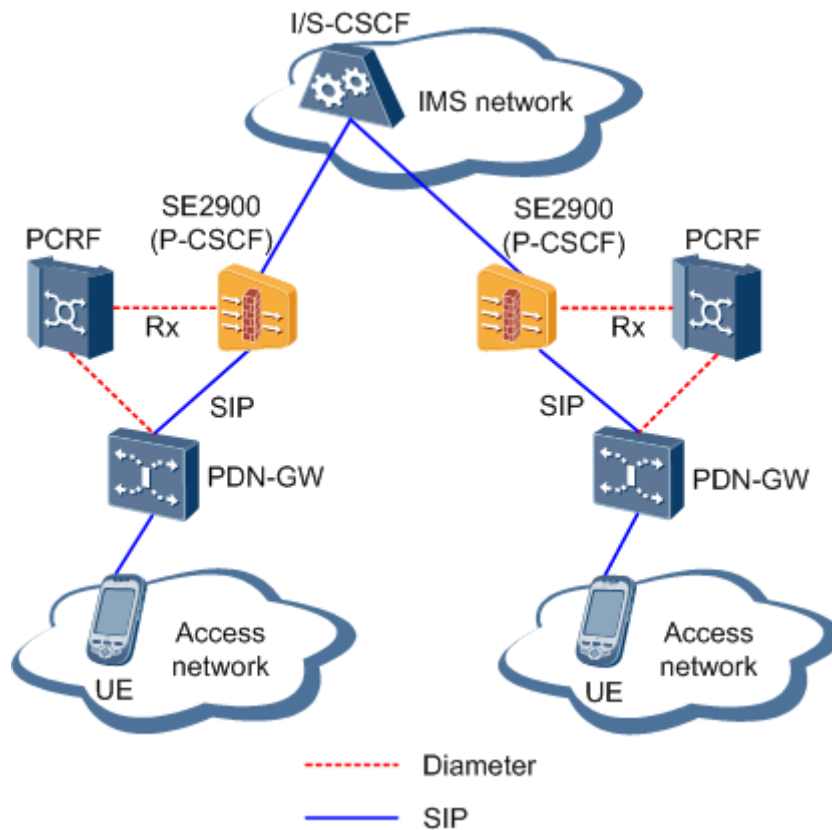


Figure 4-50 Rate adjustment



- **Voice quality reporting:** This function enables the SE2900 to measure the voice quality of calls in real time, including the packet loss rate, jitter, and round-trip delay, and sends SIP INFO messages, BYE messages, or 200 OK responses (BYE) carrying quality information to the core network.
- **Policy control support (Rx):** The Rx interface is defined in the 3GPP policy and charging control (PCC) mechanism. The SE2900 extracts the session information about a UE, such as the signaling address, media address, and media bandwidth, from SIP messages, and sends the information to the policy and charging rules function (PCRF) over the Rx interface. The PCRF uses the session information to instruct the policy and charging enforcement function (PCEF) to implement PCC.
- **MPS:** This function enables users to preferentially use multimedia services when the network quality is poor. The MPS is categorized as follows:
 - **User priority-based MPS:** The SE2900 prioritizes the calls initiated from users who have subscribed to the MPS service.

- URI-based MPS: The SE2900 identifies the calls to callees specified by URIs (in the number or address format) and preferentially processes the calls if they are of high priority.
- Rate adjustment: The eNodeB and SE2900 interwork with each other to adjust the AMR bitrate based on the changes to the transmission quality of the air interface connected to a VoLTE network, improving audio adaptive capabilities. Specifically, the adjustment is implemented as follows:
 - At cell borders where the transmission quality of the air interfaces is poor, the AMR bitrate is reduced to improve the coverage of VoLTE audio services.
 - In areas where the transmission quality of the air interfaces is good, the AMR bitrate is increased to provide better user experience.

4.4.10 IMS-AKA/IPSec

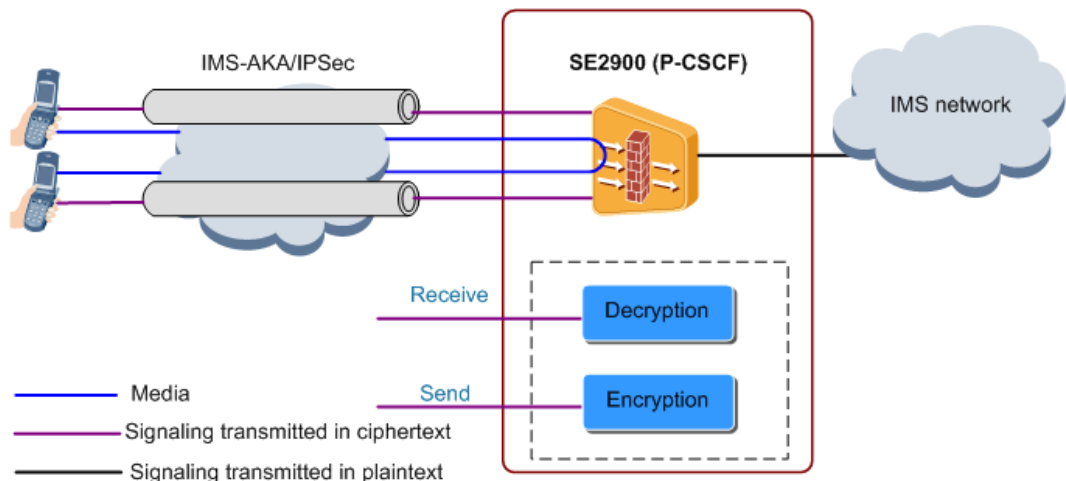
IMS-Authentication and Key Agreement (AKA)/Internet Protocol Security (IPSec) is a mechanism that enables the IMS network and IMS UEs using IP multimedia services identity module (ISIM) cards to authenticate each other. This mechanism implements mutual authentication between IMS UEs and the IMS network. During the authentication process, the IMS network delivers keys to the SE2900. The SE2900 uses the keys to prevent signaling packets from being tampered with and sensitive user information from being disclosed.

 **NOTE**

The ISIM card stores a series of parameters of the UE required by the operations performed in the IMS, such as identity identification, user authorization, and UE setting data.

When UEs access the SE2900 by using the IMS-AKA/IPSec feature, the SE2900 uses IMS-AKA to decrypt UE-originated signaling messages and sends the messages in plaintext to the core network; the SE2900 uses IPSec to encrypt core-network-originated signaling messages and sends the messages in ciphertext to UEs. See Figure 4-51.

Figure 4-51 IMS-AKA/IPSec



A quintet is used to verify the network during IMS-AKA/IPSec authentication. The quintet contains the following parameters:

- Random challenge (RAND): The network provides a RAND to UEs, and the UEs use the RAND to calculate expected response (XRES), IK, and cipher key (CK).

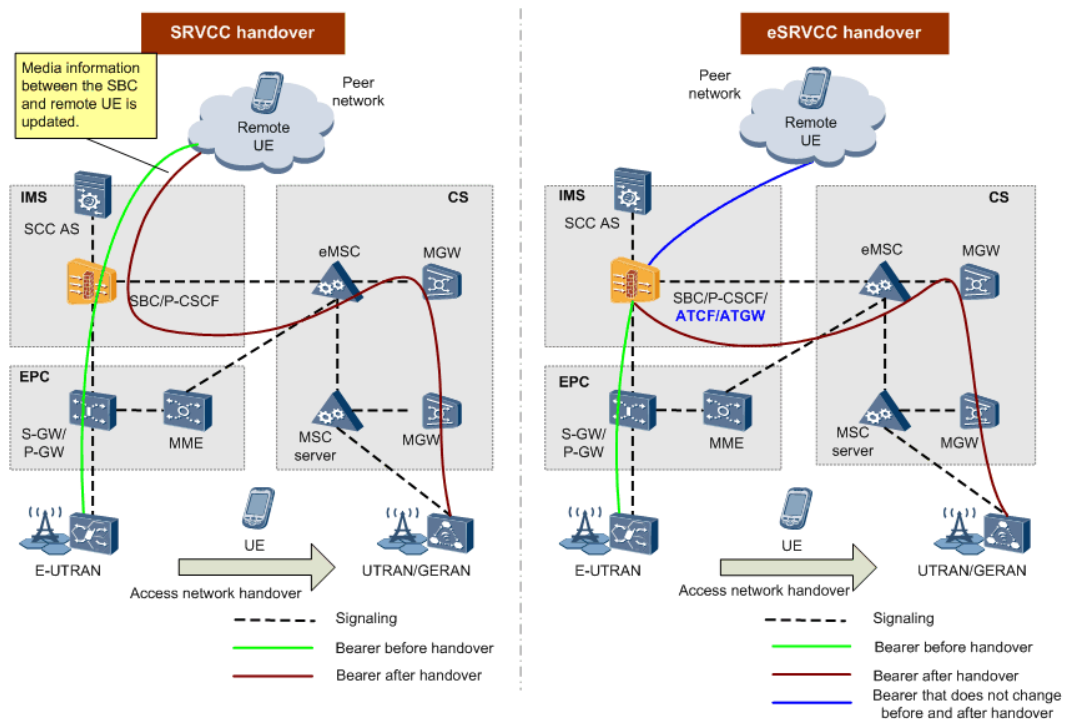
- XRES: The SE2900 compares XRES with SRES in the authentication response message sent by a UE to determine whether the UE is successfully authenticated by the network.
- CK: It is used for encrypting/decrypting signaling on the UE or network side.
- IK: It is used for verifying data integrity on the UE or network side, preventing data from being tampered with.
- Authentication token (AUTN): It is a parameter used by UEs to authenticate the network.

4.4.11 ATCF/ATGW

Single radio voice call continuity (SRVCC) is a VoLTE voice service continuity solution defined by 3GPP to solve voice service problems in the early phase of LTE network deployment. SRVCC provides single radio users with uninterrupted calls when they move from an evolved universal terrestrial radio access network (E-UTRAN) to a UMTS terrestrial radio access network (UTRAN) or GSM/EDGE radio access network (GERAN). (A single radio UE can access only one network at a time.)

As an enhancement to SRVCC, enhanced SRVCC (eSRVCC) optimizes the SRVCC networking scheme. See Figure 4-52.

Figure 4-52 ATCF/ATGW



In eSRVCC handover, the SE2900 provides the access transfer control function (ATCF)/access transfer gateway (ATGW) as well as the P-CSCF. The ATCF/ATGW is deployed between the P-CSCF and I-CSCF/S-CSCF and media is anchored on the ATGW for calls during a handover of a UE. During an eSRVCC handover of a UE, the ATCF anchors the media information of the UE on the ATGW so that the remote media information does not need to be updated when the UE is handed over from the E-UTRAN to a UTRAN or GERAN, minimizing call interruption.

4.4.12 P-CSCF

With the P-CSCF feature, the SE2900 is able to provide access to the IMS network for UEs on both the VoLTE and VoBB networks using SIP ANs on one SE2900, enhancing network convergence (such as VoLTE and VoBB convergence) and saving the expenditure of deploying a separate P-CSCF.

The P-CSCF is the entry point of the control plane on the IMS network (visited network). It is a proxy for all SIP messages, including REGISTER, INVITE, and Presence messages, from the access network (visited network) to the S-CSCF/I-CSCF on the home network. See Figure 4-53 and Figure 4-54.

Figure 4-53 P-CSCF in the VoLTE scenario

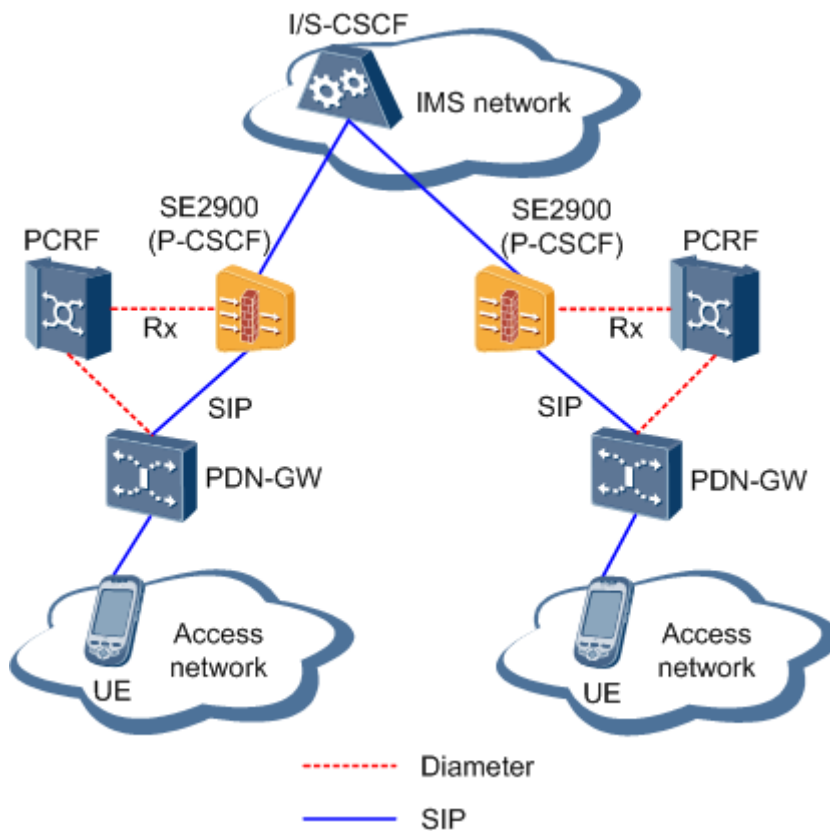
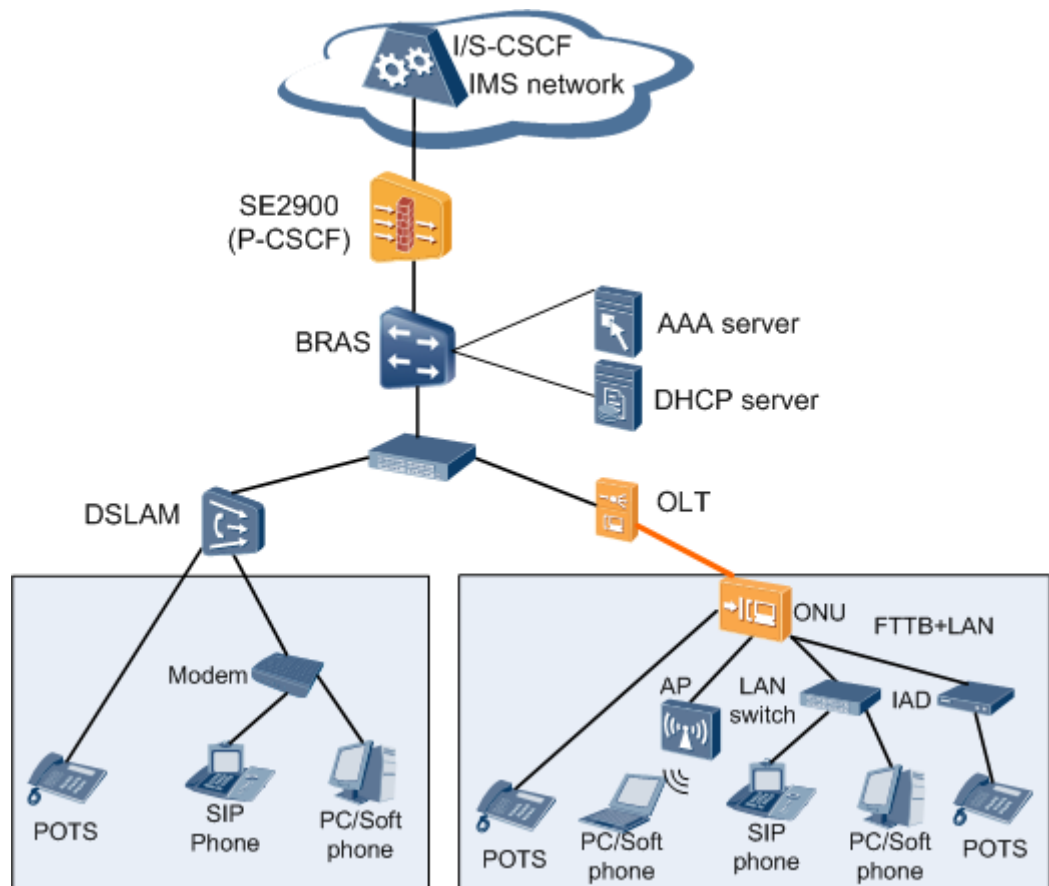


Figure 4-54 P-CSCF in the VoBB scenario



The P-CSCF feature applies to the following procedures:

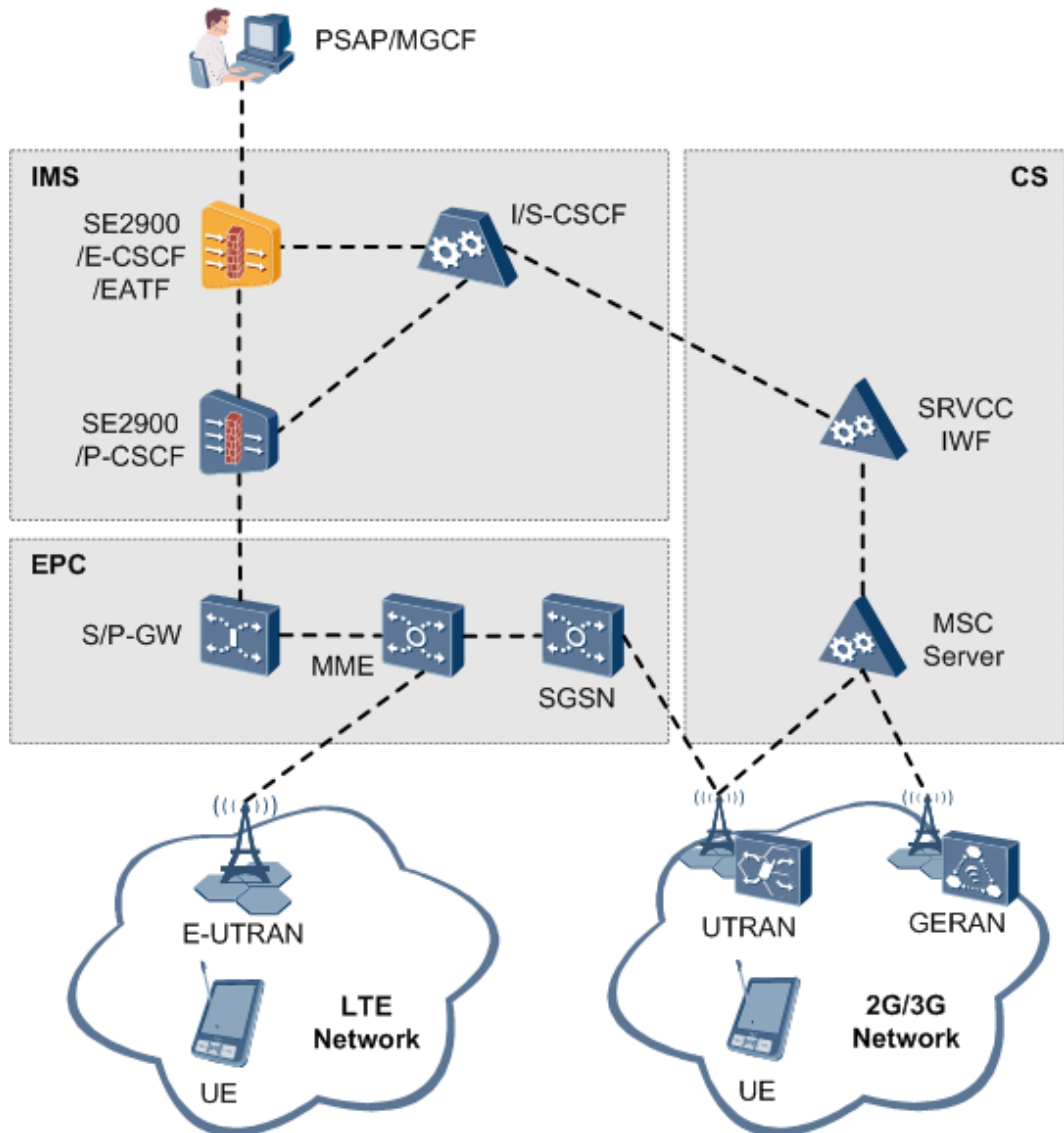
- Signaling proxy procedure
 - The SE2900 forwards UE-originated REGISTER requests to the I-CSCF. The I-CSCF selects an appropriate S-CSCF for SIP registration.
 - The SE2900 forwards UE-originated call messages to the S-CSCF. The S-CSCF processes the call messages for call control and routing.
- Roaming and nomadic procedure
 - Roaming enables users to continue using the services provided by the home network when they move from the home network to the visited network.
 - The home subscriber server (HSS) implements control on UE access to the IMS network by matching the reference position information and subscribed nomadic template information on a UE with the UE access position information. The nomadic procedure allows the SE2900 to manage UE mobility and control the access to the IMS network.
- Authentication procedure: This mechanism implements mutual authentication between UEs and the IMS network. The IMS network authenticates UEs to prevent unauthorized users from accessing the IMS network. Meanwhile, UEs authenticate the IMS network to avoid fraudulent networks. The P-CSCF enables the IMS network to initiate the authentication procedure.

- Core network redundancy procedure: When an I/S-CSCF becomes faulty, the SE2900 forwards UE-originated messages to a properly functioning I/S-CSCF to implement I/S-CSCF disaster tolerance, therefore ensuring non-stop services for UEs.

4.4.13 E-CSCF/EATF

The E-CSCF/EATF feature provides an embedded emergency-call session control function (E-CSCF) for the SE2900, which enables the SE2900 to process and route emergency calls to an emergency center (EC). The E-CSCF/EATF feature provides an embedded emergency access transfer function (EATF) for the SE2900, which enables the SE2900 to anchor emergency calls and switch emergency calls from a PS network to a CS network for call continuity. This feature enables carriers to provide emergency call services without deploying a separate E-CSCF or EATF, thereby simplifying the network structure and reducing capital expenditure (CAPEX). Figure 4-55 shows the networking for IMS emergency calls.

Figure 4-55 Networking for IMS emergency calls



The E-CSCF/EATF can be configured on the SE2900 by running **ADD SIPAN**.



NOTE

The EATF must be deployed in conjunction with the E-CSCF on the SE2900.

- If the SE2900 provides an embedded E-CSCF, the E-CSCF is deployed between the P-CSCF and public safety answering point (PSAP) and processes the emergency calls received from the P-CSCF.
 - The E-CSCF obtains local user location information, performs route analysis for emergency call numbers, and routes emergency calls to the EC.
 - If the E-CSCF cannot obtain local UE location information, it obtains user location information and emergency call routing information from the location retrieval function (LRF) and routes emergency calls to the EC.
- If the SE2900 provides an embedded E-CSCF and EATF, the E-CSCF processes the emergency calls received from the P-CSCF. During emergency call establishment, media is anchored on the EATF for the calls during which a single radio voice call continuity (SRVCC) handover is likely to occur. Then the E-CSCF routes the emergency calls to the EC. When an SRVCC handover occurs during an emergency call, the EATF instructs the E-CSCF to update remote media. After the remote media update is complete, the E-CSCF instructs the P-CSCF to release the emergency call and notifies the EATF of a handover success.

4.4.14 Flexible Routing

Flexible routing enables the SE2900 to select routes in a flexible manner for users on different networks based on configured number and route analysis data, thereby improving routing efficiency and ensuring network availability.

The SE2900's flexible routing supports the following functions:

- Route header-based routing
The SE2900 uses the IP address carried in the Route header as the next-hop IP address and forwards messages accordingly.
- ENUM query-based routing
The SE2900 sends an E.164 number to the ENUM server and determines the route based on the URI returned by the ENUM server.
- DNS query-based routing
The SE2900 queries the domain name carried in the Request-URI or the Route header against the DNS server and forwards messages to the IP address returned by the DNS server.
- Route selection name-based routing
 - The SE2900 routes messages based on the number in the TEL URI/TEL URL carried in the Request-URI.
 - The SE2900 routes messages based on the SIP URI (content and domain name format) carried in the Request-URI or Route header.
 - The SE2900 routes messages based on the **tgrp** parameter and the optional **trunk-context** parameter in the Request-URI.
- Route selection source code-based routing
The SE2900 selects the route based on the calling number and incoming trunk group.
- User type-based routing
The SE2900 determines the routes based on caller types.
- Media type-based routing

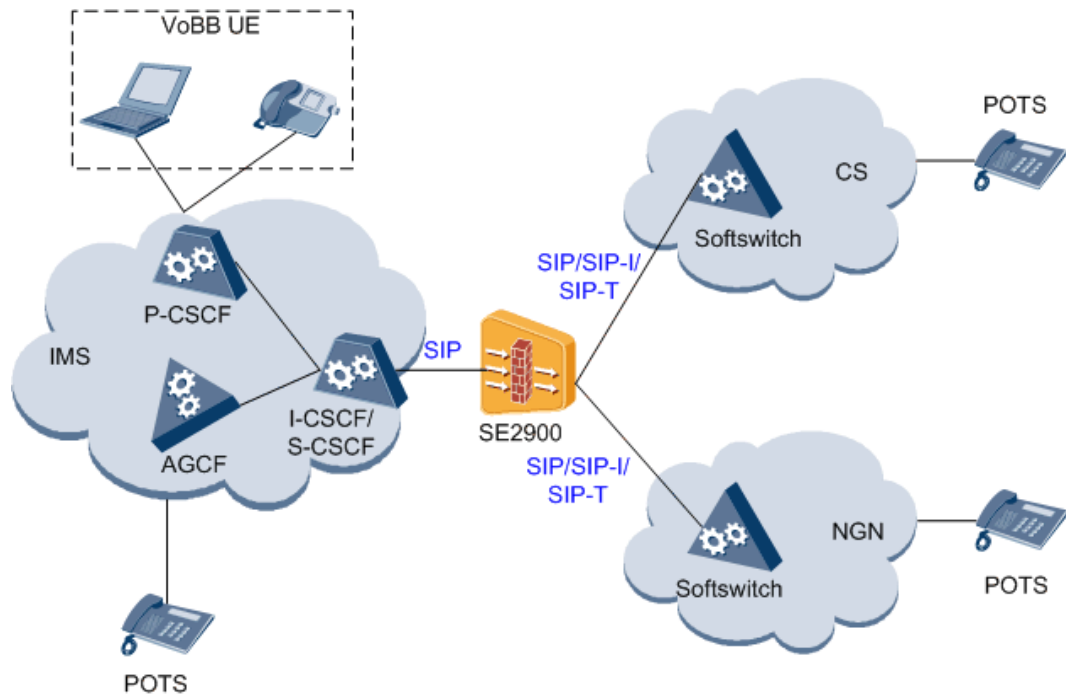
- The SE2900 determines routes based on the types of media transmitted over the routes.
- Call type-based routing
The SE2900 determines routes based on call types.
 - Codec-based routing
The SE2900 determines the routes based on the codecs carried in SDP information.
 - Message type-based routing
The SE2900 determines the routes based on types of SIP messages.
 - Validity period of the flexible routing policy
After the validity period of the flexible routing policy is specified, the SE2900 enables flexible routing as scheduled.
 - Call status-based routing
The SE2900 selects a trunk group with the least number of concurrent calls or lowest call rate in the route to forward messages of a call based on the call status.
 - Rerouting upon routing failures
The SE2900 reselects a route after receiving an OXX response from the outgoing office direction based on configured policies.
 - QoS-based routing
To improve QoS quality, the SE2900 forwards packets along a route that is selected based on real-time QoS information.

4.4.15 SIP-I/SIP-T

As networks keep growing, network interworking becomes increasingly diversified. SIP with encapsulated ISUP (SIP-I) or SIP for Telephones (SIP-T) is currently the preferred means for implementing interworking between mobile CS networks and SIP peers (NGN/CDMA networks, SIP-based service platforms, and IP PBXs). In network interworking, NEs provide various SIP capabilities, depending on the types of UEs and network services. For example, some services must be borne over SIP-T or on the basis of ISUP messages.

The SIP/SIP-I/SIP-T interworking feature allows the SE2900 to serve as an IP interworking gateway for IMS networks, NGN/CDMA networks, mobile CS networks, and IP PBXs, and to provide basic voice services and supplementary services for various networks. See Figure 4-56.

Figure 4-56 SIP/SIP-I/SIP-T interworking



SIP is a text-based and application-layer control protocol that can establish, modify, and terminate multimedia sessions or calls. It is based on an HTTP-like request/response transaction model, which can be used to implement various multimedia services, including voice, video, and instant messaging services. SIP-I and SIP-T are extensions to SIP.

- SIP-I

SIP-I, defined in ITU-T Q.1912.5, is used to carry ISUP bodies in SIP messages so that the ISUP bodies can be transmitted over SIP networks without transmission loss. ITU-T Q.1912.5 defines interworking between 3GPP SIP and Bearer Independent Call Control (BICC)/ISUP, interworking between SIP and BICC/ISUP, and interworking between SIP-I and BICC/ISUP.

SIP-I reuses many IETF-defined standards and drafts, including basic call interworking and BICC/ISUP supplementary service interworking.

- SIP-T

SIP-T, defined in IETF RFC 3372, is similar to SIP-I and. It also carries ISUP bodies in SIP messages. SIP-T provides a mechanism in which a SIP message can contain ISUP signaling to implement better interworking between the public switched telephone network (PSTN) and the SIP network. SIP-T involves three call models: PSTN-IP, IP-PSTN, and PSTN-IP-PSTN. SIP-T employs the SIP message structure and procedure. SIP-T offers encapsulation and mapping technologies for SIP and ISUP interworking. Encapsulation, which is defined in RFC 3204, means that a SIP message contains an ISUP message. Mapping, which is defined in RFC 3398, includes the ISUP-SIP message mapping and the mapping between ISUP message parameters and SIP message headers.

SIP-T involves basic call interworking but does not involve supplementary service interworking.

SIP-I and SIP-T: SIP-I and SIP-T are both extensions to SIP. They are introduced to implement the interworking between the Softswitch network and the PSTN/public land mobile network (PLMN). SIP-I is defined by ITU and SIP-T is defined by IETF. SIP can be

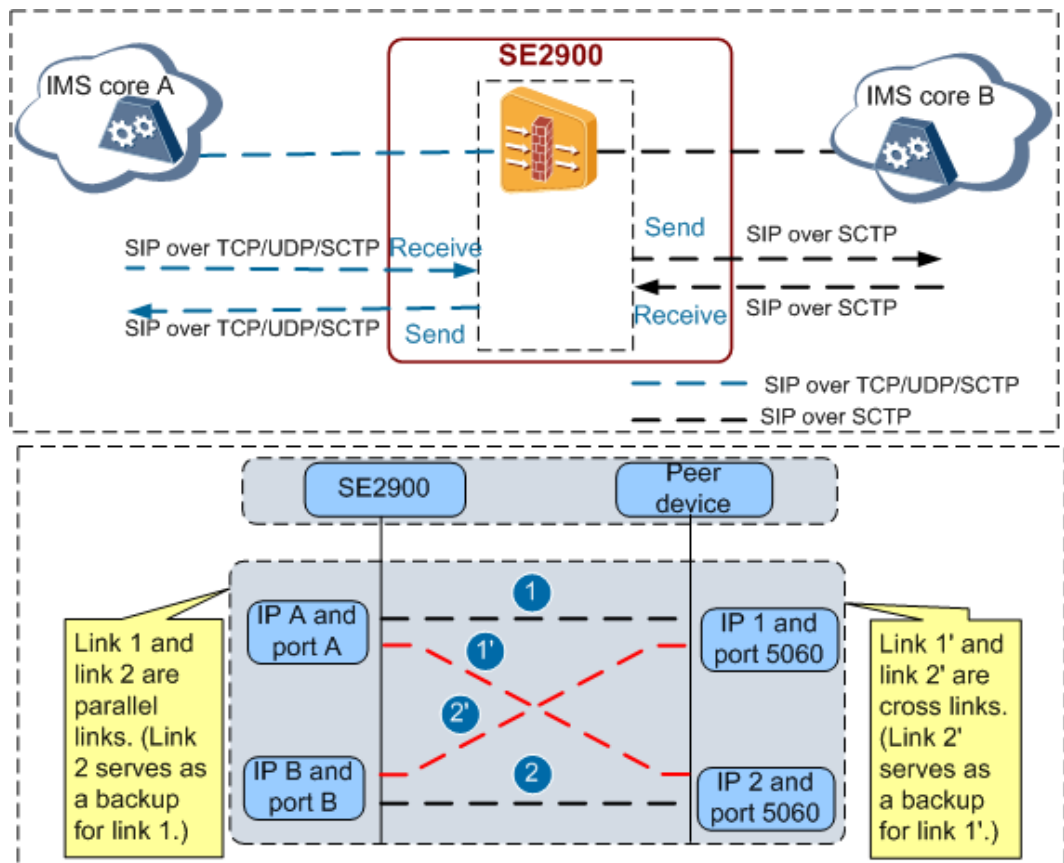
used as both a network-to-network (NNI) interface and a user-to-network (UNI) interface, whereas SIP-I and SIP-T are used as NNI interfaces.

4.4.16 SIP over SCTP

Stream Control Transmission Protocol (SCTP) is an IP-based transport layer protocol. SCTP provides efficient and reliable transmission services for MTP2-User Adaptation Layer (M2UA), MTP3-User Adaptation layer (M3UA), ISDN Q.921-User Adaptation layer (IUA), H.248, Bearer Independent Call Control (BICC), and SIP signaling over the IP network. Message exchanges on the IP network are usually implemented using UDP or TCP. UDP cannot ensure reliable message transmission, and TCP cannot ensure efficient and secure message transmission. SCTP combines the advantages of UDP and TCP and provides a connection-oriented data transmission service on the IP network.

SIP over SCTP enables the SE2900 to use SCTP as a transport-layer protocol to transmit SIP messages. With SIP over SCTP, SIP messages are transmitted over SCTP between the SE2900 and core network to enhance reliability in SIP message transmission. See Figure 4-57.

Figure 4-57 SIP over SCTP



The SE2900 supports the processing of SIP messages over SCTP and UDP.

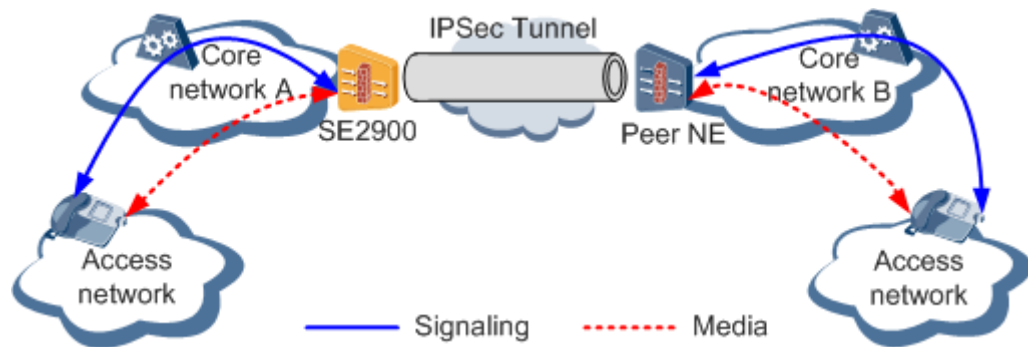
- Before forwarding a message from core network A to core network B, the SE2900 changes the transport-layer protocol from SCTP to UDP/TCP/SCTP.
- Before forwarding a message from core network B to core network A, the SE2900 changes the transport-layer protocol from UDP/TCP/SCTP to SCTP.

4.4.17 IPSec Tunnel

Internet Protocol Security (IPSec) is an IP layer standard security protocol suite that is defined by the Internet Engineering Task Force (IETF) and provides security services for the IP layer. IPSec enables the system to choose security protocols as required, determine a proper algorithm, and put required keys in place. IPSec is used to protect one or more paths between hosts, between security gateways, and between hosts and security gateways. IPSec provides high-quality, interoperable, and cryptology-based security for IP packets.

In the I-SBC scenario, IPSec can be bound to interfaces on the SE2900 and peer NE for data authentication or encryption so as to ensure security for data packets. See Figure 4-58.

Figure 4-58 Networking for IPSec tunnel interworking



- An IPSec tunnel provides an end-to-end secure connection so that IP packets can be encrypted on one end and decrypted on the peer end.
- IPSec tunnel interworking provides security services, such as access control, connectionless integrity, data source authentication, anti-playback protection, confidentiality, and limited transport stream confidentiality.
- IPSec uses Authentication Header (AH) and Encapsulating Security Payload (ESP) to provide confidentiality, data integrity, authentication, and anti-playback protection for data packets transmitted on networks. IPSec can also use Internet Key Exchange (IKE) to automatically negotiate key exchange and establish and maintain security associations (SAs) to simplify the use and management of IPSec.
 - Confidentiality: Encrypted packets are sent in ciphertext to prevent user data from disclosure during transmission.
 - Data integrity: The received data is authenticated to check whether the packets are tampered with during transmission.
 - Data authentication: The data source is authenticated to guarantee that data is transmitted from an authenticated sender.
 - Anti-replay: This function is used to prevent users from repeatedly sending data packets. The receiver rejects old or duplicate packets.

4.4.18 IPv6

IPv6 is a feature that enables the SE2900 to provide network access using IPv4/IPv6 dual-stack. With this feature, IPv4/IPv6 UEs can access an IPv4/IPv6 core network and IPv4/IPv6 core networks can interwork with each other.

SE2900 supports IPv6 in the A-SBC scenario or I-SBC scenario, including:

- A-SBC scenario:
 - An IPv6 UE accesses an IPv4 core network.
 - An IPv6 UE accesses an IPv6 core network.
 - An IPv4 UE accesses an IPv6 core network.
 - Combined configuration of IPv4 and IPv6 on the core side.
- I-SBC scenario:
 - An IPv6 core network interworks with an IPv4 core network.
 - An IPv6 core network interworks with another IPv6 core network.
 - An IPv4 core network interworks with an IPv6 core network.
 - Combined configuration of IPv4 and IPv6 on the core side.

Figure 4-59 shows the networking for an IPv6 UE to access the IPv4 core network through the SE2900 in the A-SBC scenario.

Figure 4-59 IPv4-IPv6 interworking (A-SBC scenario)

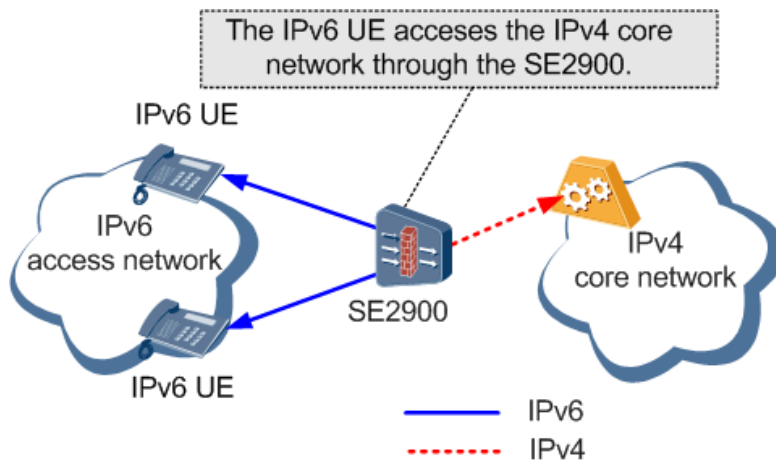
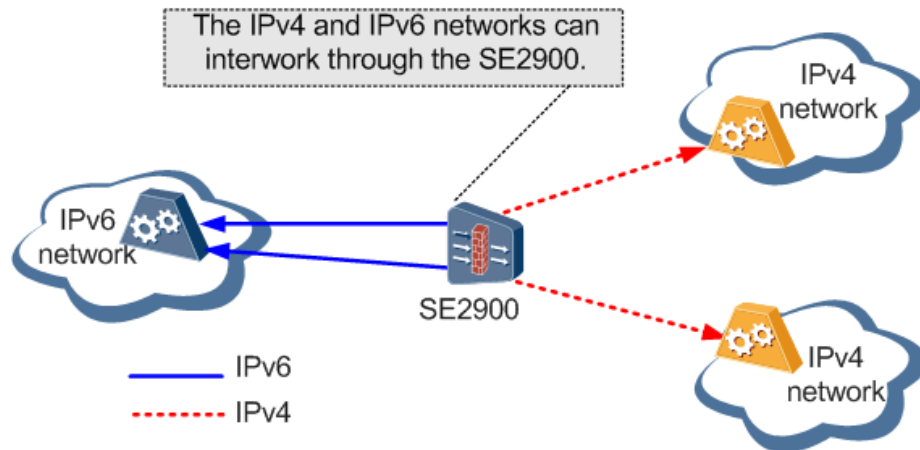


Figure 4-60 shows the networking for interworking between the IPv4 core network and the IPv6 core network through the SE2900 in the I-SBC scenario.

Figure 4-60 IPv4-IPv6 interworking (I-SBC scenario)



4.4.19 IP-PBX Trunking

The private branch exchange (PBX), also called the private automatic branch exchange (PABX), is a dedicated exchange that provides call center functions or hotline functions for corporate users, such as enterprises, companies, and banks, and provides special service console functions for such services as fire and police emergency calls. The PBX, which incorporates telephones, fax machines, modems, and other devices, interconnects the internal telephones of an enterprise and connects them to the public switched telephone network (PSTN).

The PBX can be classified into TDM-PBX and IP-PBX.

- TDM-PBX: refers to a PBX that accesses the IMS network using the time division multiplexing (TDM) technology.
- IP-PBX: refers to a PBX that accesses the IMS networking using the IP technology, excluding the H.323 IP-PBX and basic rate access (BRA) integrated services digital network (ISDN) PBX. When an IP-PBX accesses the IMS network, no media gateway is required to perform media conversion.

The SE2900 implements IP-PBX trunking to provide IP-PBXs with access to the IMS network. This feature allows carriers to provide more diverse services for the UEs attached to the IP-PBX with discontinuous number segments and enables users to access diverse services on the IMS network.

The SE2900 supports different functions for different types of IP-PBXs:

- IP-PBX with the registration capability: UEs attached to the IP-PBX do not need to initiate registration procedures. The IP-PBX initiates registration procedures for them. After the IP-PBX is registered successfully, all UEs attached to the IP-PBX can initiate calls without initiating registration procedures. The IP-PBX accesses the IMS network through the A-BCF. See Figure 4-61.
- IP-PBX without the registration capability: The SE2900 acts as a registration proxy for the IP-PBX. The IP-PBX accesses the IMS network through the IBCF. See Figure 4-62.

Figure 4-61 IP-PBX trunking (A-SBC)

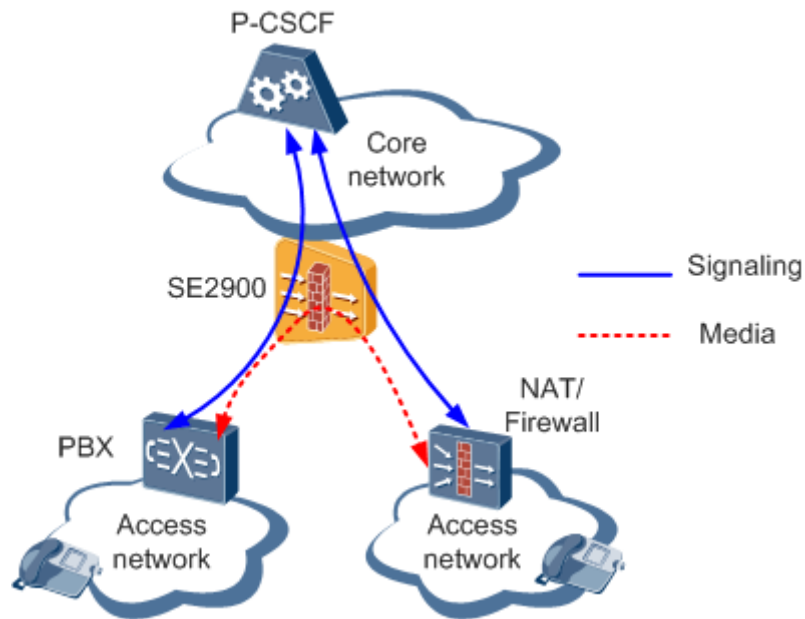
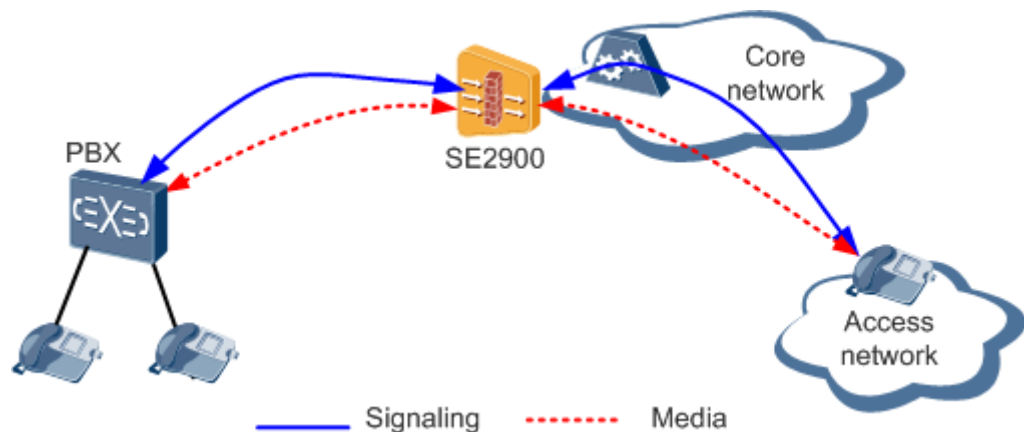


Figure 4-62 IP-PBX trunking (I-SBC)



4.4.20 Audio Transcoding

Voice data is usually compressed with codecs before being transmitted over the network so as to save bandwidth. Different audio codec standards are defined for different networks or the same network in different phases. Audio transcoding is required for UEs on different networks.

The SE2900 supports multiple codecs and can convert between G.711 (including G.711A and G.711U), G.729 (including G.729A and G.729AB), G.723.1, G.722, internet Low Bit Rate Codec (iLBC), adaptive multirate (AMR),.

Figure 4-63 and Figure 4-64 show audio transcoding networking in A-SBC and I-SBC scenarios respectively.

Figure 4-63 Audio transcoding networking in the A-SBC scenario

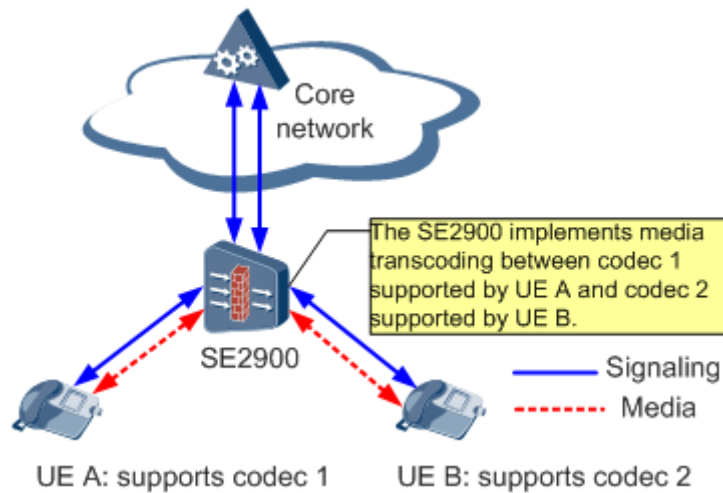
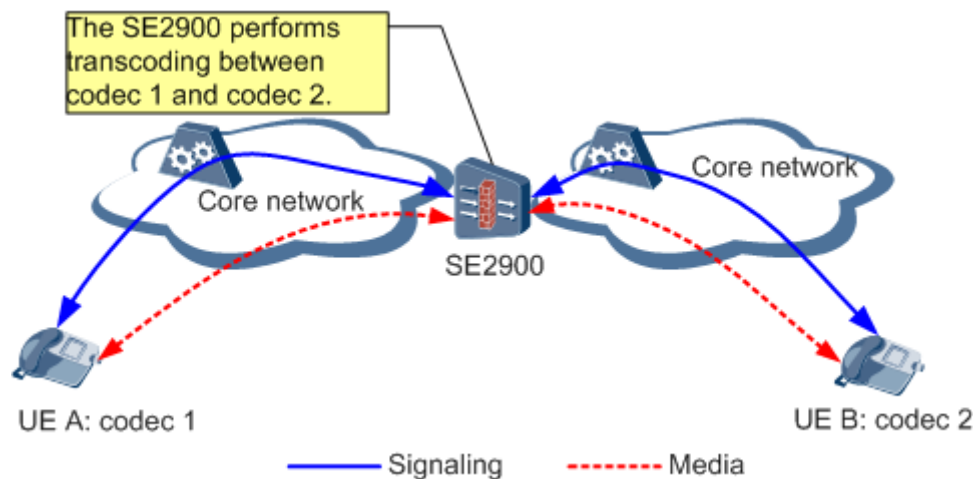


Figure 4-64 Audio transcoding networking in the I-SBC scenario



This feature enables carriers to lower their capital expenditure (CAPEX) and operating expenditure (OPEX) by implementing signaling and media interworking between different network types. This feature also helps carriers increase call complete rate, therefore improving user satisfaction and increasing revenues. This feature supports the following types of media format conversion:

- Audio conversion
 - Conversion between G.711 (including G.711A and G.711U), G.729 (including G.729A and G.729AB), G.723.1, G.722, iLBC, AMR,
 - Conversion between the same ARM/AMR-WB codec with different parameters, such as different **mode-set** parameter values, different packetization modes, and different mode control parameter values
 - Conversion between same G.711, G.729, iLBC, AMR, or AMR-WB codec format that have different ptime values
- Fax conversion

- Conversion between fax over T.38 and fax over G.711
- Conversion between fax over G.711A and fax over G.711U
- DTMF conversion
 - Conversion between G.711 dual tone multiple frequency (DTMF) and RFC2833 DTMF
 - Conversion between G.711 DTMF (on the bearer plane) and SIP INFO DTMF (on the signaling plane)
 - Conversion between RFC2833 DTMF (on the bearer plane) and SIP INFO DTMF (on the signaling plane)

4.4.21 Charging

The SE2900 can trigger charging in A-SBC and I-SBC scenarios. After the SE2900 collects charging information (such as calling and called numbers, session start time, and the session duration) from SIP signaling messages, the following situations are possible:

- The SE2900 sends Diameter Apply Charging Report (ACR) messages to the charging collection function (CCF), namely iCG9815. Based on the charging information, the CCF generates charging data records (CDRs), compares the CDRs with those generated by other NEs, and sends the CDRs to the billing center (BC). Generally, session durations in CDRs are compared. See Figure 4-65.
- The SE2900 sends Diameter ACR messages to its CCF. Based on the charging information, the CCF generates CDRs and then consolidates, sorts, and filters the CDRs, and finally sends the CDRs to the BC. See Figure 4-66.

Figure 4-65 Networking for transmitting charging information to the iCG9815

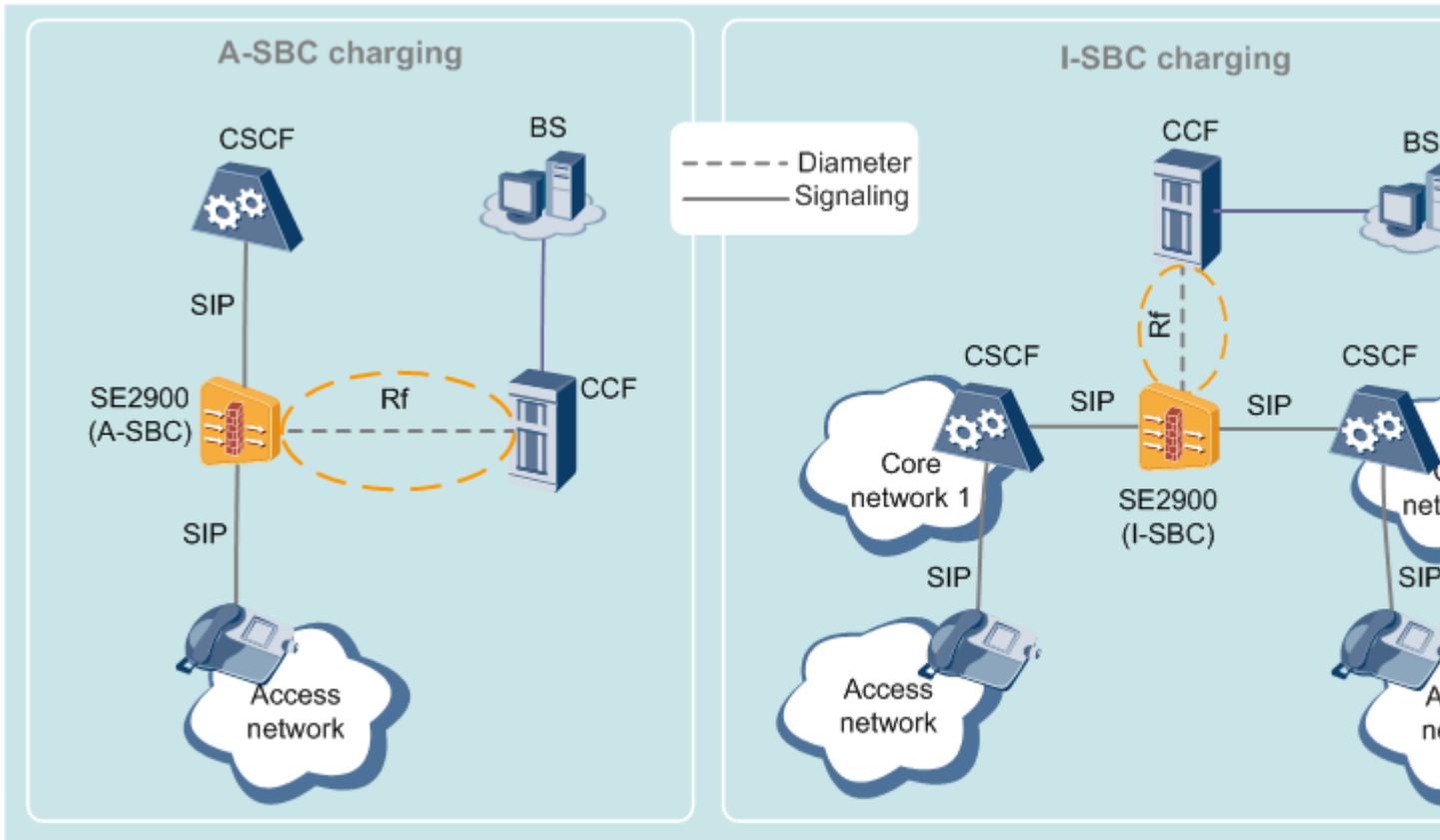
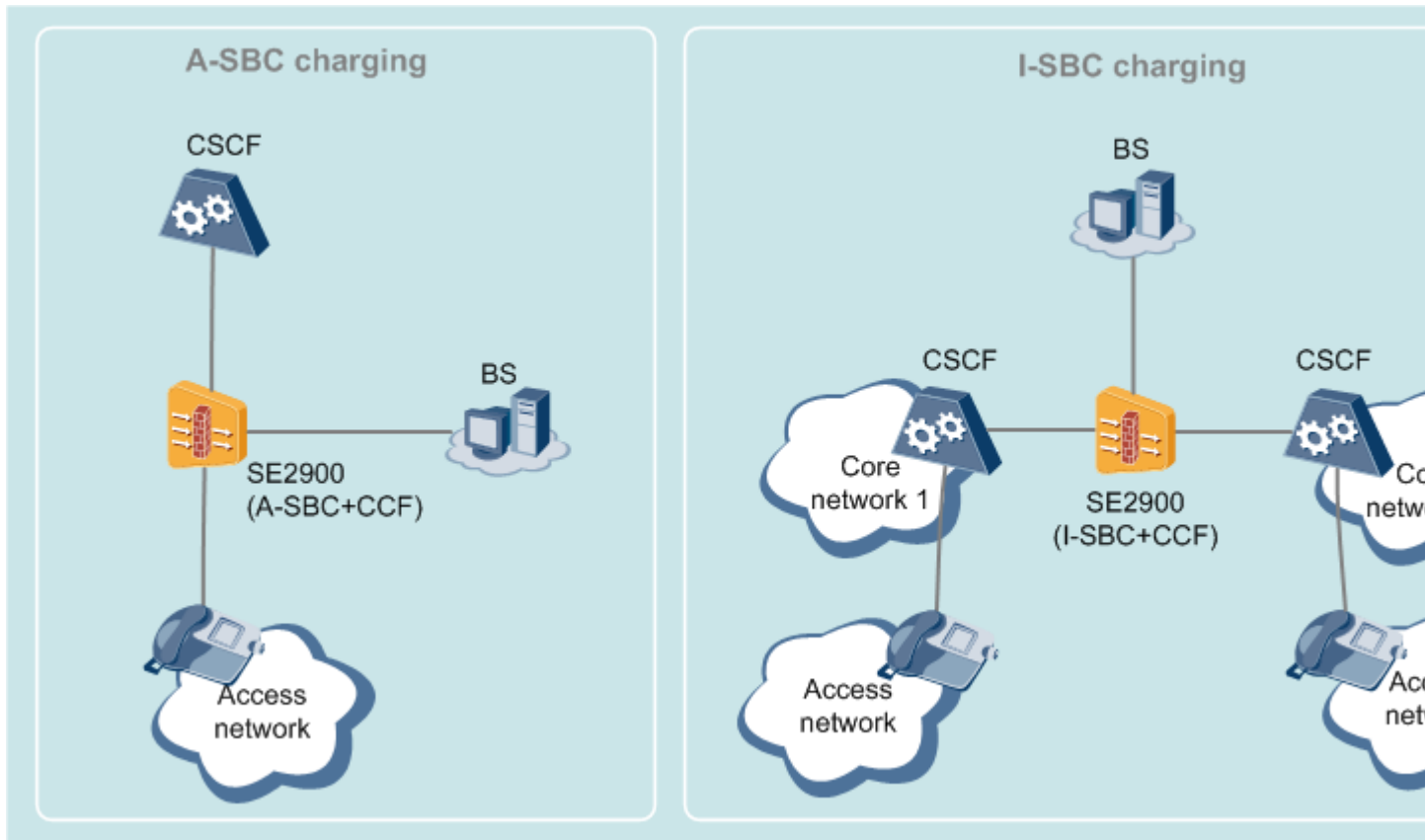


Figure 4-66 Networking for local charging



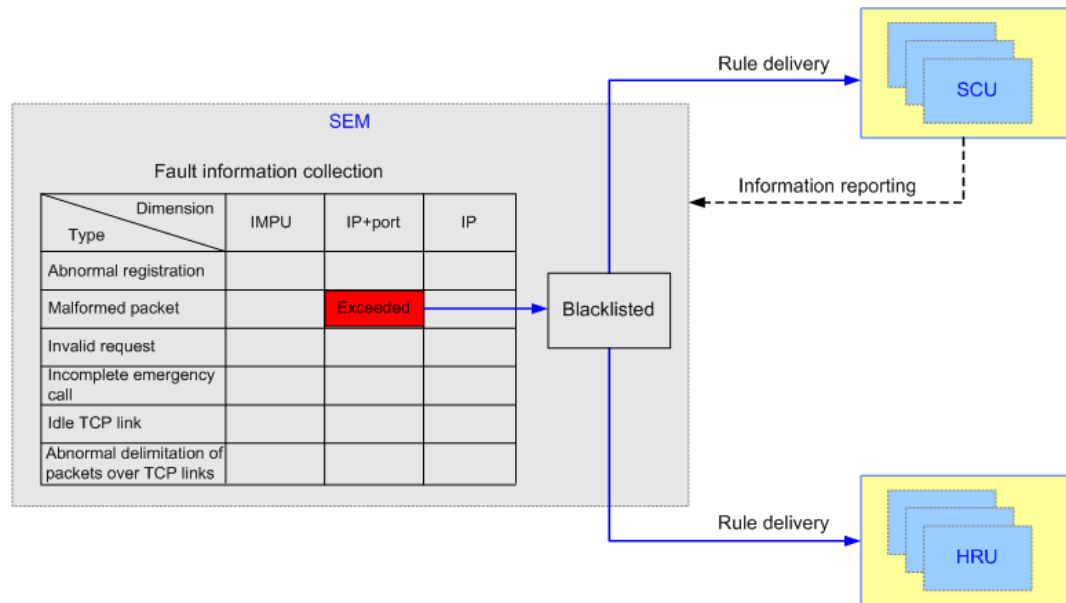
4.4.22 Security Enhancement Function

The SE2900 basic software package provides a variety of basic security functions, including topology hiding, IP layer attack defense, signaling DoS/DDoS attack defense, flow control, and media pinholing firewall. In addition to these basic security functions, the SE2900 provides a number of advanced security functions. These functions enhance the SE2900 attack defense capability, improve the flexibility in security management, and optimize the system resource management.

IDS

After inspect detection system (IDS) is enabled, the SE2900 constantly performs in-depth analysis on user behaviors, identifies attacks, and takes security measures against risks. The SE2900 can identify a variety of attacks, including malformed packet attacks, invalid request attacks, abnormal registration attacks, brute force cracking attacks, and incomplete emergency call attacks. Figure 4-67 shows the IDS mechanism.

Figure 4-67 IDS



NOTE

The security management (SEM), session control unit (SCU), and high-speed routing unit (HRU) are the modules of the SE2900. For details about the modules, see 5.2 Software Architecture.

The SEM collects fault information from service processes and classifies collected fault information by type. Then the SEM collects fault information by IMPU, source IP address, or source IP address + port. Statistics about fault information are cleared every 5 minutes. If the statistics exceed the corresponding threshold, the SEM blacklists the IMPU, source IP address, or source IP address + port.

Blacklist and Whitelist

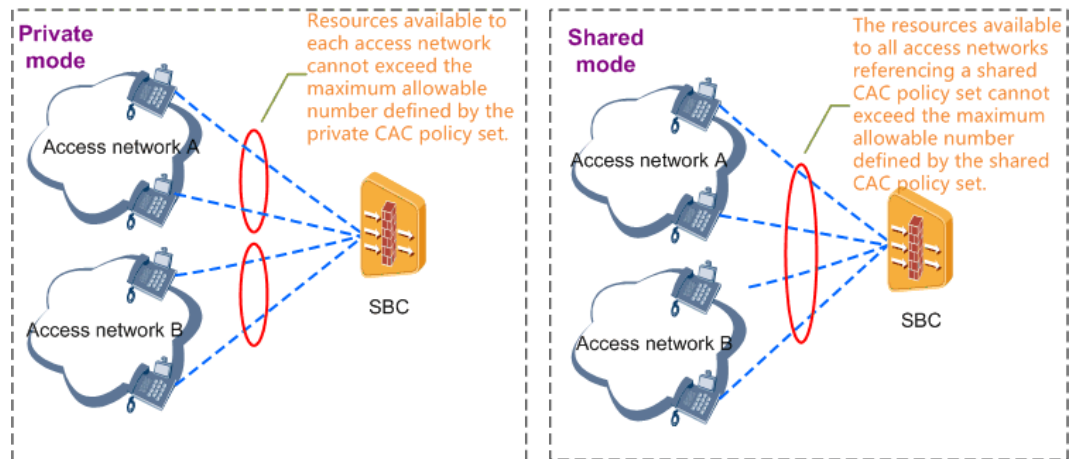
The SE2900 supports manually configured blacklists and whitelists, which enable flexible management of signaling attack defense.

- **Blacklist:** The SE2900 blacklists a specified IMPU permanently and discards all packets from the IMPU. After the SE2900 determines that an IMPU has security threats and prohibits this IMPU to use services permanently, this IMPU can be manually blacklisted.
- **Whitelist:** The SE2900 whitelists a specified IMPU so that the signaling attack defense module does not restrict the rate of the packets from this IMPU. Generally, very important person (VIP) users are added to the whitelist and their service requests are preferentially processed by the SE2900. In addition, if traffic on the core network often exceeds the signaling attack defense threshold because of traffic bursts, the IP address of the core server can also be whitelisted to prevent the packets from the core network from being discarded.

CAC

Based on local call admission control (CAC) policies, the SE2900 restricts the resources available to services such as registration, call, and subscription. A CAC policy set has private and shared modes. Figure 4-68 shows the CAC mechanism.

Figure 4-68 CAC



- Resources associated with a private CAC policy set are exclusive to the objects referencing this CAC policy set.
- Resources associated with a shared CAC policy set are shared by all the objects referencing this CAC policy set.

Media Flow Control

The SE2900 provides session-based QoS assurance for real-time sessions. The SE2900 allocates fixed bandwidth for each codec type used in a call to prevent bandwidth theft.

Each codec type consumes a fixed amount of bandwidth. In addition, the payload size and IP packet header of a codec are fixed. The SE2900 controls bandwidth use in a session based on the codec type of this session.

Media Latching Attack Defense

The SE2900 provides media latching attack defense when a network address translation (NAT) device is deployed between UEs and the SE2900. After signaling exchange, upon receiving the first media packet from a UE behind the NAT device, the SE2900 extracts the source IP address + port carried in the packet after NAT. Then the SE2900 replaces the source IP address + port in the access-side 5-tuple created in signaling exchange with the obtained transport-layer source IP address + port after NAT and enables the pinholing firewall function.

Attackers send Real-Time Transport Protocol (RTP) packets to the media IP address + port of the SE2900. If the destination IP address + port of attack packets is the same as the IP address + port of a media packet that requires media latching. The SE2900 discards the media packets.

4.4.23 Redundancy of Core Network

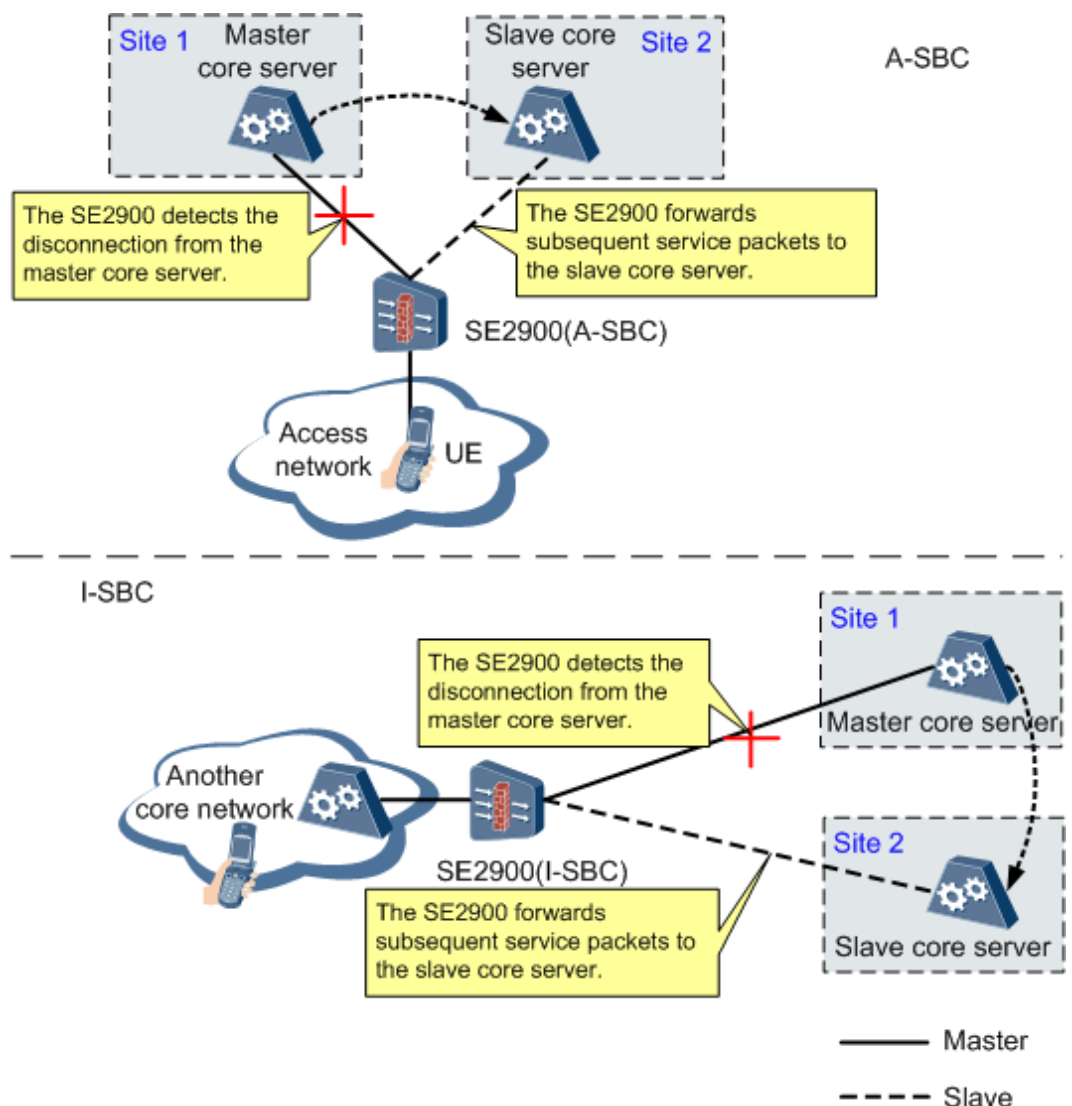
Redundancy is a proactive mechanism that minimizes the impact of system failures on service availability and data reliability. With the redundancy of core network feature, core servers can be deployed at two sites in different locations. When one site becomes unavailable due to unpredictable factors, such as natural disasters or power failures, the other site takes over to provide registration and call services. Core servers that connect to the SE2900 usually work in redundancy and are deployed at different sites. The SE2900 periodically sends detection messages to the core servers to monitor connectivity. When a core server becomes unavailable, the SE2900 redirects the traffic of affected services to other available core servers.

This feature provides a geographical disaster tolerance solution for carriers, which ensures service continuity and minimizes service loss caused by single point of failures on the core network. Dual-homing and pool are the two networking modes most commonly used to implement the redundancy of core network feature. The two modes both support automatic and manual switchovers and switchbacks.

Dual-homing

The SE2900 is homed to two core servers that work in master/slave mode. Normally, the SE2900 is controlled and managed by the master core server. The SE2900 periodically sends SIP OPTIONS messages to detect the link status between the SE2900 and core servers. When the master core server fails, the slave core server takes over all services from the master core server, as shown in Figure 4-69.

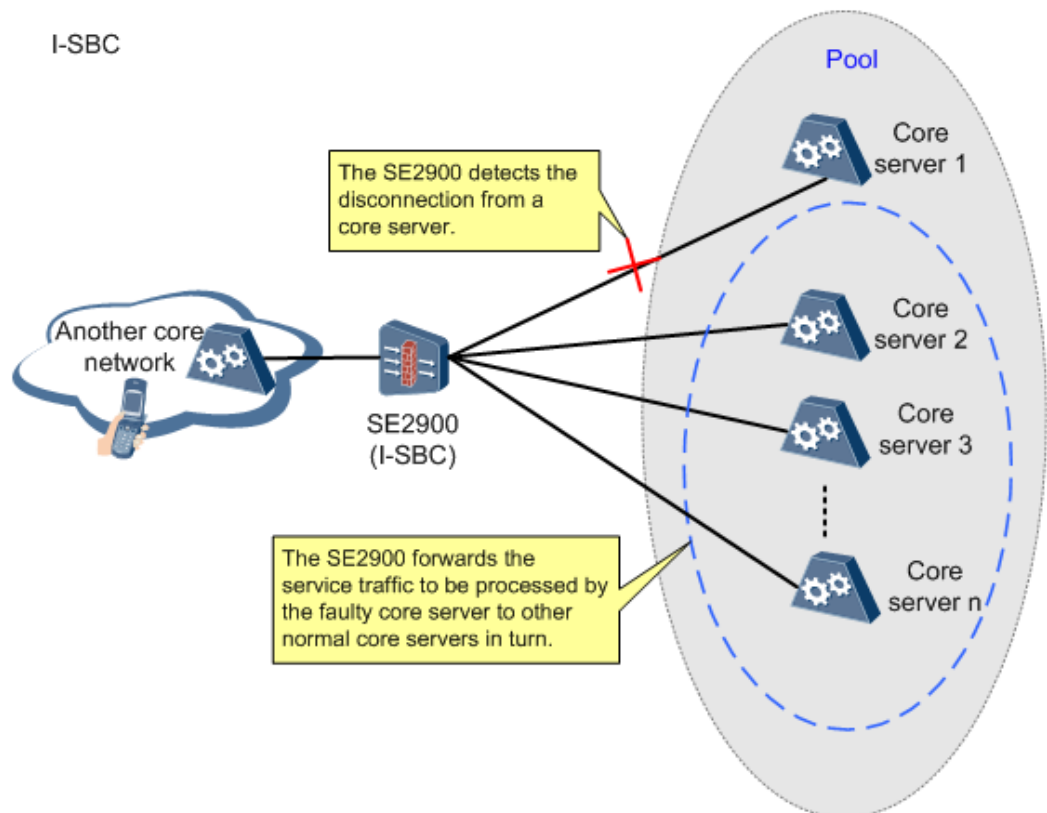
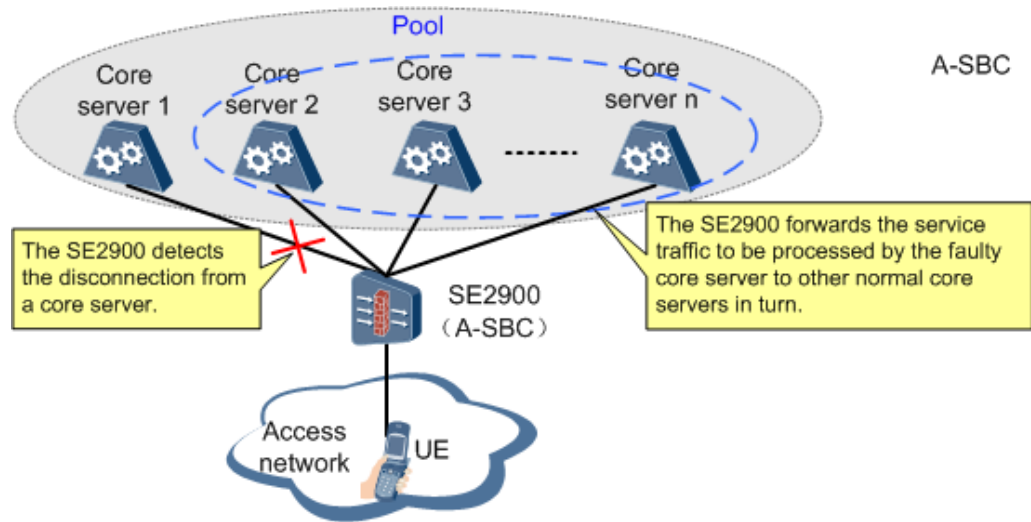
Figure 4-69 Dual-homing



Pool

The SE2900 is homed to a pool of core servers that work in load-balancing mode. Normally, the SE2900 balances loads between the core servers in the pool. The SE2900 periodically sends SIP OPTIONS messages to detect the link status between the SE2900 and the core servers in the pool. When a core server fails, the SE2900 distributes its load to other available core servers in the pool, as shown in Figure 4-70.

Figure 4-70 Pool



4.4.24 SIP-H.323 Interworking

The SIP-H.323 interworking feature is a function that enables the SE2900 to provide basic and supplementary services between IMS/NGN and H.323 networks.

The SIP-H.323 interworking feature achieves two functions: interworking between the IMS/NGN and H.323 networks and enabling H.323 UEs to access an IMS conference. Figure 4-71 shows the typical networking for the interworking between the IMS/NGN and H.323 networks. Figure 4-72 shows the typical networking for enabling H.323 UEs to access an IMS conference.

Figure 4-71 Networking for the interworking between the IMS/NGN network and the H.323 network

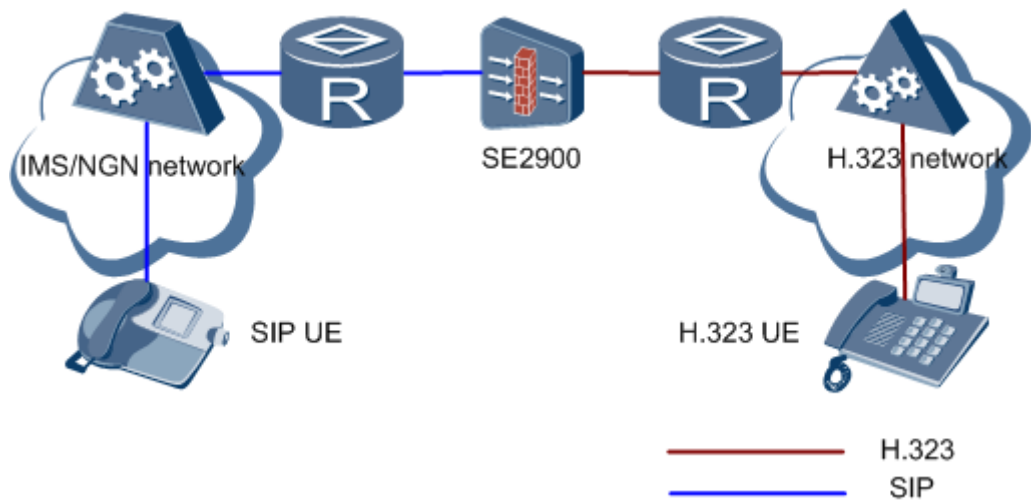
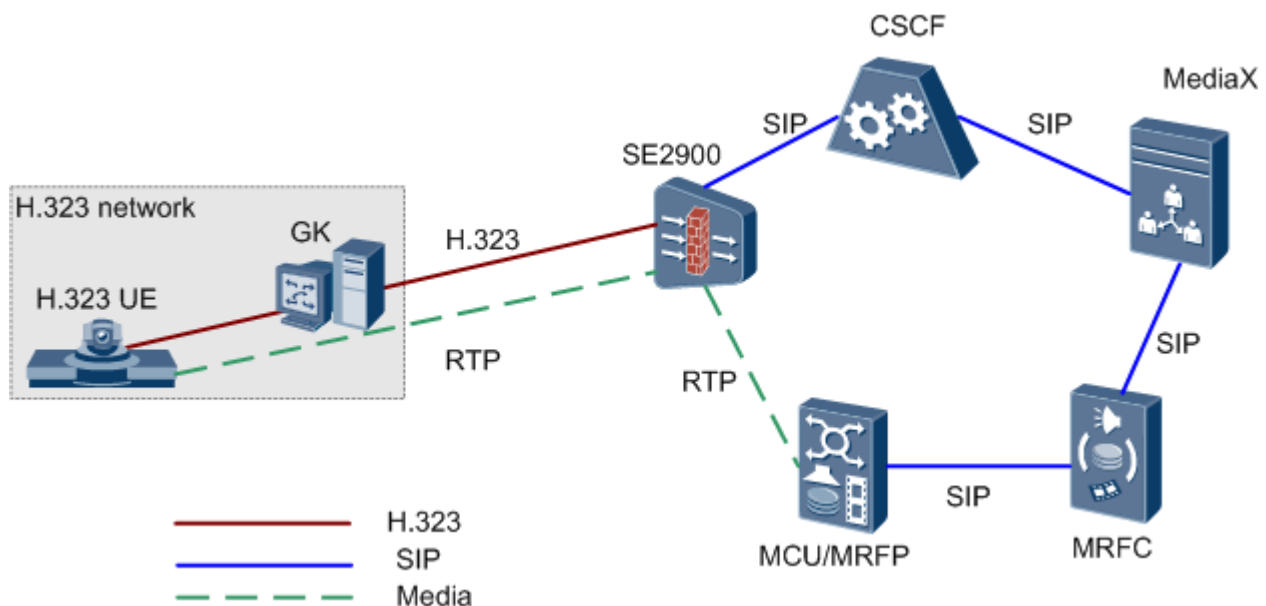


Figure 4-72 Networking for enabling H.323 UEs to access an IMS conference



In the networkings shown in Figure 4-71 and Figure 4-72:

- The SE2900 supports dual-system hot backup but does not support call information backup.
- The SE2900 supports IMS/NGN network dual-homing but not H.323 network dual-homing.
- The SE2900 supports SIP OPTIONS messages on the IMS/NGN network.
- The SE2900 does not support heartbeat messages on the H.323 network.
- The SE2900 supports SIP-I-H.323 interworking.
- The H.323 network supports both peer trunk networking and non-peer trunk networking. On the H.323 network, the call signaling addresses of the called side are obtained from the (Registration Admission and Status) RAS message.
- The SE2900 supports media negotiation in fast start, normal start, or H.245 tunnel mode.

Table 4-4 lists the services supported by the SE2900 in the SIP-H.323 interworking scenario.

Table 4-4 Services supported by the SE2900 in the SIP-H.323 interworking scenario

Service Type	Description
Basic services	<ul style="list-style-type: none"> • Call services between SIP and H.323 networks in fast start or normal start mode • The SE2900 supports the following codecs on SIP and H.323 network sides: <ul style="list-style-type: none"> – Audio codecs: G.711A, G.711μ, G.722, G.728, G.723.1, G.729A, and G.729 – Video codecs: H.261, H.263, and H.264 • The SE2900 supports audio transcoding on the SIP network side. For the codecs that can be converted, see 4.4.20 Audio Transcoding. • Fax services The H.323 network supports only T.38 fax services. The SE2900 supports the conversion between T.38 fax services on the H.323 network and G.711 fax services on the SIP network. • DTMF digit collecting
Supplementary services	<ul style="list-style-type: none"> • Video call, camera control, and auxiliary stream services • Session timer negotiation on the SIP network • Flexible routing An H.323 UE initiates a call to a SIP UE. If the call fails, the SE2900 reroutes the call only to a non-H.323 trunk group.

Service Type	Description
	<ul style="list-style-type: none"> • Call forwarding • No media stream detection • I frame update • PT value conversion • QoS reporting
Conference-related services	Enabling H.323 UEs to access an IMS conference

4.4.25 Standard Definition/High Definition Video

The popularization of VoLTE technologies accelerates the development of multimedia services, such as high definition (HD) audio calls, HD video calls, and instant messages, which gradually replace legacy audio calls and pave the way for diversified video services. Although standard definition (SD)/HD video services greatly improve user experiences, the bandwidth resources consumed by such services increase phenomenally. For example, an H.264 720P HD video consumes the bandwidth of over 1 Mbit/s. Massive concurrent video calls exhaust bandwidth resources on wireless and core networks, resulting in network performance deterioration or even network congestion. To resolve such an issue, the SE2900 implements controls over the number of concurrent video calls, ensuring experience of VIP users even in network congestion.

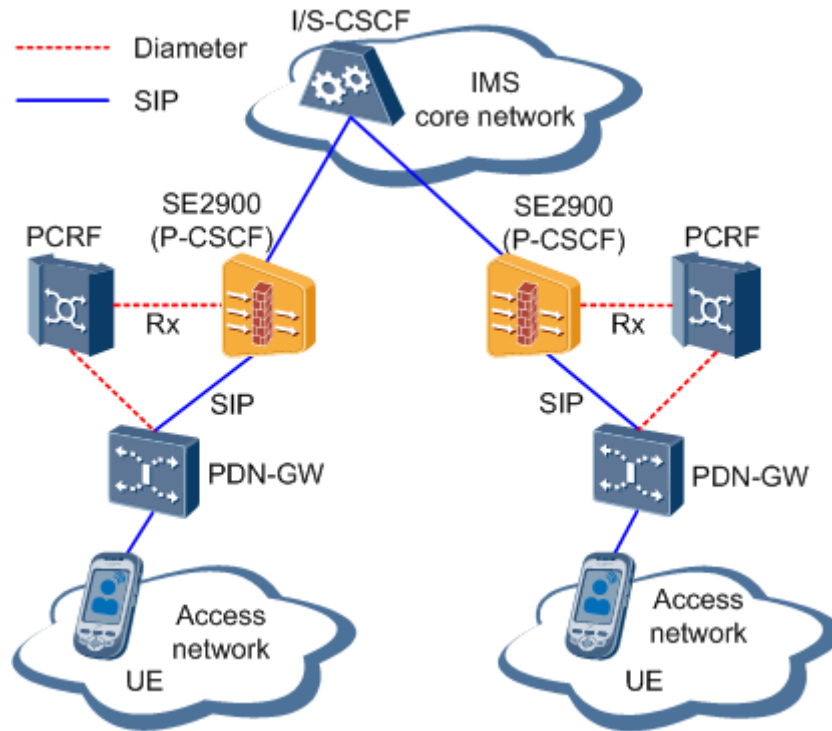


NOTE

Currently, videos are classified into common, SD, and HD videos, and they are explained as follows:

- A common video has a resolution of less than 640 x 480. Videos in QVGA format are common videos.
- An SD video has a resolution of greater than or equal to 640 x 480 but less than 1280 x 720. Videos in VGA format are SD videos.
- An HD video has a resolution of greater than or equal to 1280 x 720. Videos in 720P format are common videos.

Figure 4-73 Networking for VoLTE SD/HD video control



4.4.26 Dual-System Hot Backup

Nowadays, users have higher requirements for service continuity. The SBC is deployed between the access network and core network or two different core networks. In the presence of a single SBC, if it is faulty, the services on the entire network will be interrupted. To avoid that, the redundancy mechanism is adopted to improve the stability and reliability of the whole system.

The SE2900 supports the dual-system hot backup feature to ensure service reliability. This feature provides a geographic redundancy solution for carriers. When one SE2900 becomes faulty, the other SE2900 replaces the faulty SE2900 to process services, enabling users to use services without interruptions.

Figure 4-74 shows the remote dual-system hot backup networking.

Figure 4-74 Remote dual-system hot backup networking

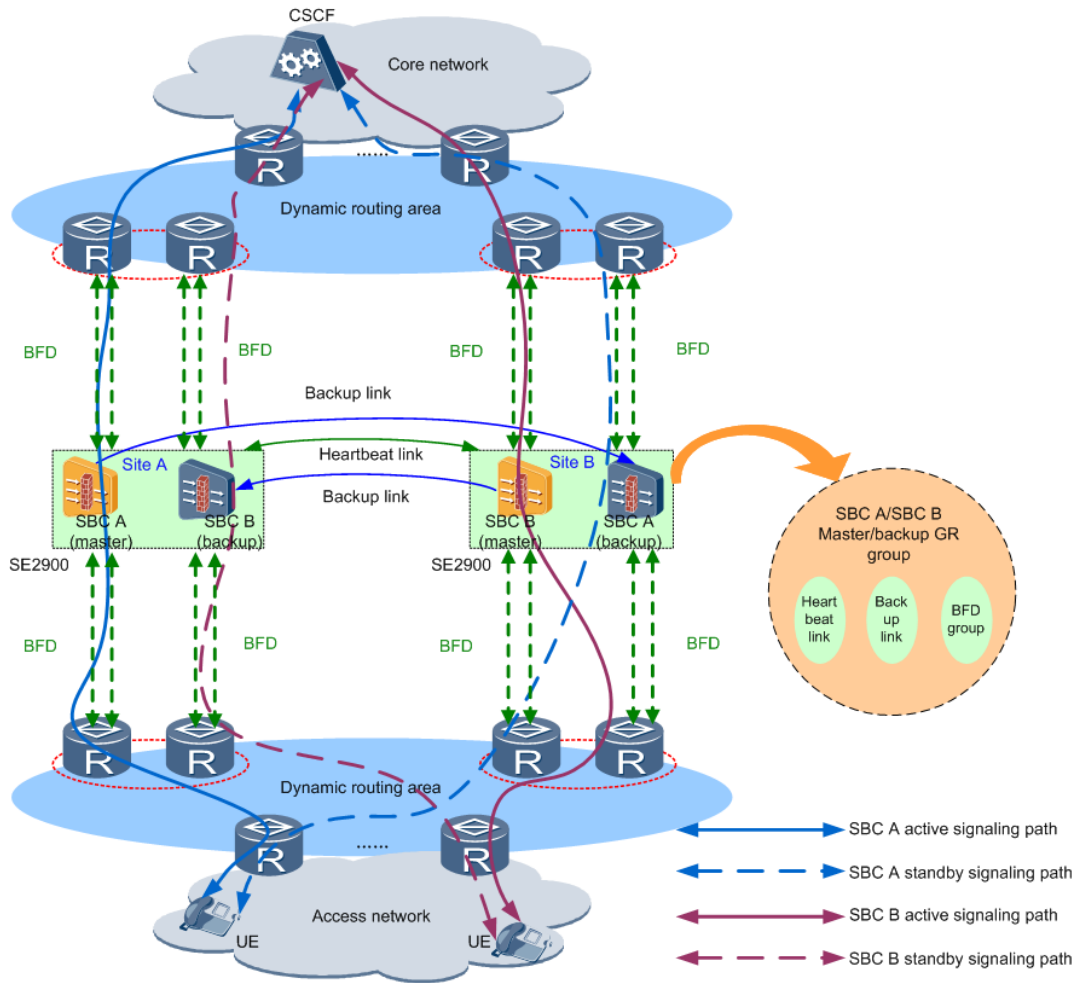
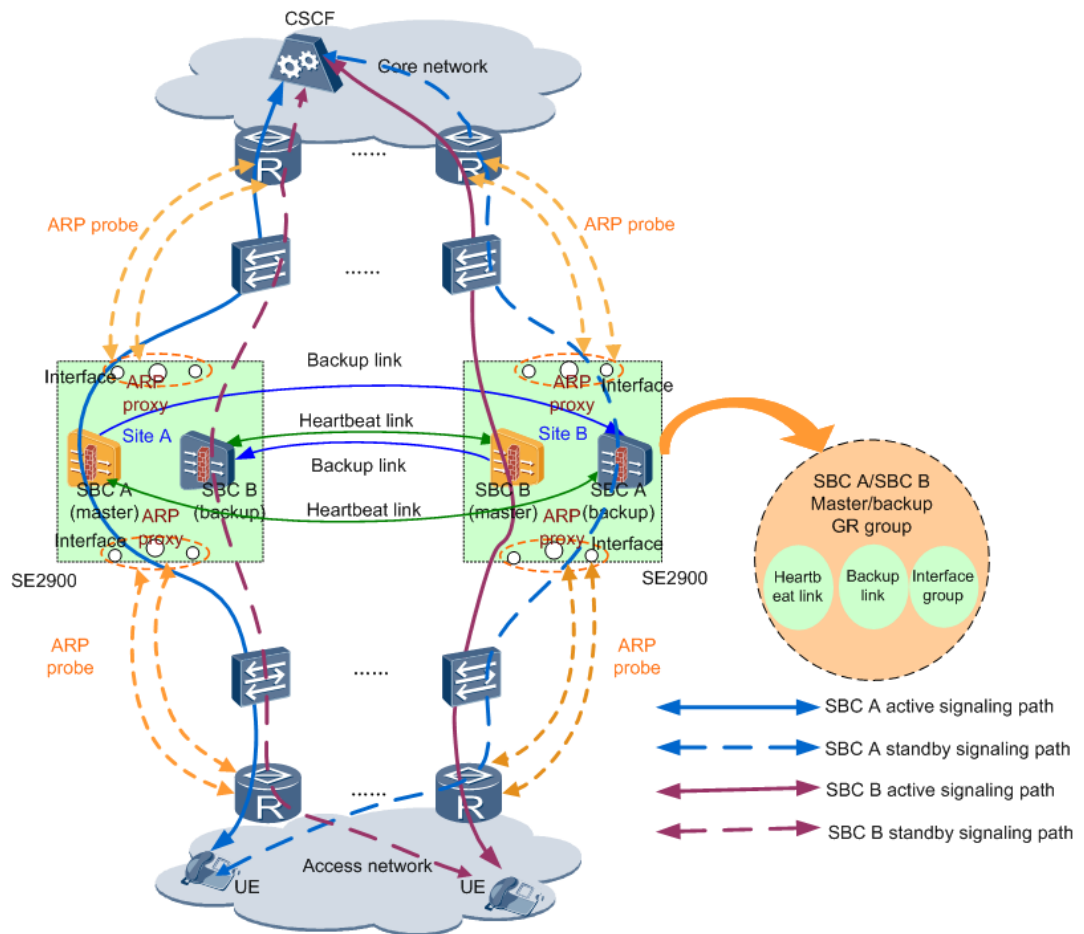


Figure 4-75 shows the local dual-system hot backup networking.

Figure 4-75 Local dual-system hot backup networking



The dual-system hot backup feature has the following advantages:

- Master/backup geographic redundancy (GR) groups use a uniform service IP address. No new service IP address needs to be planned, saving IP addresses.
- Shortens new service access time. When the master SE2900 becomes faulty, new service access time is shortened to 3 seconds. When two SE2900s are deployed in different equipment rooms (remote dual-system hot backup), new service access time is shortened to 30 seconds.
- In remote dual-system hot backup, Ethernet interface load-balancing mode + Bidirectional Forwarding Detection (BFD) is used. Only registration data is backed up from the master SE2900 to the backup SE2900. In local dual-system hot backup, Ethernet interface active/standby mode + Address Resolution Protocol (ARP) is used. Both registration and call data is backed up from the master SE2900 to the backup SE2900. During a master/backup switchover, signaling is transmitted using SIP over UDP; Real-Time Transport Protocol (RTP) calls are not interrupted.
- In local dual-system hot backup, a pair of GR groups supports link and process fault detection. A master/backup switchover occurs according to switchover policies.
- Reliability networking can adapt to carriers' different networking modes. GR groups are used as smallest units in dual-system hot backup.
- SE2900's version upgrade time is shortened. Cross-version registration data backup is also supported.

4.4.27 Security Traversing Gateway

As the development of the rich communication suite (RCS) service, IMS services become available on PCs and smart UEs as the HTTP/HTTPS services. However, the availability of IMS services on PCs and smart UEs poses the following two issues:

- If an HTTP or socket proxy server is used to connect to the public network, the proxy server only forwards HTTP/HTTPS service streams. RCS data packets are discarded, which renders the IMS service unavailable.
- If a firewall is deployed at the border between the intranet and public network, and the firewall permits port 443 (HTTPS) or 80 (HTTP), signaling and media data packets cannot traverse the firewall, causing IMS service failures.

To ensure that RCS service packets can traverse the HTTP proxy or firewall deployed at the borders of enterprise networks, the security traversing gateway is enabled on the SBC and the RCS client is enabled to encapsulate/decapsulate signaling and media packets, as shown in Figure 4-76 and Figure 4-77.

Figure 4-76 Networking with an embedded STG

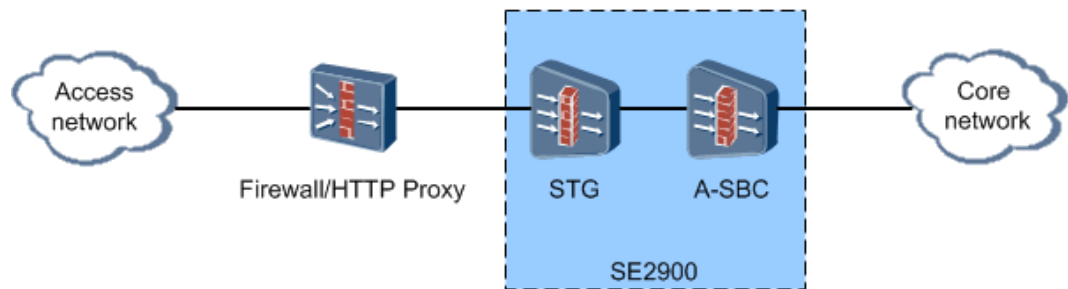


Figure 4-77 Networking with a standalone STG



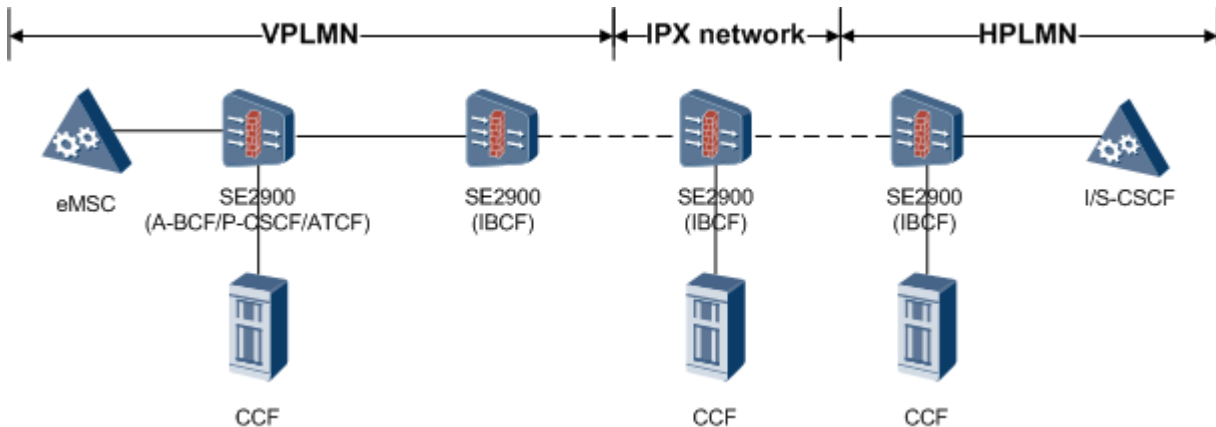
When firewall traversal is used, a firewall on an intranet needs to permit only a few ports, such as port 443, for RTP packets to ensure that VoIP data packets traverse the firewall or HTTP proxy server. In addition, the RCS client encapsulates SIP/RTP packets into HTTPS packets and transmits the encapsulated packets through port 443 of the firewall using TLS/DTLS.

4.4.28 VoLTE Roaming

The SE2900 enables VoLTE users to use roaming services on the IMS network without having to fall back to the 2G/3G network based on 3GPP and Global System for Mobile Communications Association (GSMA)'s standards.

Figure 4-78 shows VoLTE roaming networking.

Figure 4-78 VoLTE roaming networking



VoLTE roaming must support the following functions for commercial use:

- The P-CSCF supports roaming registration, roaming restriction, and roaming charging, and allows including the transit and roaming function (TRF) parameter. The access transfer control function (ATCF) supports enhanced single radio voice call continuity (eSRVCC) handovers for roaming users.
- The I-SBC supports the roaming license, roaming registration, roaming call, roaming restriction, number change, TRF, and roaming charging.
- The I-SBC supports optimal media routing (OMR) that enables media streams to be transmitted directly between VoLTE UEs (at least one is the roaming UE), improving media quality.

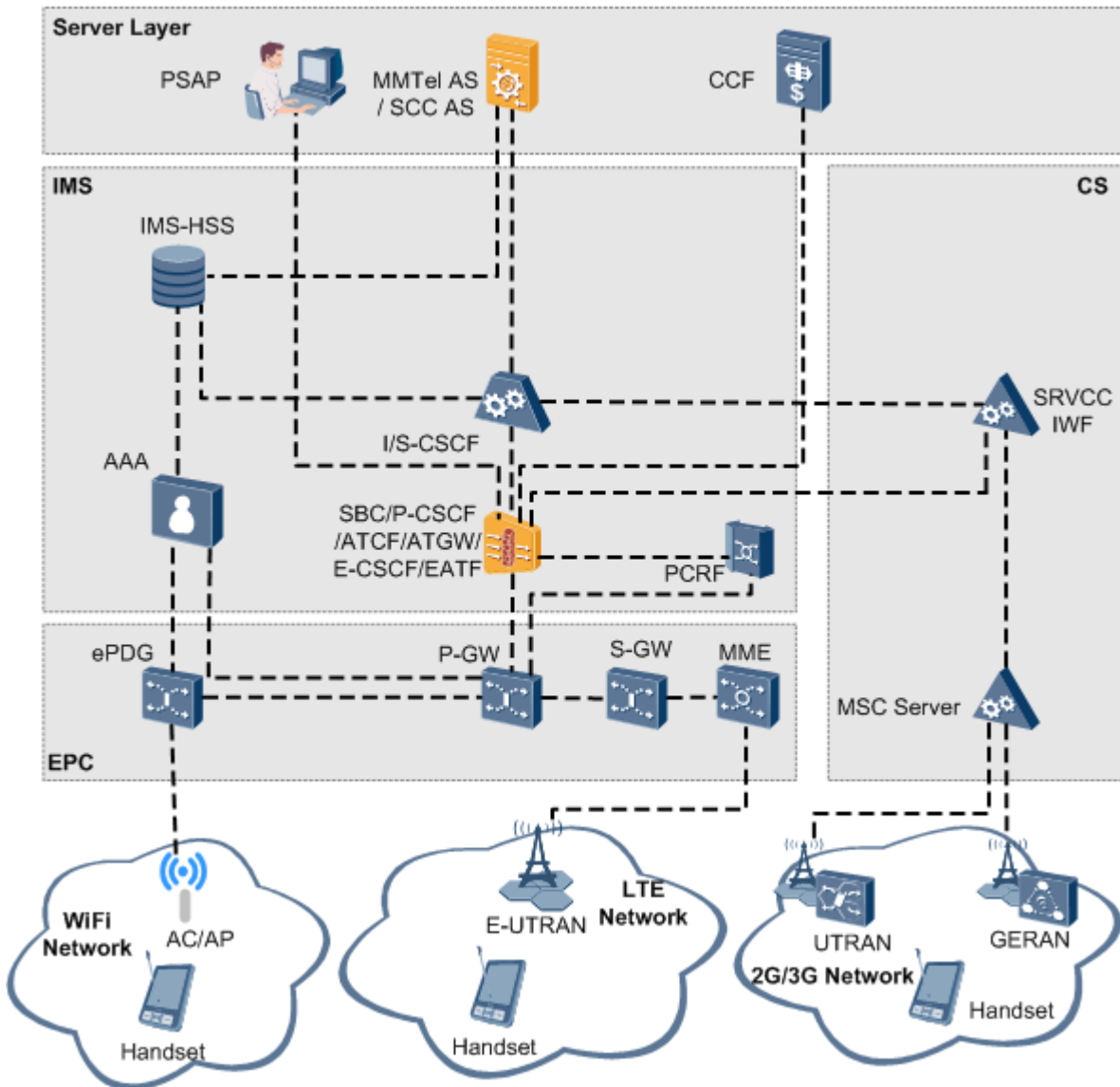
4.4.29 VoWiFi Access

The SE2900 supports the voice over Wi-Fi (VoWiFi) service in the VoLTE solution. In the VoWiFi service, UEs access the IMS network over Wi-Fi. The SE2900 supports the following functions:

- Identifies the access network type (Wi-Fi or LTE network) and notifies the core network of the access network type so that the core network performs distinctive charging for users.
- Restricts VoWiFi roaming services.
- Searches for a public safety answering point (PSAP) based on the longitude and latitude information or P-Cellular-Network-Info header carried in a UE-originated SIP message.

Figure 4-79 shows VoWiFi access networking.

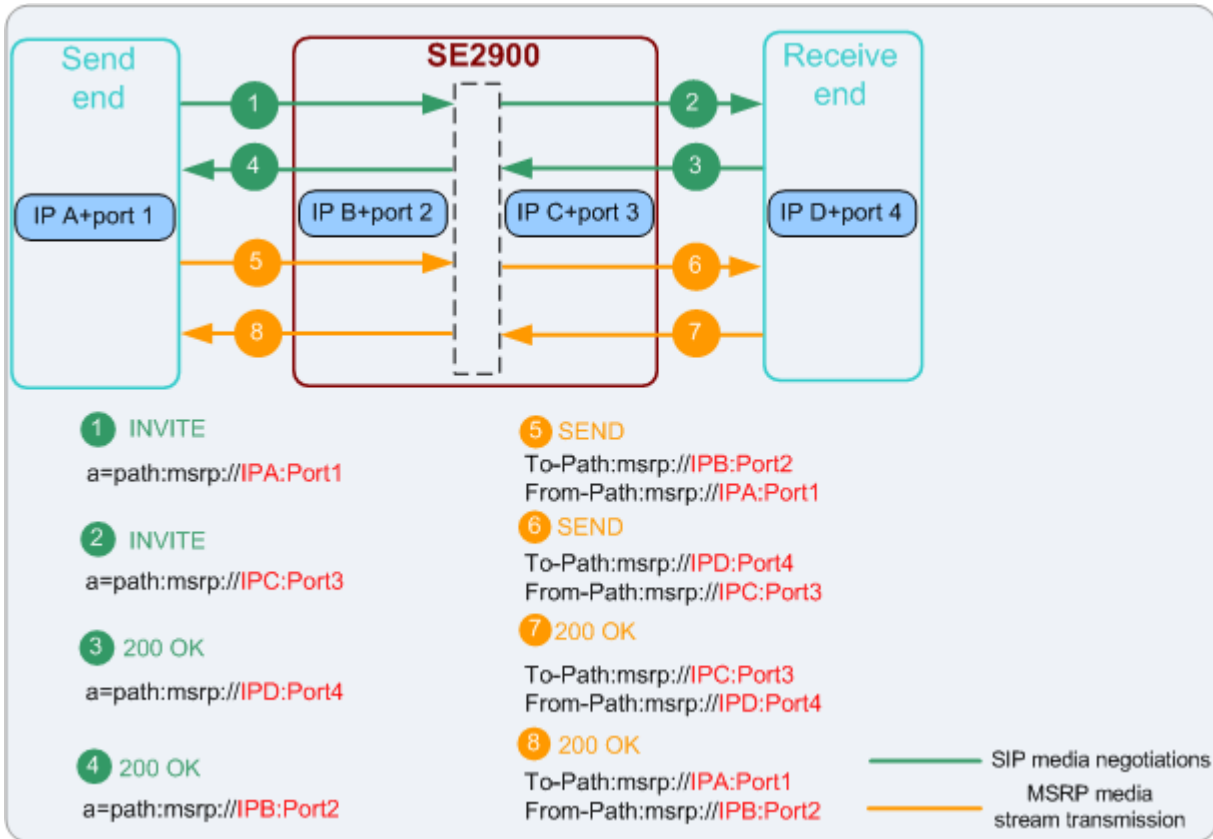
Figure 4-79 VoWiFi access networking



4.4.30 MSRP B2BUA

The SE2900 can terminate Message Session Relay Protocol (MSRP) over TCP streams, modify MSRP packet header contents, and forward MSRP media in B2BUA mode for complete topology hiding. See Figure 4-80.

Figure 4-80 MSRP B2BUA



The MSRP B2BUA applies to A-SBC and I-SBC scenarios and implement the following functions:

- Achieves independence of RCS UEs on ASs, which increases the flexibility in choosing RCS UEs and ASs.
- Hides the complete network topology to protect the SE2900 from network attacks.
- Terminates MSRP over TCP streams and provides basic capabilities for functions such as MSRP traffic measurement and charging.

5 Product Architecture

About This Chapter

- [5.1 Hardware Structure](#)
- [5.2 Software Architecture](#)

5.1 Hardware Structure

5.1.1 Physical Structure

Cabinet

The SE2900 uses the N68E-22 cabinet with the dimensions of 2200 mm x 600 mm x 800 mm (height x width x depth). Figure 5-1 shows the appearance of the N68E-22 cabinet.

Figure 5-1 N68E-22 cabinet



The N68E-22 cabinet has the following highlights:

- The available space in the N68-22 cabinet is 46 U (1 U = 44.45 mm = 1.75 in.). The cabinet is composed of the power distribution frame (PDF), F8002 subrack, cable subrack, filler panel, and rack, and can meet the requirement for flexible module configuration.
- The cabinet supports -48 V DC power supply. The design of the cabinet complies with IEC 297 standards. The cabinet adopts a modular design that facilitates expansion and maintenance.
- Electromagnetic compatibility (EMC) is considered in cabinet design. All interfaces are well protected from electromagnetic effect. The N68-22 cabinet can be installed either on the electrostatic discharge (ESD) floor or directly on the concrete floor. When the N68E-22 cabinet is installed on the ESD floor, N6X supports must be used.



NOTE

N6X supports are made of welded steel plates. Before the whole set of equipment is grounded, insulation plates must be installed under the supports and insulating coverings must be added to the expansion bolts to meet the insulation requirements.

- The front and rear doors and bottom plate have air filters inside, which protect the cabinet against dust. The cabinet is equipped with vents on the front and rear doors and bottom plates (50% perforated rate) and has good heat dissipation performance.

Subrack

The SE2900 uses the F8002 subrack (3U high) and six slots, as shown in Figure 5-2, Figure 5-3, and Figure 5-4. OMUs must be inserted in slots 2 and 5, SPU's must be inserted in slots 1, 3, 4, and 6, and VPUs must be inserted in slots 1, 3, 4, and 6.

Figure 5-2 Appearance



Figure 5-3 Front view

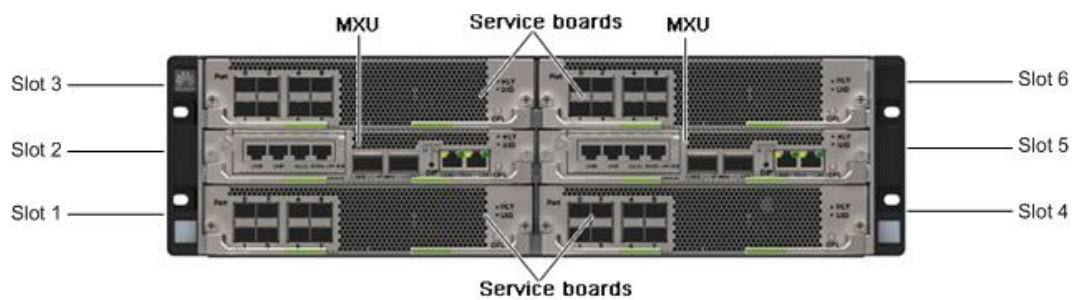
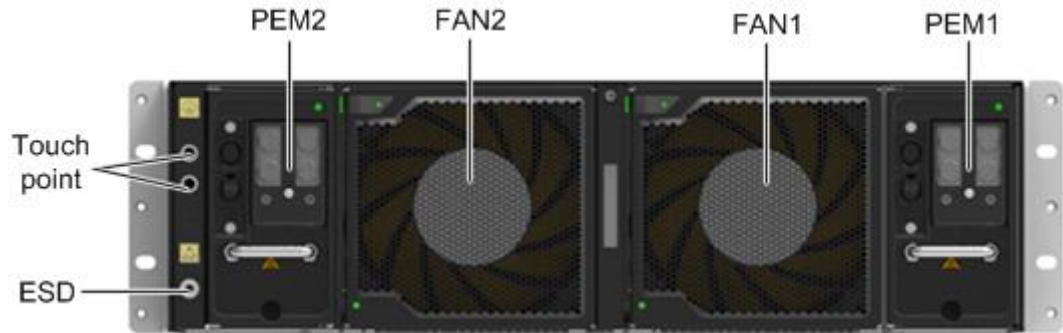


Figure 5-4 Rear view



The subrack uses DC-input power supply and supports 1+1 redundancy power entry modules (PEMs). The maximum through-current of each input is 60 A. After completing the filtering, surge protection, and overcurrent protection of -48 V power supply, PEMs input the power to the backplane, providing 1+1 redundancy power supplies for boards.

The subrack comprises two fan modules that support 1+1 redundancy. The subrack uses the front-in and back-out mode to dissipate heat, ensuring that the system can operate in temperatures ranging from 0°C to 45°C for a long time.

Boards

Table 5-1 lists the types of boards on the SE2900.

Table 5-1 Board types

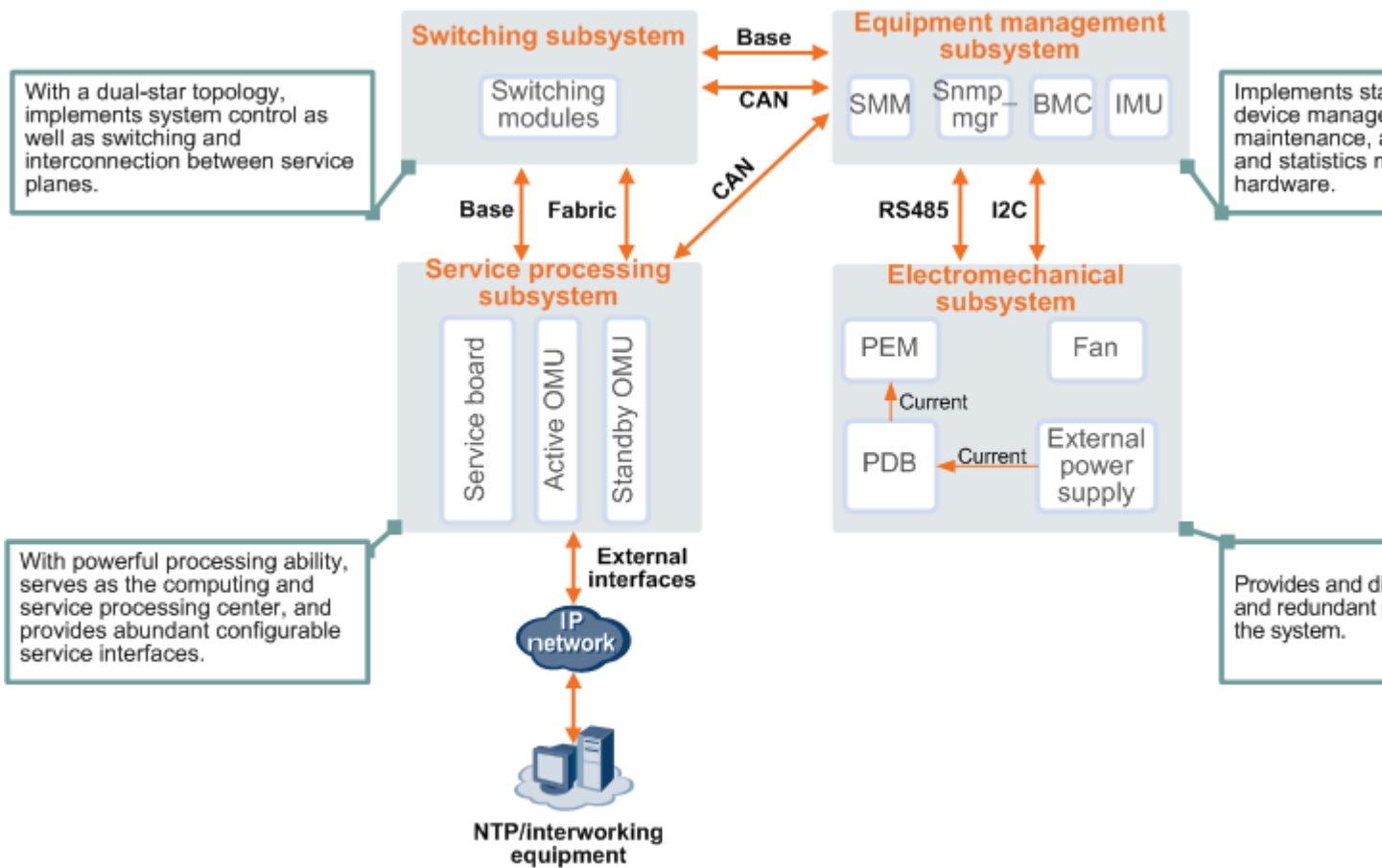
Physical Board	Full Name	Quantity	Remarks
MXUA0	Multi-Function and Switch Unit A0	2	<p>MXUA0 is the core board for system management and service switching/data exchanges and must be inserted in slots 2 and 5.</p> <p>MXUA0 implements power supply control, fan management, and power distribution management. MXUA0 manages the SPU by communicating with baseboard management controller (BMC) modules on the SPU.</p> <p>Each master subrack can be used in conjunction with two backup subracks through cascading interfaces on MXUA0 to implement three-subrack cascading. In each subrack, the cascading bandwidth of the Base plane is 1 Gbit/s, and the cascading bandwidth of the Fabric plane is 40 Gbit/s.</p>
SPUA0/S PUA1/SP UZ0	Service Processing Unit A0/A1/Z0	2	<p>SPUs are service forwarding and processing boards and must be inserted in slots 1, 3, 4, and 6. The SPUs in slots 1 and 4 or slots 3 and 6 operate in active/standby mode.</p> <p>SPUs support service processing, interface, and board management functions. SPUs can be</p>

Physical Board	Full Name	Quantity	Remarks
			<p>classified into three types: SPUA0, SPUA1, and SPUZ0, which are similar in functions, appearances, interfaces, indicators, and technical specifications. The letters "A" and "Z" specify board versions and the digits "0" and "1" specify board models to distinguish between boards that have the same functions but slightly different configurations. The differences among SPUA0, SPUA1, and SPUZ0 are as follows:</p> <ul style="list-style-type: none"> • SPUA0: provides one CPU and one Cave Creek module • SPUA1: provides two CPUs and two Cave Creek modules • SPUZ0: provides one CPU and one Cave Creek module
VPUA0/V PUA1	Voice and Video Process Unit A0/A1	2	<p>VPUA0/VPUA1 are media processing boards and must be inserted in slots 1, 3, 4, and 6. One VPU occupies a half slots.</p> <p>VPUA0/VPUA1 support media processing, interface, and board management functions. VPUA0/VPUA1 can be classified into VPUA0 and VPUA1 based on the number of digital signal processor (DSP) daughter boards on them. VPUA0 and VPUA1 are similar in functions, appearances, interfaces, indicators, and technical specifications. The letter "A" specifies the version and the digits "0" and "1" specify the board models to distinguish between boards that have the same functions but slightly different configurations. The differences between VPUA0 and VPUA1 are as follows:</p> <ul style="list-style-type: none"> • VPUA0: provides one DSP daughter board • VPUA1: provides two DSP daughter boards

5.1.2 System Architecture

In the whole system, the switching subsystem acts as the pivot and the service processing subsystem acts as the core. These two subsystems, together with the electromechanical subsystem and equipment management subsystem, form a powerful service processing platform. Figure 5-5 shows the system logic architecture.

Figure 5-5 System logical architecture



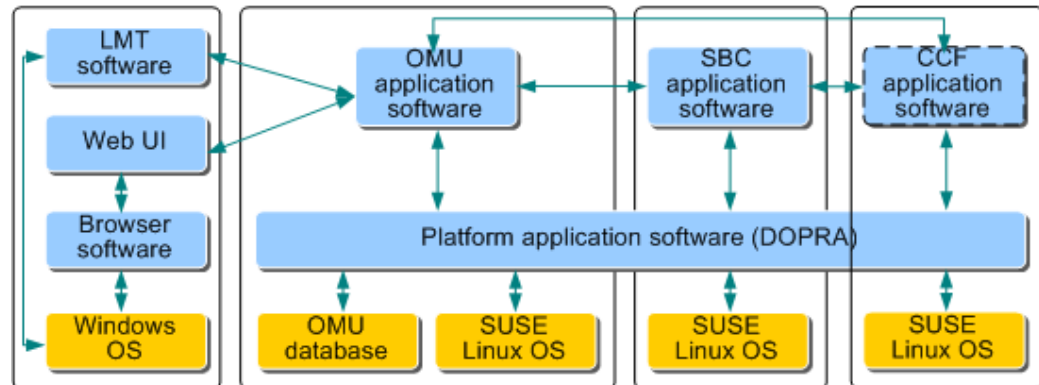
Fabric: Transmits service data in the system.
Base: Manages subracks, and provides a channel for software loading, alarm reporting, and maintenance message delivery.
CAN: As one of the system buses, transmits service data in the system.
RS485: Connects the MXU management unit to the fan, monitors fan status, and adjusts fan speed.
I2C: Is used for the communication between power entry modules (PEMs) on the MXUs, and monitors the input power supply status in a subrack.
BMC: Baseboard management controller on each processor board.
SMM, snmp_mgr: Device management unit process
IMU: I/O board management unit process

5.2 Software Architecture

Overall Architecture

The SE2900 software consists of platform software (including OMU application software and LMT software) and application software. Figure 5-6 shows the overall SE2900 software architecture.

Figure 5-6 Overall software architecture



The OMU and SPU use the Linux operating system and the following software:

- Platform software: in cooperation with the LMT/WebUI client, platform software responds to operation commands delivered by maintenance personnel and performs software data management, device management, alarm management, performance measurement, and signaling trace.
 - OMU application software: runs on the Multi-Function and Switch Unit A0 (MXUA0), functions as the communication and database server, and is the core of operation, administration and maintenance (OAM) software. The OMU application software forwards operation and maintenance (O&M) commands delivered by the LMT/WebUI client to the host and directs the responses or operation results returned by the host to the LMT/WebUI client.
 - LMT application software: runs on the Windows operating system (OS) of the PC hardware platform, functions as the client connecting to the OMU server, and provides man-machine language (MML)-based graphical terminal. The LMT can be used both locally or remotely, for example, the LMT allows dial-up access to the OMU server through the wide area network (WAN). Users can use the LMT to perform data maintenance, device management, alarm management, call and signaling trace, and report generation.
 - WebUI: runs on browsers in the Windows OS, and enables users to use performance management functions and upgrade tools, and download OMU clients.
- SE2900 application software refers to the processes that are running on SPUs/VPUs. For details, see [SE2900 Service Processes](#).
- CCF application software refers to the processes that are running on MXUA0s and is installed in the Linux operating system. CCF application software is optional. When the SE2900 is used for charging, apply for a license for charging and then install the CCF application software. Different modules are designed for different services. Modules with associated service functions are combined into a service process. Different

processes communicate with each other in client/server mode, with one process managing the others. For details, see [CCF Service Processes](#).

SE2900 Service Processes

Service Processes

The SE2900 provides open and standard protocol interfaces. These interfaces support multiple protocols and enable the SE2900 to interwork with multiple types of devices, as shown in Figure 5-7.

Figure 5-7 Service processes

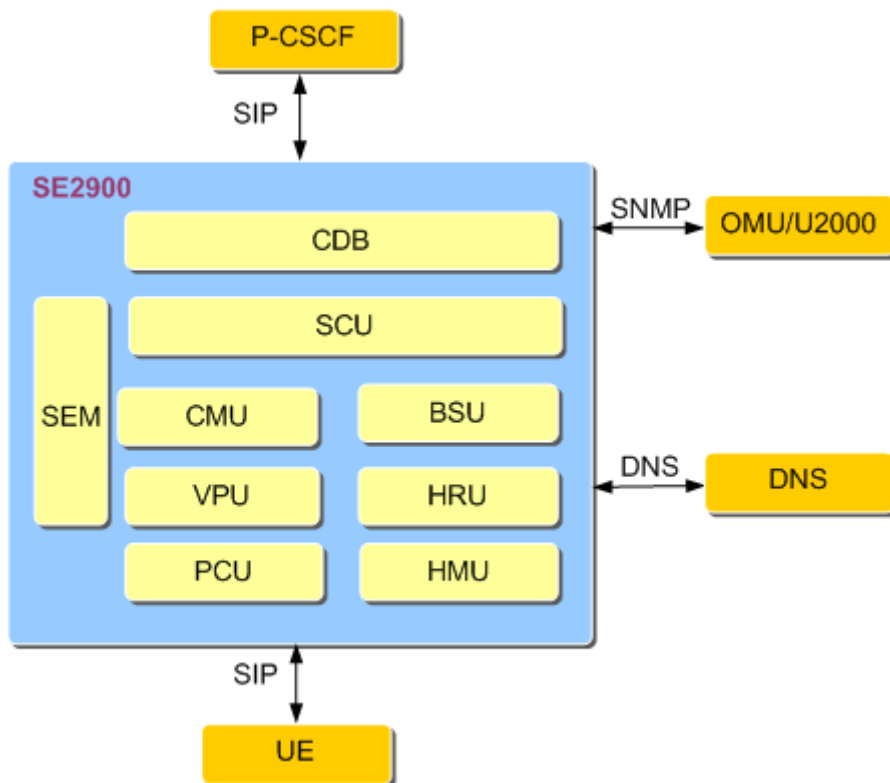


Table 5-2 describes the functions and protocols of SE2900 service processes that are shown in Figure 5-7.

Table 5-2 SBC service processes

Process Name	Function Description	Operating Mode
Central Database (CDB)	Serves as the subscriber data management module of the SCU and manages subscriber distribution data.	Only a pair of active and standby CDBs can be configured for each ME.
Security Management (SEM)	Performs system security defense, delivers security policies to processes, collects security reports	Only a pair of active and standby SEMs can be configured for each ME.

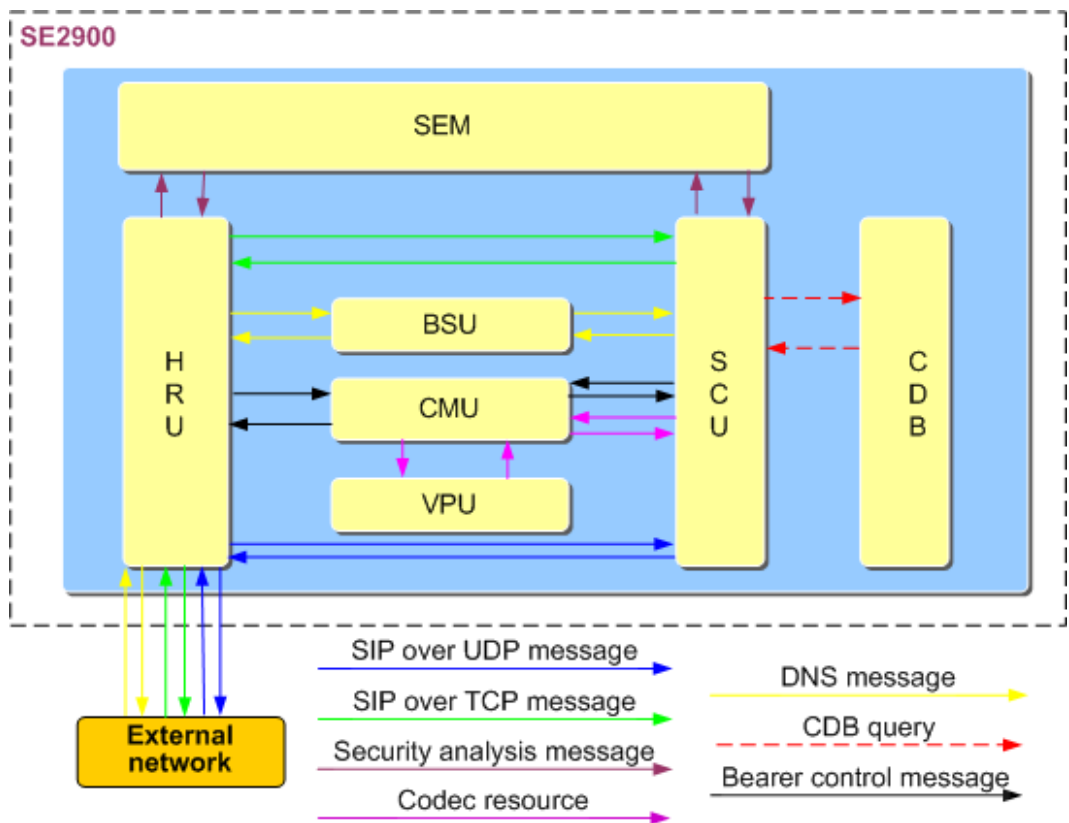
Process Name	Function Description	Operating Mode
	reported by the processes, and intercepts untrusted messages.	
Connection Maintenance Unit (CMU)	Processes the services related to calls and managing call connections for other modules.	CMUs work in active/standby mode.
Highspeed Routing Unit (HRU)	Forwards signaling messages (for example, SIP messages) and processes media messages (for example, SRTP, RTP, and MSRP messages) under the control of CMU.	Only one HRU can be configured on each board. The HRUs on active/standby boards work in active/standby mode.
Packet Control Unit (PCU)	Manages IP forwarding and control.	PCUs work in active/standby mode.
Broadband Signaling Unit (BSU)	Functions as the fixed link (DNS) protocol processing and forwarding module, and processes IP, TCP, and SCTP messages.	BSUs work in load-balancing mode.
Highspeed-Routing Management Unit (HMU)	Manages hardware (for example, FPGA, ports, and DSP) dedicated for media forwarding, manages hardware configurations, and detects hardware status. When the HMU process finds that the hardware configuration or status has changed, it informs other processes of the change. For example, if a physical port fails, the HMU process informs the PCU process of the failure. Then the PCU process updates the routing information about the port and sends the updated routing information to the HRU process. The HRU process can route the new messages destined for the failed port to other processes.	Only one HMU can be configured on each SPU. The HMUs on active and standby SPUs work in load-balancing mode. Only one HMU can be configured on each VPU. The HMUs on all VPUs work in load-balancing mode.
Session Control Unit (SCU)	<ul style="list-style-type: none"> Processes services on the A-BCF, BGF and I-BCF. Processes and forwards 	SCUs work in active/standby mode.

Process Name	Function Description	Operating Mode
	IP, TCP, and SCTP messages over dynamic links (SIP over TCP and SIP over TLS).	
Voice and Video Process Unit (VPU)	Processes media data, including audio and video data.	VPU's work in load-balancing mode.

Relationships Between Service Processes

Figure 5-8 shows the relationships between service processes on the SE2900.

Figure 5-8 Relationships between service processes



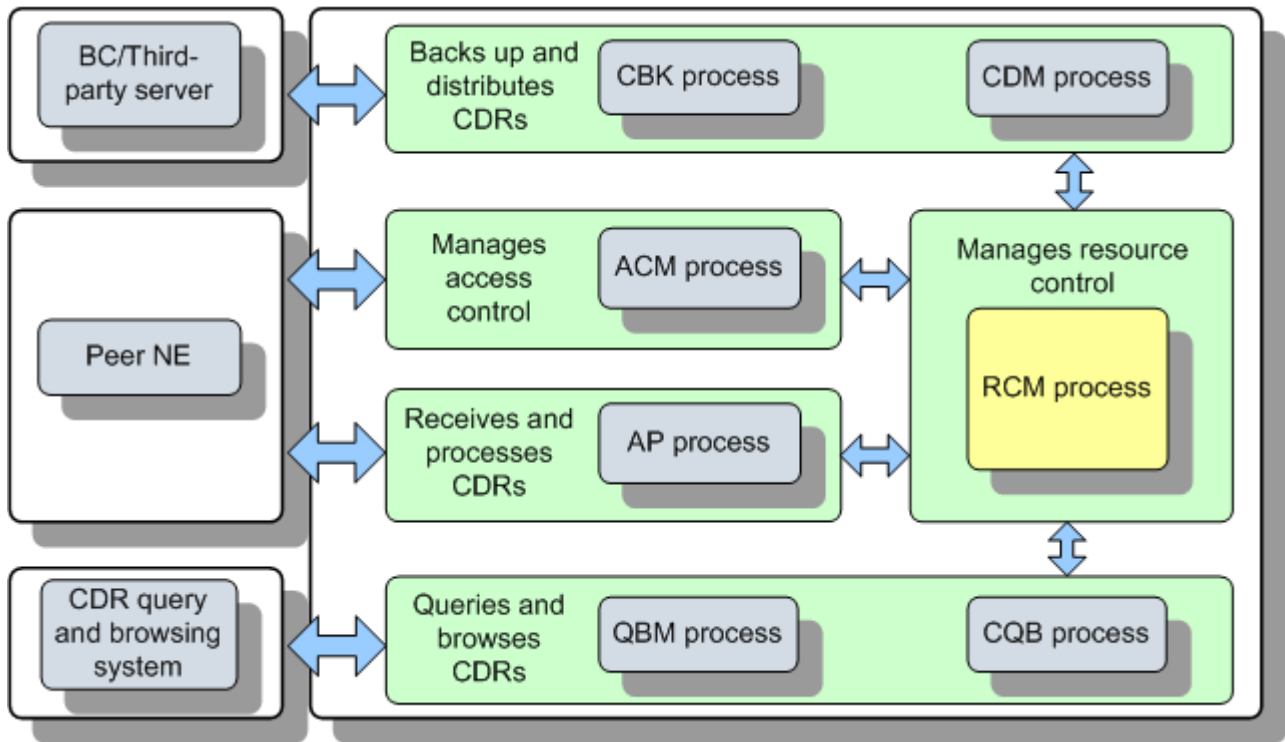
- Signaling message processing
 - DNS signaling messages
 - i. When an SCU performs DNS query, the SCU constructs a DNS query request and selects a link to the DNS server. Then the SCU sends the request to the BSU over the selected link.
 - ii. The BSU encapsulates source and destination IP addresses of the request and then sends the request to the HRU.

- iii. The HRU sends the request to the external DNS server.
- iv. The DNS server returns a DNS query response to the HRU, and the HRU forwards the response to the BSU.
- v. The BSU forwards the response to the SCU.
- SIP signaling messages over TCP
 - i. The HRU module receives a SIP message from the access side. If this SIP message is transmitted through a static SIP link over TCP, the HRU module forwards the message to the SCU module through the BSU module. If this SIP message is transmitted through a dynamic SIP link over TCP, the HRU module directly forwards the message to the SCU module.
 - ii. After receiving the SIP message from the HRU, the SCU processes the IP-layer and TCP-layer data of this SIP message. During message processing, the SCU queries the CDB for user dispatching data.
 - iii. After receiving the SIP message destined for the access side from the SCU, the HRU processes the IP-layer and TCP-layer data of this SIP message and then forwards the message to the external network through a physical interface.
- SIP signaling messages over UDP
 - i. The HRU receives a SIP message from the access side. If this SIP message is transmitted over UDP, the HRU forwards the message to the SCU.
 - ii. The SCU processes the received SIP message. During message processing, the SCU queries the CDB for user dispatching data.
 - iii. After processing the SIP message, the SCU forwards the message to the HRU.
 - iv. The HRU forwards the message to the external network through a physical interface.
- Media message processing: Media messages (such as RTP or MSRP messages) are processed by HRUs only.
- Bearer control message processing:
 - a. The SCU sends a bearer control message to the CMU to apply for bearer resources required for processing a call.
 - b. The CMU selects an HRU and sends the bearer control message to this HRU.
 - c. After receiving the message from the CMU, the HRU returns bearer resource information to the CMU.
 - d. After receiving bearer resource information from the HRU, the CMU sends the bearer control message to the SCU.
- Codec resource message processing
 - a. The SCU sends a message to the CMU to apply for bearer resources required for processing audio/video services.
 - b. The CMU selects a VPU from the local resource list and sends a message to the VPU to apply for codec resources.
 - c. After receiving the message from the CMU, the VPU allocates codec resources to the CMU.
 - d. After receiving the message from the VPU, the CMU returns codec resource information to the SCU.
 - e. If the media messages receiving from the access network require audio transcoding resources, the HRU applies for codec resources from the VPU. The VPU performs audio transcoding and sends media messages to the access network through the HRU.

- Security problem analysis and handling: The SEM collects exception statistics from the HRU, and SCU. Then the SEM categorizes exception statistics by IMPU, source IP address, and source IP address + source port and clears the statistics every 5 minutes. If the exception statistics exceed the threshold, the corresponding IMPU, source IP address, or source IP address + source port is blacklisted, and the connection between the attacker and SE2900 is disconnected.

CCF Service Processes

Figure 5-9 Software architecture



The iCG9815 is composed of seven service processes, and each of these processes consists of relatively independent service modules, as shown in Table 5-3.

Table 5-3 Service processes

Process	Full Name	Description
RCM	Resource control management	<p>The RCM process activates, monitors, deactivates, and clears resources used by other six processes to start or stop the six processes. The resources include network ports, IP addresses, and application programs. The RCM process serves as the core process that monitors the iCG9815 software.</p> <p>The RCM process also monitors and manages hardware resources. For example, when the RCM process detects a hardware fault that cannot be rectified, it starts a failover to the standby board.</p>
ACM	Access	Before a peer network entity (NE) sends original call detail records

Process	Full Name	Description
	control module	(CDRs), the ACM process assigns an AP process to the peer NE, balancing the loads of AP processes among different peer NEs.
AP	Access point	After the ACM process assigns an AP process for a peer NE, the AP process receives, processes, and stores CDRs. The AP process is responsible for CDR-related functions.
QBM	CDR query & browse management	The QBM process distributes query and browsing requests from clients to the CQB process on each board. After the CQB processes return query and browsing results, the QBM process merges and displays them on the CDR query and browsing system.
CQB	CDR query & browse	The CQB process receives an instruction from the QBM process, executes the instruction, and reports CDR query and browsing results to the QBM process.
CDM	CDR distribution management	The CDM process distributes the second copies of final CDRs to the billing center (BC) or a local directory. It supports three CDR distribution modes: PUSH, PULL, and local.
CBK	CDR backup	The CBK process backs up original CDRs, the first copies of final CDRs, and the second copies of final CDRs to a local directory or third-party server.

6 Interfaces and Protocols

About This Chapter

- 6.1 Physical Ports
- 6.2 Protocols and Interfaces
- 6.3 Standards Compliance

6.1 Physical Ports

Ports on the MXUA0

Figure 6-1 shows the ports on the MXUA0, and Table 6-1 lists the specifications of physical ports on the MXUA0.

Figure 6-1 Ports on the MXUA0

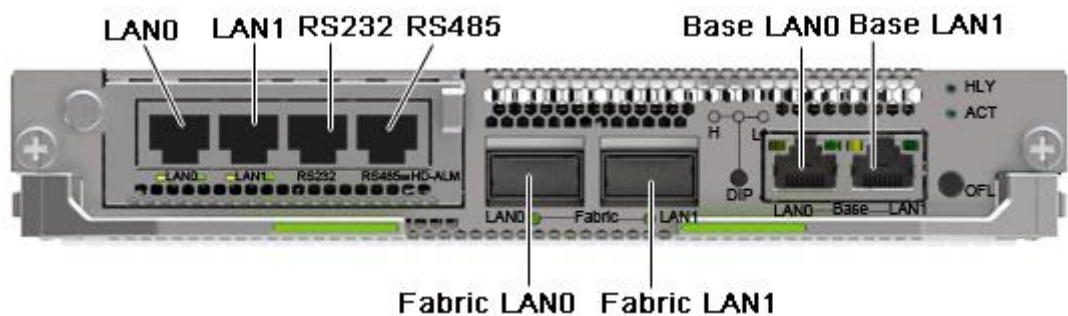


Table 6-1 Specifications of physical ports on the MXUA0

Board Name	Port Name	Function	Description	Port Quantity
MXUA0	LAN port	O&M network port	The port mode is 10/100/1000M Base-T autonegotiation. The port type is RJ-45.	2

Board Name	Port Name	Function	Description	Port Quantity
			The cable type is CAT5E. A LAN port has two indicators.	
	RS232 network port	Port for system commissioning	The port type is RJ-45. The cable type is DB9-RJ45. The standard RS232 network port provides channels for program loading, communication, commissioning, and monitoring.	1
	RS485 network port	Serial port for power distribution monitoring	The port type is RJ-45. The cable type is DB9-RJ45. The standard RS485 network port monitors the PDB status.	1
	Fabric LAN0/LAN1	Cascade port on the Fabric plane	The port mode is 40G BASE-XR4. The port type is QSFP+. The cable type is MPO. Fabric ports are used to implement Fabric cascading between the active and standby subracks.	2
	Base LAN0/LAN1	Cascade port on the BASE plane	The port mode is 10/100/1000M Base-T autonegotiation. The port type is RJ-45. The cable type is twisted pair. BASE ports are used to implement Base cascading between the active and standby subracks.	2

Ports on the SPUZ0/SPUA0/SPUA1

Figure 6-2 shows the ports on the SPUZ0/SPUA0/SPUA1. Table 6-2 lists the specifications of physical ports on the SPUZ0/SPUA0/SPUA1. On the SPUZ0/SPUA0/SPUA1, even-numbered ports can be changed from optical ports to electrical ports. 10GE ports can be used as 1GE ports.

Figure 6-2 Ports on the SPUZ0/SPUA0/SPUA1

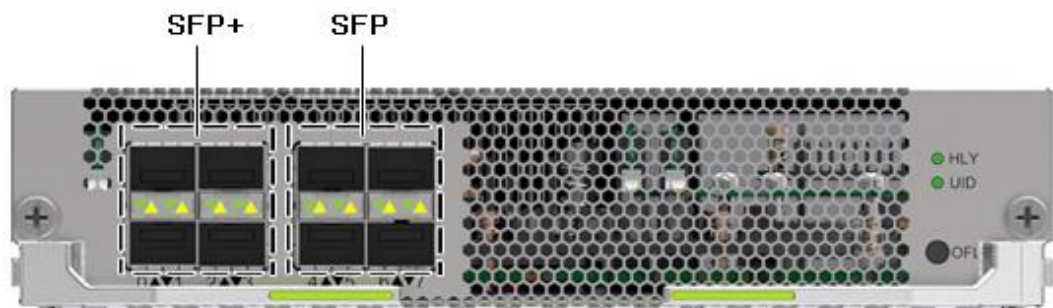


Table 6-2 Specifications of physical ports on the SPUZ0/SPUA0/SPUA1

Board Name	Port Name	Function	Description	Port Quantity
SPUZ0/SPUA0/SPUA1	SFP	1 GE signaling/management interface	The port type is LC jumpering square optical fiber connector or RJ45. The cable type is optical fiber or ethernet cable. The SPUA0/SPUA1 provides media interfaces.	4
	SFP+	10 GE/1 GE media interface	The port type is LC jumpering square optical fiber connector. The cable type is optical fiber. The SPUA0/SPUA1 provides signaling/NFS interfaces.	4

Ports on the VPUA0/VPUA1

Figure 6-3 shows the ports on the VPUA0/VPUA1. Table 6-3 lists the specifications of physical ports on the VPUA0/VPUA1.

Figure 6-3 Ports on the VPUA0/VPUA1



Table 6-3 Specifications of physical ports on the VPUA0/VPUA1

Board Name	Port Name	Function	Description	Port Quantity
VPUA0/VPUA1	SFP+	10 GE media interface	The port type is LC jumpering square optical fiber connector. The cable type is optical fiber. This port is reserved.	2
	SFP	1 GE signaling/media/network file server (NFS) interface	The port type is LC jumpering square optical fiber connector. The cable type is optical fiber. This port is reserved.	2

6.2 Protocols and Interfaces

Protocols and Interfaces Supported by the SE2900

Figure 6-4 and Figure 6-5 show the protocols and interfaces supported by the SE2900.

Figure 6-4 Protocols and interfaces supported by the SE2900 on the IMS network

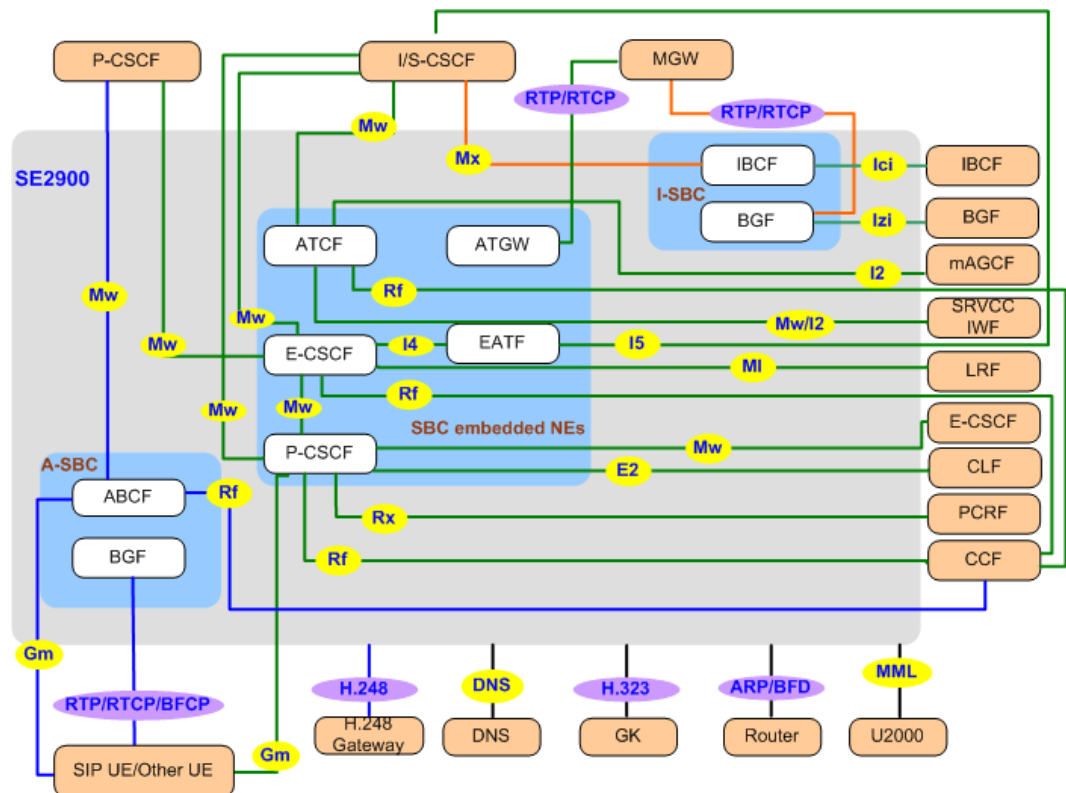


Table 6-4 describes the protocols and interfaces supported by the SE2900 on the IMS network.

Table 6-4 Protocols and interfaces supported by the SE2900 on the IMS network

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
SBC - U2000	MML	SNMP/MML	The SE2900 reports alarm information and traffic statistics to the EMS through the NM interface.	RFC 1157
• A-BCF -	Mw	SIP	• If the SE2900 does not provide an embedded	• 3GPP TS 23.228, 3GPP TS 24.228,

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
<ul style="list-style-type: none"> • P-CSCF • Embedded ATCF - I/S-CSCF • Embedded E-CSCF - P-CSCF • Embedded E-CSCF - embedded P-CSCF • Embedded E-CSCF - I/S-CSCF • Embedded P-CSCF - E-CSCF • Embedded P-CSCF - I/S-CSCF 			<p>P-CSCF, the A-BCF exchanges messages with the P-CSCF through the Mw interface to forward session messages to the core network for session control and service processing.</p> <ul style="list-style-type: none"> • If the SE2900 provides an embedded access transfer control function (ATCF), the ATCF controls enhanced single radio voice call continuity (eSRVCC) handover procedure through the Mw interface. • If the SE2900 provides an embedded E-CSCF, the P-CSCF identifies UE-originated calls as emergency calls and sends call messages to the E-CSCF through the Mw interface. The E-CSCF processes and routes emergency calls to an emergency center (EC). • If the SE2900 provides an embedded E-CSCF and an embedded P-CSCF, the P-CSCF identifies UE-originated calls as emergency calls and sends call messages to the E-CSCF through the Mw interface. The E-CSCF processes and routes emergency calls to an EC. • If the SE2900 provides an embedded P-CSCF, the P-CSCF identifies UE-originated calls as emergency calls and sends call messages to the E-CSCF through the Mw interface. The E-CSCF processes and routes emergency calls to an EC. • When the SE2900 that provides an embedded P-CSCF interworks with the I/S-CSCF through the Mw interface, the Mw interface 	<p>3GPP TS 24.229, 3GPP TS 23.218, and 3GPP TS 23.002</p> <ul style="list-style-type: none"> • ETSI TS 182 006 and ETSI ES 283 003

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
			<p>implements the following functions:</p> <ul style="list-style-type: none"> - During the registration procedure, the P-CSCF forwards UE-originated SIP registration and session setup messages to the I-CSCF in the home domain through the Mw interface. The I-CSCF forwards the messages to the appropriate S-CSCF. - During the call procedure, the P-CSCF forwards call messages to the S-CSCF through the Mw interface. The S-CSCF performs session control and session routing. 	
SBC - DNS	DNS	DNS	The SE2900 implements domain name query and resolution through the DNS interface.	RFC 1034, RFC 1035, RFC 2181, and RFC 2782
SBC - router	-	ARP/BFD	ARP/BFD is employed between the router and SE2900 to detect communication failures on a peer device. Upon detecting a communication failure, the SE2900 switches traffic to the backup link to ensure service continuity, minimize the impact of device or link faults on services, and improve network availability.	<ul style="list-style-type: none"> • ARP: RFC 826 • BFD: RFC 5880
<ul style="list-style-type: none"> • A-BCF - SIP UE/H.323 UE/another type of UE • Embedded P-CSCF - SIP UE/another 	Gm	SIP	SIP UEs or other types of UEs access the VoBB and RCS networks through the SE2900 over the Gm interface. The SE2900 performs NAT traversal and signaling encryption for the UEs.	<ul style="list-style-type: none"> • 3GPP TS 23.228, 3GPP TS 24.228, 3GPP TS 24.229, and 3GPP TS 23.002 • ETSI TS 182 006 and ETSI ES 283 003
	-	UDP/TCP	SIP UEs, H.323 UEs, or other types of UEs exchange messages with other types of UEs through the SE2900 using UDP/TCP. The SE2900 encrypts and detects transmitted RTP/RTCP/MSRP	RFC 3550 and RFC 3711

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
type of UE			media streams. (RTP: Real-Time Transport Protocol; RTCP: Real-Time Transport Control Protocol; MSRP: Message Session Relay Protocol)	
	-	BFCP	SIP UEs, H.323 UEs, or other types of UEs access IMS/NGN conferences or perform video communication with other types of UEs using Binary Floor Control Protocol (BFCP). The SE2900 performs flow control for BFCP auxiliary streams.	<ul style="list-style-type: none"> • RFC 4582 • RFC 4583 • draft-sandbakken-xcon-bfcp-udp-00 • draft-sandbakken-dispatch-bfcp-udp-00
<ul style="list-style-type: none"> • IBCF - I-CSCF • IBCF - S-CSCF 	Mx	SIP	<ul style="list-style-type: none"> • The SE2900 exchanges messages with the I-CSCF through the Mx interface to select an S-CSCF. • The SE2900 exchanges messages with the S-CSCF through the Mx interface to forward sessions to the core network for session control and service processing. 	3GPP TS 23.228
<ul style="list-style-type: none"> • Embedded ATCF - CCF • Embedded E-CSCF - CCF • Embedded P-CSCF - CCF • A-BCF - CCF 	Rf	Diameter	The embedded ATCF/E-CSCF/P-CSCF or A-BCF exchanges messages with the charging collection function (CCF) through the Rf interface to implement offline charging.	<ul style="list-style-type: none"> • 3GPP TS 32299-760 • RFC 3588
<ul style="list-style-type: none"> • Embedded P-CSCF - PCRF • Embedded P-CSCF - CLF 	Rx	Diameter	The P-CSCF exchanges session information with the policy and charging rules function (PCRF) through the Rx interface. Based on the information, the PCRF implements policy and charging control.	3GPP TS 29.214
	E2	Diameter	If the SE2900 provides an embedded P-CSCF, the P-CSCF	ETSI ES 283 035

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
			obtains location information about the UE on the fixed network from the connectivity session location and repository function (CLF).	
<ul style="list-style-type: none"> Embedded ATCF - mAGCF Embedded ATCF - SRVCC IWF 	I2	SIP	The ATCF exchanges messages with the mAGCF/SRVCC IWF to resume calls in the hold state after SRVCC handovers. (mAGCF: mobile access gateway control function; IWF: interworking function)	<ul style="list-style-type: none"> 3GPP TS 23.237 V12.0.0 and 3GPP TS 24.237 V12.0.0 IETF RFC3261 and extension
Embedded E-CSCF - embedded EATF	I4	SIP	If the SE2900 provides an embedded E-CSCF and emergency access transfer function (EATF), the E-CSCF anchors emergency calls to the EATF through the I4 interface for the eSRVCC handover that is likely to occur.	<ul style="list-style-type: none"> 3GPP TR 23.870 3GPP TS 24.237
Embedded EATF - I/S-CSCF	I5	SIP	If the SE2900 provides an embedded E-CSCF, the E-CSCF sends emergency call handover requests to the I-CSCF through the I5 interface. The I-CSCF then forwards the requests to the EATF.	<ul style="list-style-type: none"> 3GPP TR 23.870 3GPP TS 24.237
IBCF - IBCF	Ici	SIP	Used to exchange messages between an IBCF and another IBCF belonging to a different IMS network.	3GPP TS 29.165
BGF - BGF	Izi	SIP	Used to forward media streams from a BGF to another BGF belonging to a different IMS network.	3GPP TS 29.165
Embedded E-CSCF - LRF	M1	Diameter	If the SE2900 provides an embedded E-CSCF, the E-CSCF, according to local policies, obtains the calling number, called number, and location information about UEs from the location registration function (LRF) through the M1 interface for	<ul style="list-style-type: none"> 3GPP TS 23.167 3GPP TS 24.229

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
			emergency call routing.	
SBC - GK	-	H.323	The SE2900 exchanges messages with the gatekeeper (GK) using H.323 to provide basic and supplementary services.	<ul style="list-style-type: none"> • ITUT H.245 • ITUT H.225.0 • ITUT Q.931 • ITUT H.224 • ITUT H.239
SBC - AGCF	-	H.248	The SE2900 exchanges messages with the access gateway control function (AGCF) using H.248 to provide basic and supplementary services.	<ul style="list-style-type: none"> • Q/CT 2283-2010 • RFC3525
SBC - H.248 gateway	-	H.248	The SE2900 exchanges messages with the H.248 gateway using H.248 to provide basic and supplementary services.	<ul style="list-style-type: none"> • Q/CT 2283-2010 • RFC3525

Figure 6-5 Protocols and interfaces supported by the SE2900 on the NGN

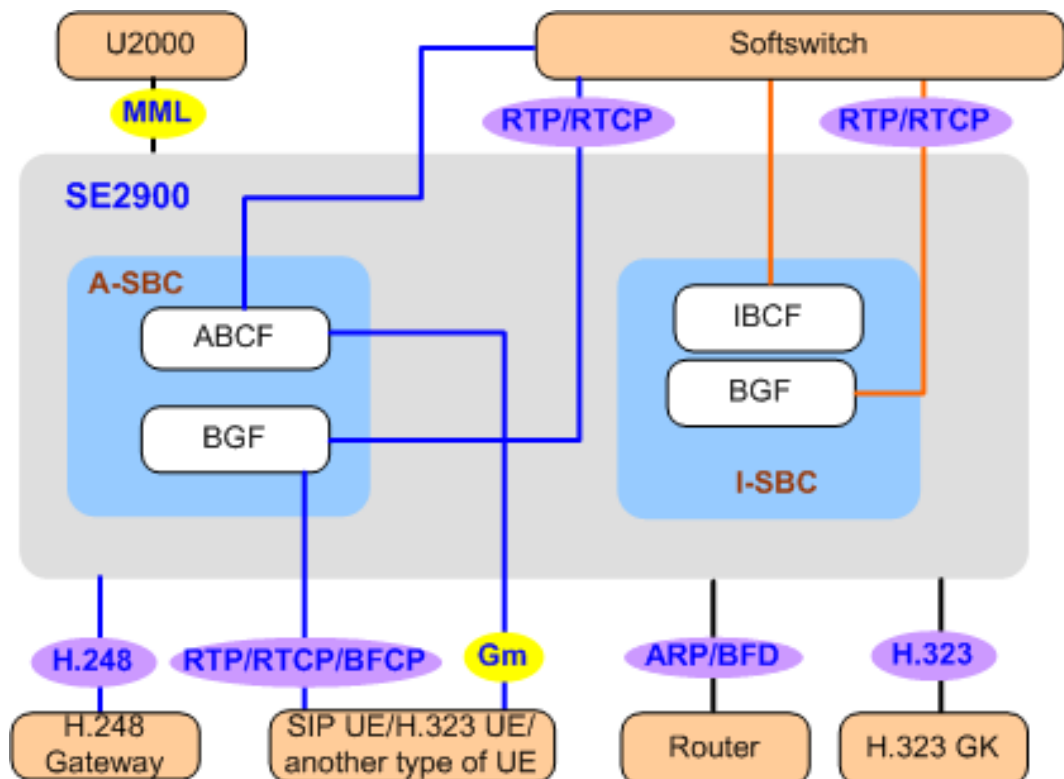


Table 6-5 describes the protocols and interfaces supported by the SE2900 on the NGN.

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
SBC - U2000	MM L	SNMP/MML	The SE2900 reports alarm information and traffic statistics to the EMS through the NM interface.	RFC 1157
ABCF - Softswitch	-	SIP	The SE2900 exchanges messages with the Softswitch using SIP to forward session messages to the core network for session control and service processing.	<ul style="list-style-type: none"> 3GPP TS 23.228, 3GPP TS 24.228, 3GPP TS 24.229, 3GPP TS 23.218, and 3GPP TS 23.002 ETSI TS 182 006 and ETSI ES 283 003
SBC - router	-	ARP/BFD	ARP/BFD is employed between the router and SE2900 to detect communication failures on a peer device. Upon detecting a communication failure, the SE2900 switches traffic to the backup link to ensure service continuity, minimize the impact of device or link faults on services, and improve network availability.	<ul style="list-style-type: none"> ARP: RFC 826 BFD: RFC 5880
A-BCF - SIP UE/H.323 UE/another type of UE	-	SIP	SIP UEs, H.323 UEs or other types of UEs access the NGN through the SE2900 using SIP. The SE2900 performs NAT traversal and signaling encryption for the UEs.	<ul style="list-style-type: none"> 3GPP TS 23.228, 3GPP TS 24.228, 3GPP TS 24.229, and 3GPP TS 23.002 ETSI TS 182 006 and ETSI ES 283 003
	-	UDP/TCP	SIP UEs, H.323 UEs, or other types of UEs exchange messages with other types of UEs through the SE2900 using UDP/TCP. The SE2900 encrypts and detects transmitted RTP/RTCP media streams.	RFC 3550 and RFC 3711
	-	BFCP	SIP UEs, H.323 UEs, or other types of UEs access IMS/NGN conferences or perform video communication with other types of UEs using BFCP. The SE2900 performs flow control for BFCP auxiliary streams.	<ul style="list-style-type: none"> RFC 4582 RFC 4583 draft-sandbakken-xcon-bfcp-udp-00 draft-sandbakken-dispatch-bfcp-udp

Interconnected Devices	Interface	Protocol	Interface Function	Compliance Standard or Protocol
				-00
IBCF - Softswitch	-	SIP	The SE2900 exchanges messages with the Softswitch using SIP to forward session messages to the core network for session control and service processing.	3GPP TS 23.228
SBC - GK	-	H.323	The SE2900 exchanges messages with the GK using H.323 to provide basic and supplementary services.	<ul style="list-style-type: none"> • ITUT H.245 • ITUT H.225.0 • ITUT Q.931 • ITUT H.224 • ITUT H.239
SBC - Softswitch	-	H.248	The SE2900 exchanges messages with the Softswitch using H.248 to provide basic and supplementary services.	<ul style="list-style-type: none"> • Q/CT 2283-2010 • RFC3525
SBC - H.248 gateway	-	H.248	The SE2900 exchanges messages with the H.248 gateway using H.248 to provide basic and supplementary services.	<ul style="list-style-type: none"> • Q/CT 2283-2010 • RFC3525

Protocols and Interfaces Supported by the CCF

The CCF provides interfaces for interworking with the peer NEs, maintenance terminals, and billing center (BC), as shown in Figure 6-6.

Figure 6-6 Protocols and interfaces supported by the CCF on the IMS network

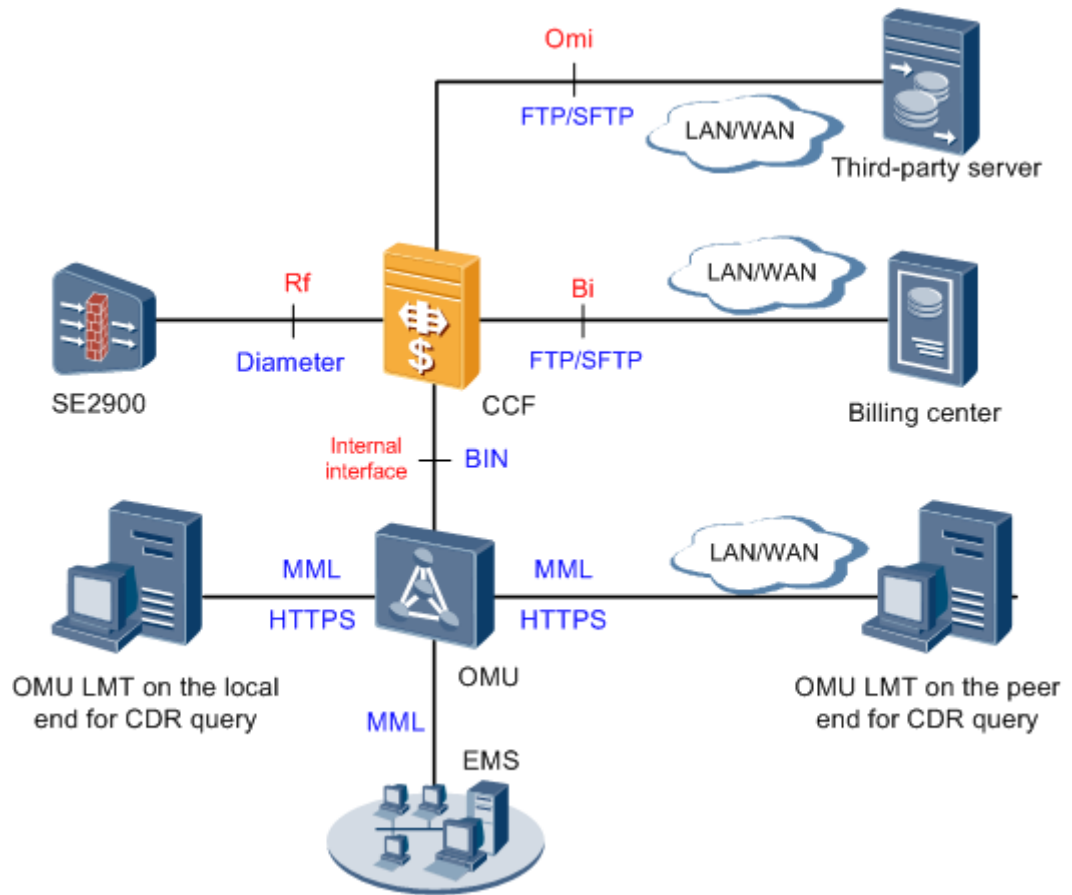


Table 6-5 describes the protocols and interfaces supported by the CCF on the IMS network.

Table 6-5 Protocols and interfaces supported by the CCF on the IMS network

NEs	Interface	Protocol	Description
CCF - peer NE	Rf	Diameter	The Rf interface is an interface between the SE2900 logical entity (such as the A-BCF, IBCF, ATCF, P-CSCF, or E-CSCF) and CCF. It is used to receive Accounting Records (ACRs) from the logical entity and ensure that no ACR is lost or duplicated.
CCF - third-party server	OMi	FTP/SFTP	The OMi interface is used to back up original CDRs and the first copies of final CDRs to a third-party server.
CCF - BC	Bi	FTP/SFTP	The Bi interface uses FTP or SFTP for CDR distribution. The CCF uses this interface to send final CDRs to the BC.
CCF - OMU (local and remote)	Internal interface	BIN (internal)	The internal interface allows users to use an OMU client, a WebUI, or a centralized EMS. The CCF communicates with the OMU using an internal interface and an internal

NEs	Interface	Protocol	Description
maintenance terminals)	face	protocol)	protocol. The interface and protocol are shielded from users.

6.3 Standards Compliance

The SE2900 complies with protocols and standards released by 3GPP, ITU-T, ANSI, ETSI, IETF, ISO, and IEC.

For detailed protocols and standards that each function complies with, see *Standards and Protocols Compliance*.

7 Application Scenarios

About This Chapter

- 7.1 SE2900 in the RCS Solution
- 7.2 SE2900 in the VoBB Solution
- 7.3 SE2900 in the VoLTE Solution
- 7.4 Application of the SE2900 in Network Interconnection
- 7.5 SE2900 on the NGN

7.1 SE2900 in the RCS Solution

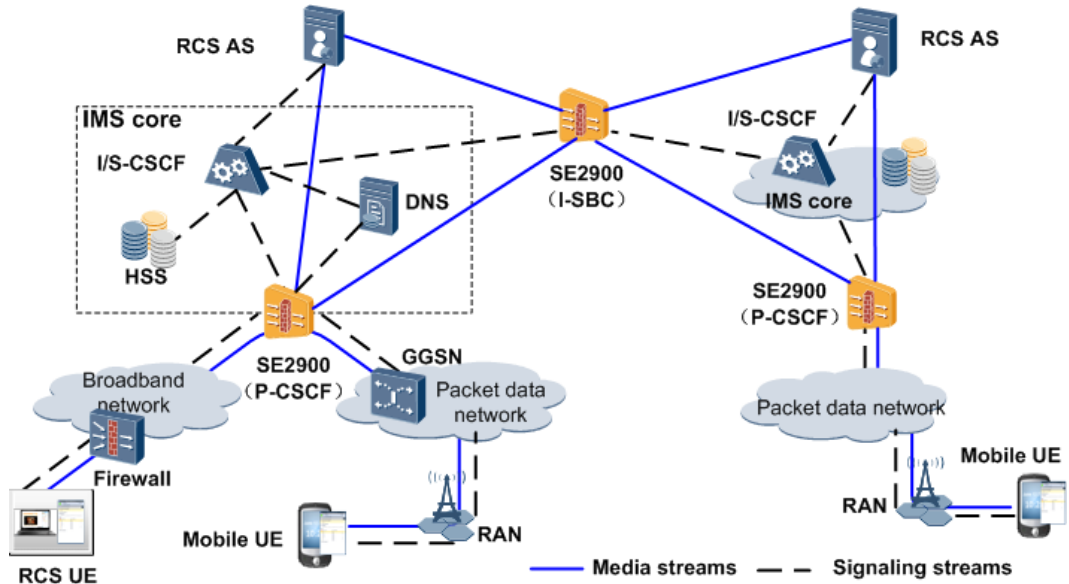
As the wireless broadband technology continues to rapidly evolve and be deployed, intelligent terminals are gradually becoming popularized, owing to their affordable prices. Over-the-top (OTT) service providers frequently launch widely-anticipated social service applications over carriers' networks to constantly tap into potential communication needs, such as instant messaging, multimedia content sharing, and social applications.

The popularization of the OTT services leads to a sharp decline in carriers' core services, such as voice and short message revenues. The root cause lies in the partial or complete replacement of traditional communication modes and ever-changing user requirements. To boost revenue and meet end-users' rich media communication needs, carriers must rapidly transform traditional services by focusing on end-user experience and gradually develop socially-centered Internet service modes. The Rich Communication Suite (RCS) defined by the Global System for Mobile Communications Association (GSMA) enables carriers to provide cross-platform rich media communications services running on PCs and intelligent UEs for users. The services include content sharing, network address book synchronization, and instant messaging. However, the all-IP network architecture and cross-platform nature of the RCS solution bring about the following challenges:

- The emergence of more intelligent UEs and the growing integration of services present serious security issues and challenges to the core network. Ensuring network and user information security is the top concern for network deployment.
- If a firewall permits only some fixed ports or serves as an HTTP proxy on the intranet, the RCS service is unavailable.
- In wireless access, for example, Wireless Fidelity (Wi-Fi), call quality may be affected by packet loss from poor network quality.

The preceding problems significantly limit the application of the RCS to users. To address these problems and extend the reach of the RCS, the SE2900 is deployed between the core network and access network in the RCS solution, as shown in Figure 7-1.

Figure 7-1 SE2900 in the RCS solution



DNS: domain name server

HSS: home subscriber server

IMS: IP multimedia subsystem

RAN: radio access network

S-CSCF: serving-call session control function

GGSN: gateway GPRS support node

I-CSCF: interrogating-call session control function

P-CSCF: proxy-call session control function

RCS AS: rich communication suite application server

SBC: session border controller

In the RCS solution, the SE2900 implements the following functions:

- Access/interworking security

In the RCS solution, the SE2900 provides the following major security functions:

- Data encryption: The SE2900 deployed between RCS UEs and the core network uses SIP over TLS, Media Session Relay Protocol (MSRP) over TLS, and Secure Real-time Transport Protocol (SRTP) to enhance the security of data transmission between RCS UEs.

NOTE

Because of the openness of the IP network, the network environment between RCS UEs and the core network has complex security issues. Data transmitted between RCS UEs and the core network needs to be encrypted to protect data from unauthorized access. By comparison, data between the SE2900 and core network is transmitted in carriers' equipment rooms or over dedicated networks, and the transmission environment is secure. Therefore, data packets can be transmitted in plaintext.

- Signaling/media attack defense: The SE2900 provides IP layer attack defense, signaling DoS/DDoS attack defense, and media pinholing firewall to prevent network attacks launched by unauthorized users.
- Firewall traversal
To improve network security, some enterprises deploy a firewall between the local area network (LAN) and public network, and the firewall permits only port 443 (HTTPS) or 80 (HTTP) for data packet transmission. As a result, data packets originating from RCS UEs cannot traverse the firewall, rendering RCS services unavailable.
When the firewall deployed between an RCS UE and the SE2900 does not permit RCS service packets between the RCS UE and SE2900, the firewall traversal feature can be used to address the packet transmission problem and ensure the availability of RCS services.



NOTE

If firewall traversal is not used on the SE2900, the firewall needs to permit a large number of ports for RTP packet transmission, posing threats to intranet security. If firewall traversal is used, the firewall needs to permit only port 443 or 80 to transmit data packets originating from RCS UEs, thereby meeting RCS service requirements.

- Voice QoS assurance
Communication on unstable networks, such as Wi-Fi and WiMAX, is subject to data packet loss. RFC2198 redundancy compensates for packet loss on the access side to ensure reliable audio transmission and improve audio transmission quality.
- MSRP proxy
MSRP proxy enables the SE2900 to provide MSRP-based picture sharing, file transmission, and chat services.
 - In the A-SBC scenario, the SE2900 forwards MSRP media streams between a UE and an AS, or between UEs.
 - In the I-SBC scenario, the SE2900 transparently transmits MSRP media streams between ASs/UEs.
- Embedded NEs
With the P-CSCF, the SE2900 is able to provide access to the RCS network for UEs on different networks using SIP ANs on one SE2900, enhancing network convergence and reducing the expenditure of deploying a separate P-CSCF.

The SE2900 also provides basic functions for RCS networking. For details, see 4.1 Feature Matrix.

7.2 SE2900 in the VoBB Solution

As the telecommunications market becomes more and more open, traditional carriers that offer only narrowband-based audio services no longer meet users' service requirements. They need to find new bandwidth services as growth points. The VoBB solution employs the all-IP network architecture. It implements VoBB services by providing xDSL/FTTx/LAN/Wi-Fi access to fixed network carriers and Wi-Fi/WiMAX access to mobile network carriers.

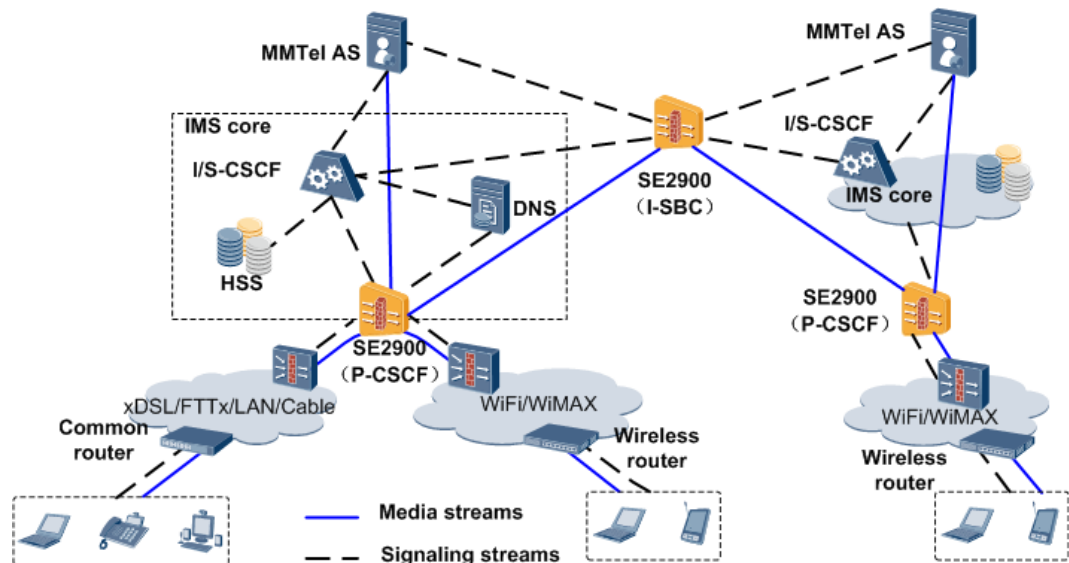
The VoBB network adopts the all-IP network structure. It accommodates various access technologies (such as xDSL and Wi-Fi) and provides services to diverse UEs. Therefore, VoBB solutions are in face of the following challenges:

- The emergence of more intelligent UEs and the growing integration of services present serious security issues and challenges to the core network. Ensuring network and user information security is the top concern for network deployment.

- How to ensure synchronous processing of media resources and signaling control to prevent high resource usage in the case of separation between bearer control and call control.
- How to use network bandwidth properly so as to prevent bandwidth overuse.

The preceding problems increases VoBB application risks and pose challenges to wide VoBB application. To address these problems, the SE2900 is deployed between the access network and core network and provides security and signaling/media proxy on the VoBB network, as shown in Figure 7-2.

Figure 7-2 SE2900 in the VoBB solution



DNS: domain name server

FTTx: fiber to the x

HSS: home subscriber server

I-CSCF: interrogating-call session control function

IMS: IP multimedia subsystem

LAN: local area network

MMTel AS: multimedia telephony application server

P-CSCF: proxy-call session control function

S-CSCF: serving-call session control function

SBC: session border controller

Wi-Fi: Wireless Fidelity

WiMAX: Worldwide Interoperability for Microwave Access

xDSL: x digital subscriber line

-

In the VoBB solution, the SE2900 provides the following functions:

- Access/interworking security
 - Data encryption: The SE2900 deployed between VoBB UEs and the core network uses SIP over TLS and MSRP over TLS to enhance the security of data transmission between VoBB UEs.

 **NOTE**

Because of the openness of the IP network, the network environment between VoBB UEs and the core network has complex security issues. Data transmitted between VoBB UEs and the core network needs to be encrypted to protect data from unauthorized access. By comparison, data between the SE2900 and core network is transmitted in carriers' equipment rooms or over dedicated networks, and the transmission environment is secure. Therefore, data packets can be transmitted in plaintext.

- Signaling/media attack defense: The SE2900 provides IP layer attack defense, signaling DoS/DDoS attack defense, and media pinholing firewall to prevent network attacks launched by unauthorized users.
- CAC: The CAC feature allows carriers to restrict the number of concurrent calls per user based on the source IP address, preventing the overuse of resources. The CAC feature also allows carriers to set the registration and call rate thresholds and discard the packets that have registration and call rates greater than the thresholds, protecting carrier network devices from attacks.
- Topology hiding: Deployed between the public network and private network, the SE2900 hides the core network topology from the access network and hides the access network topology from the core network. The SE2900 performs topology hiding in the processing of messages at the IP layer, transport layer, and signaling layer. With the topology hiding function, the SE2900 translates between access-side addresses and core-side addresses to ensure the information security of the core network.
- Call management
In the VoBB solution, the SE2900 serves as a signaling proxy, media proxy, and network interworking gateway to detect signaling and media streams in VoBB services. If a fault occurs, there is a probability that signaling is unavailable but media streams are not released or media streams are unavailable but signaling is not released, resulting in an extra-long call detail record (CDR). With the session timer or no media stream detection feature, abnormal sessions can be terminated in time, thereby ensuring accurate charging and avoiding unnecessary loss to users.
- Bandwidth management
The SE2900 provides session-based QoS assurance for real-time sessions. This is implemented by allocating a fixed amount of bandwidth to each VoBB session according to the codec type in each session to prevent bandwidth overuse or theft by unauthorized users.
- Embedded NE
With the P-CSCF, the SE2900 is able to provide access to the IMS network for UEs on VoBB networks using SIP ANs on one SE2900, enhancing network convergence (such as VoLTE and VoBB convergence) and saving the expenditure of deploying a separate P-CSCF.

The SE2900 also provides basic functions for VoBB networking. For details, see 4.1 Feature Matrix.

7.3 SE2900 in the VoLTE Solution

The popularity of the 3G mobile communication technology and intelligent UEs boosts users' needs for mobile broadband services. As data traffic burst, network capacity needs to be expanded. Carriers must upgrade the network promptly to enhance the network transmission speed and meet users' ever-changing needs. The Long Term Evolution (LTE) technology is the best choice in the mobile broadband age.

In the LTE age, voice services are still carriers' main revenues, but basic audio service cannot meet network users' requirements. With the emergence of more intelligent UEs and popularity of over the top (OTT) services, users pursue rich audio services. Therefore, carriers must rapidly transform traditional audio and short message services.

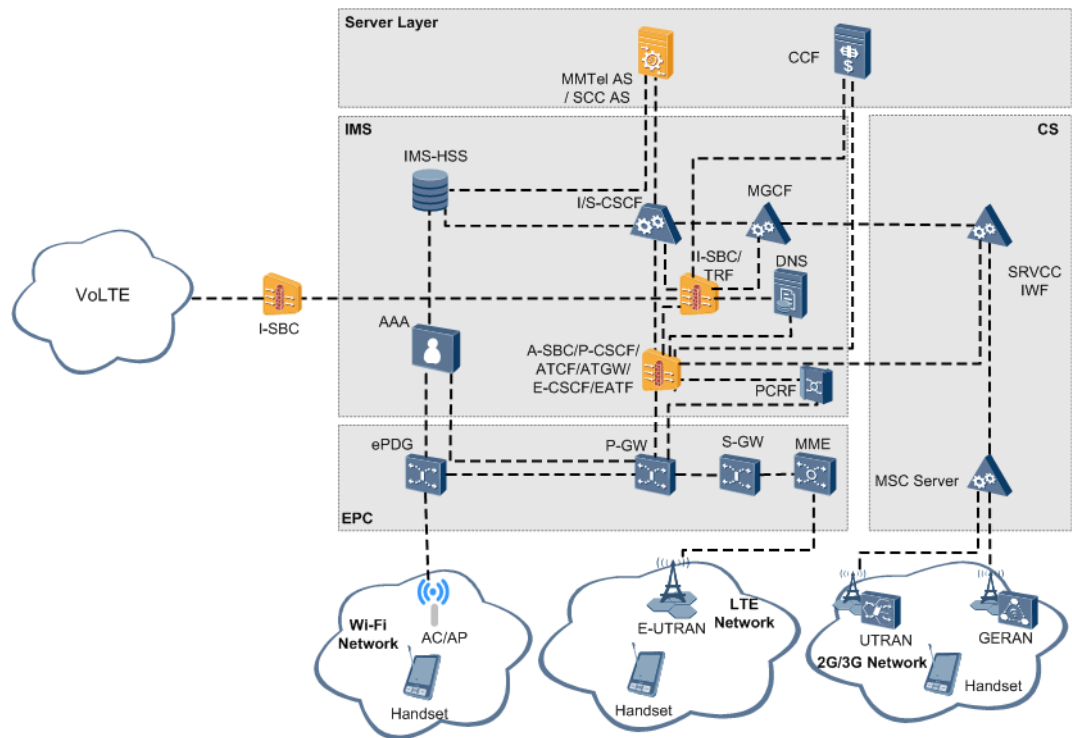
Voice over LTE (VoLTE) is an IMS network-based LTE audio solution defined in 3GPP. Through the IMS network, mobile carriers integrate audio calls with rich enhancement functions to provide diverse services in addition to inheriting traditional audio and short message services.

The VoLTE solution builds the IMS network and LTE network on the legacy CS network. Interworking between the networks is an issue. The VoLTE solution must effectively solve the following problems:

- How to simplify VoLTE deployment and minimize the impact of VoLTE deployment on the existing 2G/3G network.
- The emergence of more intelligent UEs and the growing integration of services present serious security issues and challenges to the core network. Ensuring network and user information security is the top concern for network deployment.
- How to use network bandwidth properly so as to prevent bandwidth overuse.
- How to implement a smooth call handover when UEs on the 2G/3G network interwork with UEs on the CS network or LTE UEs move in different areas.
- How to ensure voice quality in audio/video calls between UEs since voice is over IP.
- How to implement service provisioning and NE charging since network services are inherited to the LTE network.
- How to implement codec interworking since the UEs are on different networks and use different codecs to access the LTE network.
- How to implement distinctive charging for users in Wireless Fidelity (Wi-Fi) access and LTE access during a UE handover between Wi-Fi and LTE.
- How to enable VoLTE users to use roaming services on the IMS network.

The preceding problems significantly limit the application of the VoLTE solution to users. To address these problems and solve issues such as security and signaling/media proxy, the SE2900 is deployed on the VoLTE network, as shown in Figure 7-3.

Figure 7-3 SE2900 in the VoLTE solution



ATCF: access transfer control function

ATGW: access transfer gateway

CCF: charging collection function

DNS: domain name server

E-UTRAN: evolved universal terrestrial radio access network

GERAN: GSM/EDGE radio access network

HSS: home subscriber server

I-CSCF: interrogating-call session control function

IMS: IP multimedia subsystem

IMS-HSS: IP multimedia subsystem home subscriber server

LTE CPE: long term evolution customer premises equipment

MME: mobility management entity

MMTel AS: multimedia telephony application server

MSC server: mobile switching center server

PCRF: policy and charging rules function

P-CSCF: proxy-call session control function

PGW: PDN gateway

SBC: session border controller

S-CSCF: serving-call session control function

SCC AS: service centralization and continuity application server

S-GW: serving gateway

SGSN: serving GPRS support node

SRVCC IWF: single radio voice call continuity interworking function

UTRAN: universal terrestrial radio access network

ePDG: evolved packet data gateway

AAA: authentication, authorization and

accounting

AC/AP: access controller/access point

TRF: transit and roaming function

In the VoLTE solution, the SE2900 provides the following functions:

- Access/interworking security
 - Signaling/media attack defense: The SE2900 provides IP layer attack defense, signaling DoS/DDoS attack defense, and network address translation (NAT) to prevent network attacks launched by unauthorized users.
 - CAC: The CAC feature allows carriers to restrict the number of concurrent calls per user based on the source IP address, preventing the overuse of resources. The CAC feature also allows carriers to set the registration and call rate thresholds and discard the packets that have registration and call rates greater than the thresholds, protecting carrier network devices from attacks.
 - Topology hiding: Deployed between the public network and private network, the SE2900 hides the core network topology from the access network and hides the access network topology from the core network. The SE2900 performs topology hiding in message processing at the IP layer, transport layer, and signaling layer. With the topology hiding function, the SE2900 translates between access-side addresses and core-side addresses to ensure the information security of the core network.
 - Audio transcoding: The SE2900 supports audio transcoding for the UEs that are on different networks and use different codecs to access the LTE network. This function enables carriers to lower their capital expenditure (CAPEX) and operating expenditure (OPEX) by implementing signaling and media interworking between different network types. There is no need to deploy a separate audio transcoding device.
 - IMS-Authentication and Key Agreement (AKA)/IPSec: IMS-AKA/IPSec is a mechanism that enables the IMS network and IMS UEs using IP multimedia services identity module (ISIM) cards to authenticate each other. This mechanism implements mutual authentication between IMS UEs and the IMS network. During the authentication process, the IMS network delivers keys to the SE2900. The SE2900 uses the keys to prevent signaling packets from being tampered with and sensitive user information from being disclosed.
- Call management
 - Signaling and media proxy: In the VoLTE solution, the SE2900 serves as a signaling and media proxy to detect signaling and media streams in VoLTE services. If a fault occurs, there is a probability that signaling is unavailable but media streams are not released or media streams are unavailable but signaling is not released, resulting in an extra-long charging data record (CDR). With the session timer or no media stream detection feature, abnormal sessions can be terminated in time, thereby ensuring accurate charging and avoiding overcharging.
 - Offline charging: The SE2900 interworks with the CCF to implement offline charging. The SE2900 generates ACRs based on session information and sends charging information to the CCF over the Diameter-based Rf interface. The CCF then generates CDRs based on the received ACR messages. Offline charging enables carriers to compare time-based CDRs generated by the SE2900 with those generated by other network elements (NEs).
- Bandwidth management

Quality of service (QoS) assurance provides expected quality for network communication services in terms of bandwidth, packet loss rate, round-trip delay, and jitter. QoS assurance involves three major functions: policy control support (Rx), voice quality reporting and multimedia priority service (MPS).

- Policy control support (Rx): It enables the SE2900 to interwork with the PCRF over the Diameter-based Rx interface. The SE2900 extracts the session information about a UE, such as the signaling address, media address, and media bandwidth, from SIP messages, and sends the information to the PCRF over the Rx interface.
- Voice quality reporting: It enables the SE2900 to measure voice quality of calls in real time, including the packet loss rate, jitter, round-trip delay, and mean opinion score (MOS).
- Multimedia priority service (MPS): It enables the SE2900 to include priority information in the messages of certain calls so that these calls are preferentially processed and allocated with more physical resources.
- Embedded NEs
 - P-CSCF: With the P-CSCF, the SE2900 is able to provide access to the IMS network for UEs on both the VoLTE and VoBB networks using SIP ANs on one SE2900, enhancing network convergence (such as VoLTE and VoBB convergence) and saving the expenditure of deploying a separate P-CSCF.
 - E-CSCF/EATF: The SE2900 provides an embedded E-CSCF and an embedded EATF. The E-CSCF enables the SE2900 to process and route emergency calls to an emergency center (EC). The EATF enables the SE2900 to anchor emergency calls and switch emergency calls from a PS network to a CS network or from an LTE network to a 2G/3G network for call continuity.
 - ATCF/ATGW: Enhanced SRVCC (eSRVCC) ensures voice call continuity when an LTE UE is handed over from the E-UTRAN to the UTRAN/GERAN.
- Voice over WiFi (VoWiFi) access
 - The SE2900 identifies the access network type change and notifies the change to the core network.
 - The SE2900 supports emergency calls initiated over Wi-Fi.
- UE roaming
 - The SE2900 supports UE roaming across IMS networks.
 - The SE2900 supports media bypass for roaming UEs.
- SD/HD video call
 - The SE2900 supports high-quality SD/HD video calls.
 - The SE2900 supports the control over the concurrent number of SD/HD video calls, ensuring the completion rate and quality of audio calls.

The SE2900 also provides basic functions for VoLTE networking. For details, see 4.1 Feature Matrix.

7.4 Application of the SE2900 in Network Interconnection

The popularization of IP technologies around the globe facilitates IP-based interconnection between carrier networks with a relatively low cost. The interconnection border control function (IBCF) and interconnection border gateway function (IBGF) implement such interconnection between carrier networks. The IBCF provides functions, such as packet

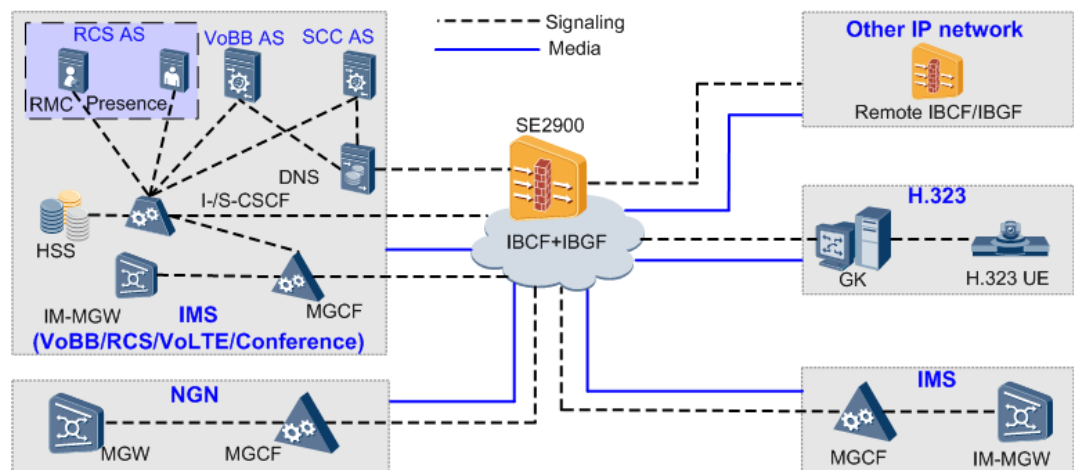
routing, packet forwarding, border control, and topology hiding, and instructs the IBGF to implement media interworking across domains.

The interconnection between heterogeneous networks that are formed because of asynchronous evolution of carrier networks faces the following challenges:

- Threats to network and user security caused by various smart devices and diversified convergent services
- Adaptation to various protocols, such as SIP, SIP-I, and SIP-T, among heterogeneous networks and interconnection between devices of different vendors
- Requirements on high-efficient multimedia service interconnection in addition to legacy audio and SMS services

To overcome preceding challenges, the SE2900 is introduced in network connection. In Figure 7-4, the SE2900 supports the interconnection between IMS networks and IMS/NGN/CS/H.323 networks.

Figure 7-4 Application of the SE2900 in network interconnection



ATS: advanced telephony server

DNS: domain name server

HSS: home subscriber server

IBGF: interconnection border gateway function

IM-MGW: IP multimedia media gateway

MGW: media gateway

RMC: RCS messaging center

S-CSCF: serving-call session control function

VoLTE: voice over LTE

AS: application server

GK: gate keeper

IBCF: interconnection border control function

I-CSCF: interrogation-call session control function

MGCF: media gateway control function

RCS: rich communication suite

SCC: service control center

VoBB: voice over broadband

-

In network connection, the SE2900 provides the following functions:

- Interconnection security
 - Signaling/media attack defense: The SE2900 provides IP layer attack defense and signaling DoS/DDoS attack defense to prevent network attacks launched by unauthorized users.
 - Call admission control (CAC): The CAC feature allows carriers to restrict the number of concurrent calls per user based on the source IP address, preventing the overuse of resources. The CAC feature also allows carriers to set the call rate threshold and discard the packets that have call rates greater than the thresholds, protecting carrier network devices from attacks.
 - Topology hiding: The SE2900, deployed between two interconnected networks, isolates the networks from each other so that UEs on either network cannot learn the topology of the other network. The SE2900 performs topology hiding in message processing at the IP layer, UDP/IP layer, and signaling layer. The SE2900 provides topology hiding during message processing at the network and application layers. This function enables the SE2900 to replace the address, port, and header information in messages to ensure core network security.
- Call management
 - Signaling and media detection: If a fault occurs, there is a probability that signaling is unavailable but media streams are not released or media streams are unavailable but signaling is not released, resulting in an extra-long call detail record (CDR). With the session timer, abnormal sessions can be terminated in time, thereby ensuring accurate charging and avoiding unnecessary loss to users.
 - Charging
 - CDR reporting: The SE2900 sends Diameter Apply Charging Report (ACR) messages to the charging collection function (CCF), namely iCG9815. Based on the charging information, the CCF generates charging data records (CDRs), compares the CDRs with those generated by other NEs, and sends the CDRs to the billing center (BC). Generally, session durations in CDRs are compared.
 - Local charging: The SE2900 sends Diameter ACR messages to its CCF. Based on the charging information, the CCF generates CDRs and then consolidates, sorts, and filters the CDRs, and finally sends the CDRs to the BC.
- Flexible routing
 - Route header-based routing

The SE2900 uses the IP address carried in the Route header as the next-hop IP address and forwards messages accordingly.
 - ENUM query-based routing

The SE2900 sends an E.164 number to the ENUM server and determines the route based on the URI returned by the ENUM server.
 - DNS query-based routing

The SE2900 queries the domain name carried in the Request-URI or the Route header against the DNS server and forwards messages to the IP address returned by the DNS server.
 - Route selection name-based routing
 - The SE2900 routes messages based on the number in the TEL URI/TEL URL carried in the Request-URI.
 - The SE2900 routes messages based on the SIP URI (content and domain name format) carried in the Request-URI or Route header.
 - The SE2900 routes messages based on the **tgrp** parameter and the optional **trunk-context** parameter in the Request-URI.

- Route selection source code-based routing
The SE2900 selects the route based on the calling number and incoming trunk group.
- User type-based routing
The SE2900 determines the routes based on caller types.
- Media type-based routing
The SE2900 determines routes based on the types of media transmitted over the routes.
- Call type-based routing
The SE2900 determines routes based on call types.
- Codec-based routing
The SE2900 determines the routes based on the codecs carried in SDP information.
- Message type-based routing
The SE2900 determines the routes based on types of SIP messages.
- Validity period of the flexible routing policy
After the validity period of the flexible routing policy is specified, the SE2900 enables flexible routing as scheduled.
- Call status-based routing
The SE2900 selects a trunk group with the least number of concurrent calls or lowest call rate in the route to forward messages of a call based on the call status.
- Rerouting upon routing failures
The SE2900 reselects a route after receiving an OXX response from the outgoing office direction based on configured policies.
- QoS-based routing
To improve QoS quality, the SE2900 forwards packets along a route that is selected based on real-time QoS information.
- Signaling/media interworking
 - Media interworking
Audio transcoding: The SE2900 supports audio transcoding for the UEs that are on different networks and use different codecs to access the IMS and CS (2G/3G) networks. This function enables carriers to lower their capital expenditure (CAPEX) and operating expenditure (OPEX) by implementing signaling and media interworking between heterogeneous networks. There is no need to deploy a separate audio transcoding device.
 - Signaling interworking
 - SIP/SIP-I/SIP-T interworking: The SIP/SIP-I/SIP-T interworking feature allows the SE2900 to serve as an IP interworking gateway for IMS, NGN, CS networks, and IP PBXs, and to provide basic voice services and supplementary services for various networks.
 - Table 7-1 lists the functions of the interworking between SIP and H.323, H.323 and H.323, and SIP-I and H.323.

Table 7-1 Interworking between SIP and H.323, H.323 and H.323, and SIP-I and H.323

Service Type	Function
--------------	----------

Service Type	Function
Basic service	<p>The SE2900 supports basic calls for which the interworking between SIP and H.323, H.323 and H.323, and SIP-I and H.323 is implemented.</p> <ul style="list-style-type: none"> • Supports SIP-to-H.323 and H.323-to-SIP audio and video calls established in fast start and normal start modes but does not support the backup of such calls. <ul style="list-style-type: none"> – Sends SIP OPTIONS messages at intervals. Once receiving an SIP OPTIONS message, the core server returns a 200 OK response. – Supports flexible routing. – Calling/called number-based routing, CIC/RN parameter-based routing, user type-based routing, media type-based routing, and call type-based routing for SIP-to-H.323 calls – Calling/called number-based routing and media type-based routing for H.323-to-SIP calls and redirection of the initial INVITE request of such a call to a non-H.323 trunk group for route reselection if the call fails – Supports codecs. – Audio codecs G.711a, G.711u, G.722, G.728, G.723.1, G.729a, and G.729 – Video codecs H.261, H.263, and H.264 • The SE2900 supports audio transcoding on the SIP network side. For the codecs that can be converted, see 4.4.20 Audio Transcoding. • SIP and H.323 UEs can initiate audio and video calls in slow or fast start mode. • Supports SIP-I-to-H.323 or H.323-to-SIP-I calls.
Supplementary services	<p>The SE2900 supports call forwarding services for calls originated from the SIP and H.323 networks.</p> <ul style="list-style-type: none"> • In a call destined for the H.323 network, the GK sends a FACILITY message to inform the caller of the ongoing call forwarding. • In a call destined for the SIP network, the SBC sends a FACILITY message that is converted from a received 181 response to inform the caller of the ongoing call forwarding.
Fax	<p>The SE2900 supports T.38 fax switching services for SIP-H.323 interworking.</p> <ul style="list-style-type: none"> • Supports switching from audio services to T.38 fax services but not switching from T.38 fax services to audio services. • Supports fax switching initiated using media negotiation for SIP-to-H.323 and H.323-to-SIP calls established in fast and normal modes.
Video conference	<p>The SE2900 supports the access from SIP and H.323 UEs to video conferences.</p> <ul style="list-style-type: none"> • Supports the invitation of H.323 UEs to join the video conference during a call established in forced normal start or normal start mode. After the H.323 joins the video conference, auxiliary streams are controlled using binary floor control protocol (BFCP). • Supports the reuse of established TCP links for the transmission of BFCP packets during call renegotiation. At the SIP network side, the SE2900 converts BFCP messages to H.323 messages to implement the BFCP

Service Type	Function
	negotiation.

For details, see 4.1 Feature Matrix.

7.5 SE2900 on the NGN

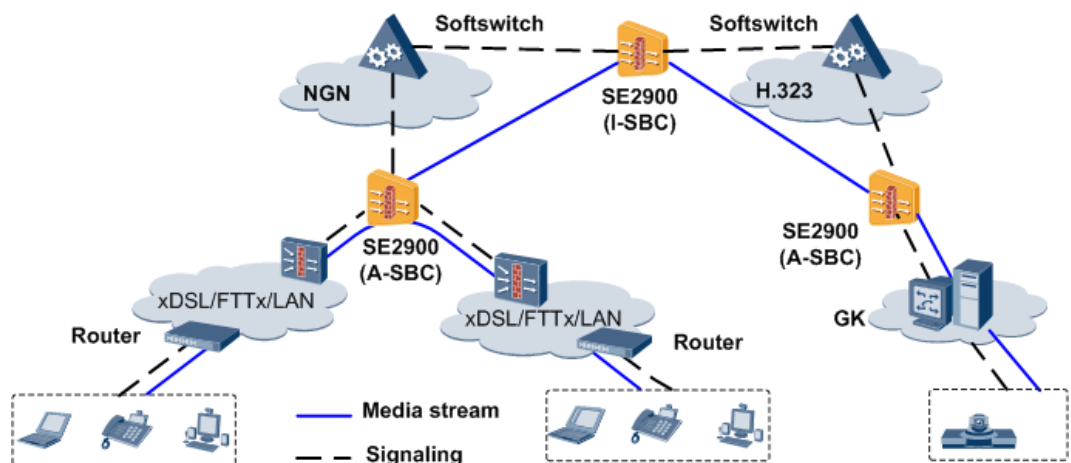
An NGN combines a TDM-based voice network and an IP/ATM-based packet network. It can provide integrated services, such as voice, video and data services. As networks evolve towards all-IP, the access network, MAN, and WAN develop into IP-based networks. The NGN uses the all-IP network architecture, meeting increasing service demands, improving carrier networks' comprehensive competitiveness, achieving sustainable development.

The NGN accommodates various access technologies (such as xDSL and Wi-Fi) and provides services to diverse UEs. Therefore, the NGN must effectively address the following problems:

- The emergence of more intelligent UEs and the growing integration of services present serious security issues and challenges to the core network. Ensuring network and user information security is the top concern for network deployment.
- How to ensure synchronous processing of media resources and signaling control to prevent high resource usage in the case of separation between bearer control and call control.
- How to use network bandwidth properly so as to prevent bandwidth overuse.

To address these problems and solve issues, such as security and signaling/media proxy, the SE2900 can be deployed between the core network and access network as shown in Figure 7-5.

Figure 7-5 SE2900 on the NGN



FTTx: fiber to the x

LAN: local area network

GK: gatekeeper

SBC: session border controller

xDSL: x digital subscriber line

-

On the NGN, the SE2900 provides the following functions:

- Access/interworking security
 - Data encryption: The SE2900 deployed between UEs and the core network uses SIP over TLS to enhance the security of data transmission between NGN UEs.
 - Signaling/media attack defense: The SE2900 provides IP layer attack defense, signaling DoS/DDoS attack defense, and media pinholing firewall to prevent network attacks launched by unauthorized users.
 - CAC: The CAC feature allows carriers to restrict the number of concurrent calls per user based on the source IP address, preventing the overuse of resources. The CAC feature also allows carriers to set the registration and call rate thresholds and discard the packets that have registration and call rates greater than the thresholds, protecting carrier network devices from attacks.
 - Topology hiding: Deployed between the public network and private network, the SE2900 hides the core network topology from the access network and hides the access network topology from the core network. The SE2900 performs topology hiding in the processing of messages at the IP layer, transport layer, and signaling layer. With the topology hiding function, the SE2900 translates between access-side addresses and core-side addresses to ensure the information security of the core network.
 - Audio transcoding: The SE2900 supports audio transcoding for the UEs that are on the SIP/H.323 network and use different codecs to access the NGN. This function enables carriers to lower their capital expenditure (CAPEX) and operating expenditure (OPEX) by implementing signaling and media interworking between different network types. There is no need to deploy a separate audio transcoding device.
- Call management

On the NGN, the SE2900 serves as a signaling proxy, media proxy, and network interworking gateway to detect signaling and media streams in NGN services. If a fault occurs, there is a probability that signaling is unavailable but media streams are not released or media streams are unavailable but signaling is not released, resulting in an extra-long call detail record (CDR). With the session timer or no media stream detection feature, abnormal sessions can be terminated in time, thereby ensuring accurate charging and avoiding unnecessary loss to users.
- Bandwidth management

The SE2900 provides session-based QoS assurance for real-time sessions. This is implemented by allocating a fixed amount of bandwidth to each NGN session according to the codec type in each session to prevent bandwidth overuse or theft by unauthorized users.

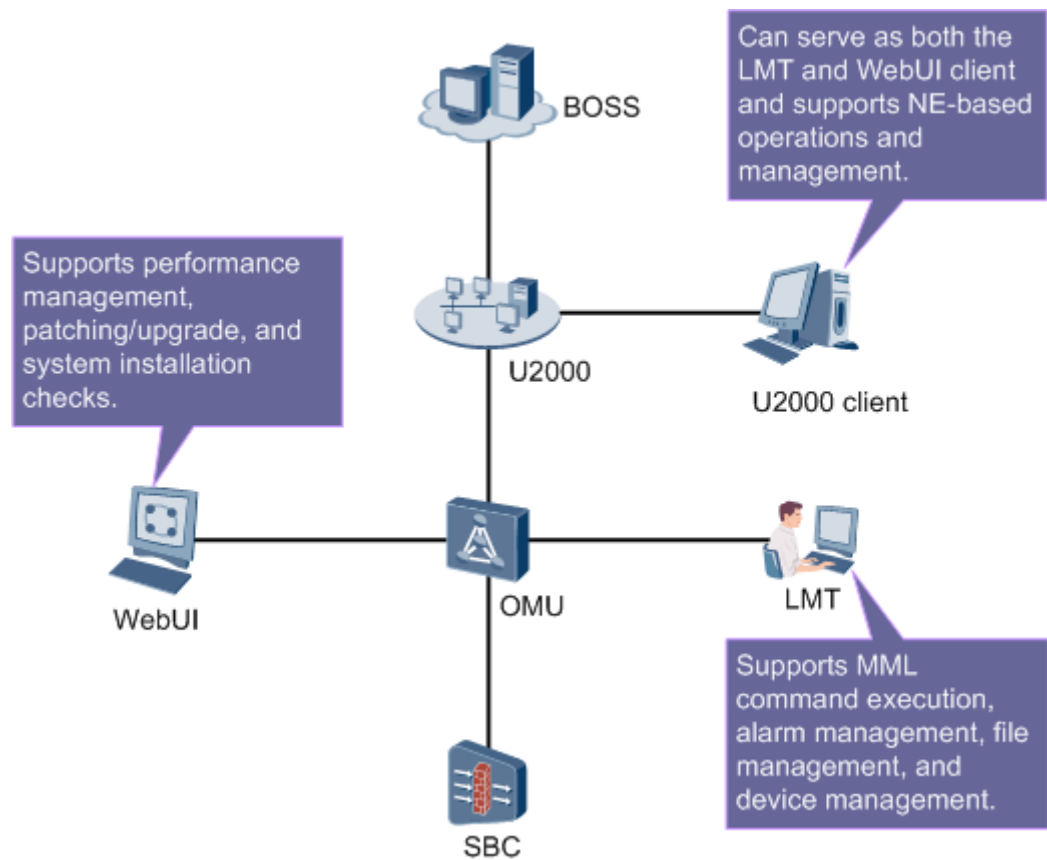
The SE2900 also provides basic functions for NGN networking. For details, see 4.1 Feature Matrix.

8 Operation and Maintenance

About This Chapter

The SE2900 can be managed by the OMU or U2000. The U2000 client can serve as both the LMT and web user interface (WebUI) client. The U2000 client or OMU enables users to perform alarm handling, performance management, and command configurations for the SE2900, as shown in Figure 8-1.

Figure 8-1 Operation and maintenance



After receiving an operation instruction from the U2000, the OMU runs commands on the SE2900 through a northbound interface (NBI) according to the instruction. After receiving alarm and log information reported by the SBC, the OMU forwards it to the U2000 for centralized management.


- 8.1 Fault Management
- 8.2 Configuration Management
- 8.3 Performance Management
- 8.4 Security Management
- 8.5 Charging Management

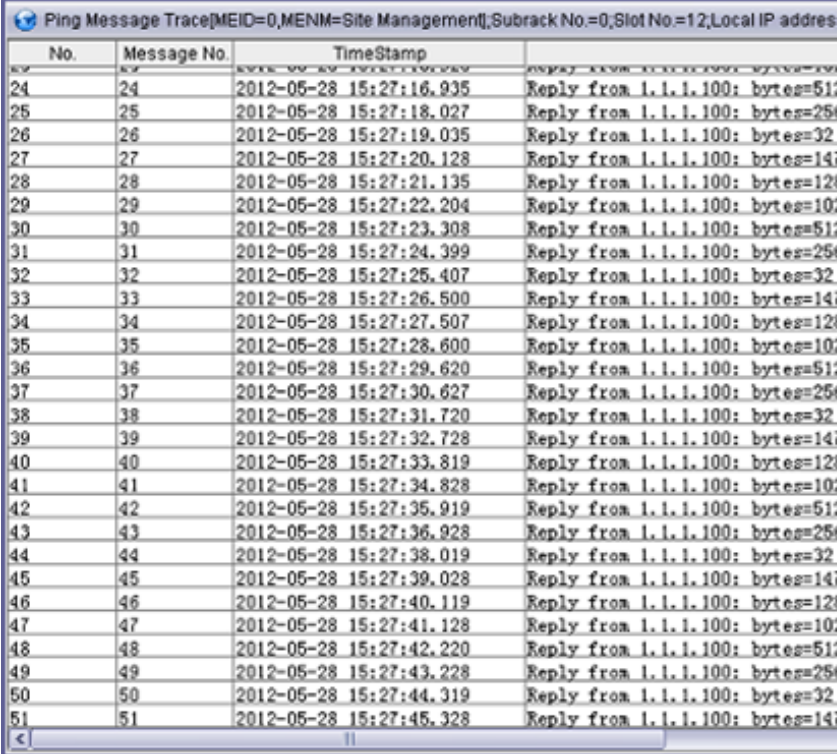
8.1 Fault Management

Fault management involves fault detection, fault locating, and troubleshooting. SBCs provide tools that assist maintenance personnel in preventive maintenance on the system. The fault management of the SE2900 comprises the system self-check, alarm management, maintenance management, message tracing, and fault location, as listed in Table 8-1.

Table 8-1 Fault management

Function	Description
System Self-Check	The SE2900 periodically checks the system resource usage and load status, and automatically rectifies faults, thereby minimizing the impact caused by faults.
Alarm management	The alarm management system provides the following alarm management functions: <ul style="list-style-type: none"> • Detects and reports any device fault or abnormality to the EMS in real time; generates audible and visual alarm signals through the alarm terminal devices, such as the alarm box or alarm subsystem, based on the alarm type and severity; sends the parsed alarm messages to the EMS through the NM interface. <p>Figure 8-2 Alarm browsing</p>

Function	Description
	 <ul style="list-style-type: none"> • Saves alarm information and enables maintenance personnel to view historical alarm records and configure alarm handling methods. When the CPU usage is high, relevant CPU thresholds are displayed in the alarms reported to the EMS. • Displays alarm handling suggestions on the alarm subsystem, which helps users troubleshoot device faults efficiently.
Maintenance management	<p>Maintenance management is the basic function of the OMU O&M system. Most routine maintenance commands can be executed through the MML or GUI.</p> <p>By performing operations such as query, view, switch, reset, deactivate, block, and activate through the OMU O&M system, you can efficiently manage and maintain the hardware, system resources, and physical interfaces of the SE2900.</p>
Message trace	<p>The OMU O&M system provides GUIs for message trace and allows data verification and fault rectification by tracing interfaces or signaling messages.</p> <p>Figure 8-3 Message trace</p>

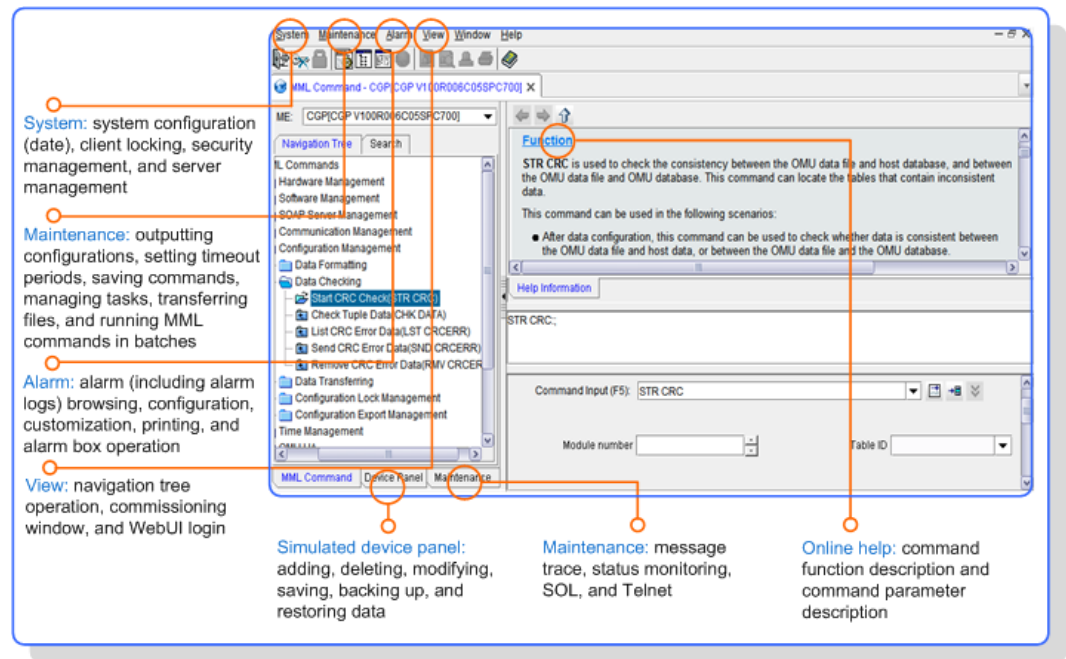
Function	Description
	 <p> <ul style="list-style-type: none"> • Provides standard interface-specific message trace, such as SIP message trace. • Provides the message explanation function, which explains traced interface or signaling messages in detail. <p>The SE2900 provides online and offline trace view and exports message trace results to the LMT for online or offline query.</p> <p>The SE2900 also supports E2E message trace on the element management system (EMS), which allows operators to locate faults and improves fault locating efficiency.</p> </p>
Fault location	<p>The SE2900 supports the call history record (CHR) function, which helps the SE2900 save registration and call records. If a fault occurs during the registration or call procedure, the SE2900 provides policy-based control over diversified registration or call records and outputs the result to the third-party analysis tool, such as SmartNTA and Session Insight, reducing the scope of registration or call faults and improving fault location efficiency.</p>

8.2 Configuration Management

The SE2900 provides a configuration system that is based on the man-machine language (MML), an interface defined in compliance with ITU Z.301-Z.341 series recommendations

for managing network devices. MML commands are provided for users to monitor and manage the SE2900. The SE2900 uses a relational database to manage the configured data. It supports operations such as adding, deleting, modifying, saving, backing up, and restoring data. It allows users to effectively manage and maintain various types of data such as hardware data, signaling data, and module data. Figure 8-4 shows the Huawei operation and maintenance system.

Figure 8-4 Huawei operation and maintenance system



The SE2900 provides the following configuration management functions:

- Online and offline data configuration

NOTE

Using the Huawei operation and maintenance system in offline mode, you can edit MML command scripts and save the information to a local PC. The next time you log in to the client, you can directly run the scripts. Using Huawei operation and maintenance system in online mode, you can perform real-time maintenance and management as well as operations such as outputting configurations, setting timeout periods, saving commands, managing tasks, transferring files, and running MML commands in batches.

- Local and remote data configuration
- Online upgrade
- Data verification

NOTE

Data configuration is stored in the OMU database, data file, and service database. The system provides the cyclic redundancy check (CRC) function to ensure data consistency in the three locations. At 03:00 every day, the system automatically executes the CRC task.

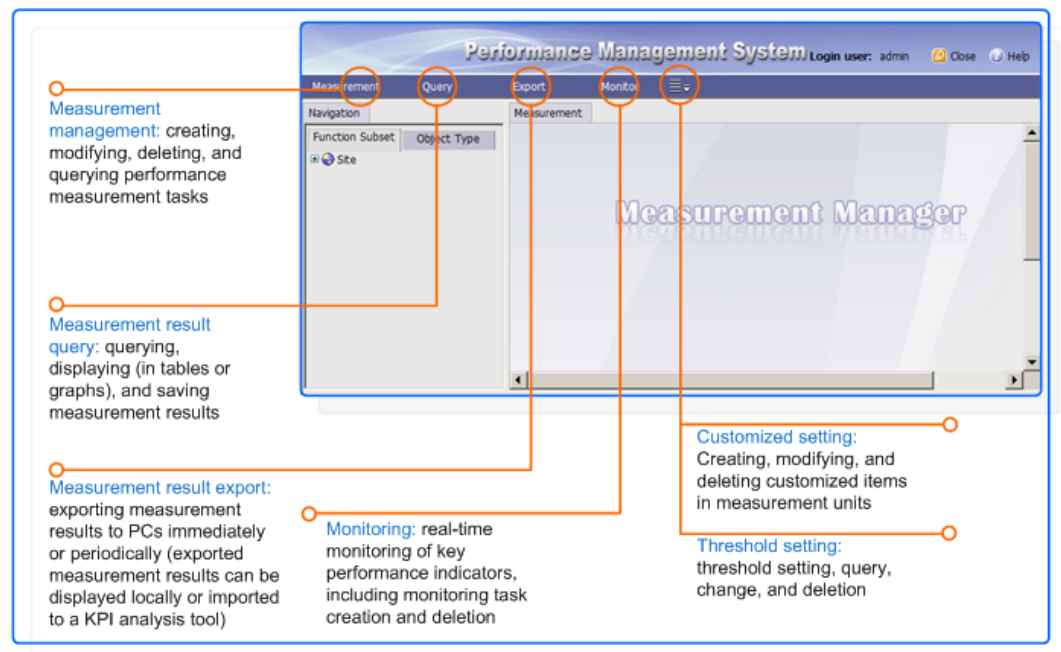
Configuration management on the SE2900 can be performed either using the local maintenance terminal (LMT) or the element management system (EMS).

8.3 Performance Management

The performance management system checks network devices and logical configurations to detect potential problems in a timely manner. Performance management involves generating, converting, collecting, storing, consolidating, and displaying the measurement data about the usage of system resources on the SE2900 and the running status of its peripheral network. Performance management provides reliable data for the operating management and fault locating of the SE2900 and the measurement, design, planning, and operation management of a network.

The performance management system of the SE2900 provides Web-based traffic measurement. It can measure the traffic in each direction for function entities, between different types of interworking devices, and on various links. The measurement provides data for users to learn about the operating status of devices, manage devices, and optimize network performance. Figure 8-5 shows the performance management system.

Figure 8-5 Performance management system



The performance management system provides the following functions:

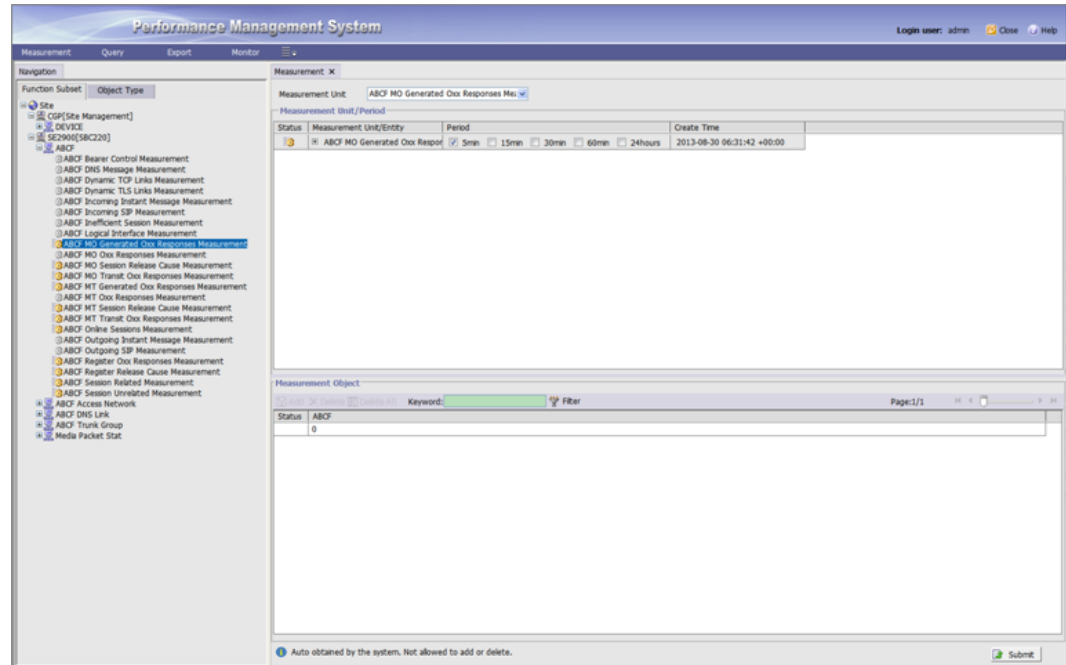
- Create, modify, run, suspend, delete, and query performance measurement tasks, as well as provide visualized performance measurement results.
- Re-analyze the measurement results and display them results in graphs and bar charts for future use.

The performance management system supports the creation of measurement tasks according to the measurement period specified by the system. Measurement entities are organized and managed by measurement units, which facilitate measurement entity management and maintenance personnel's operations.

For some common measurement entities, the system provides the default measurement function. After the OMU is installed and starts running, the system automatically measures these measurement entities. If the icon of a measurement unit is highlighted, the measurement

tasks of the measurement unit are running. If the icon is gray, no measurement task is running. Figure 8-6 shows the detail. Measurement units that support automatic measurement are defined by device manufacturers.

Figure 8-6 Measurement units



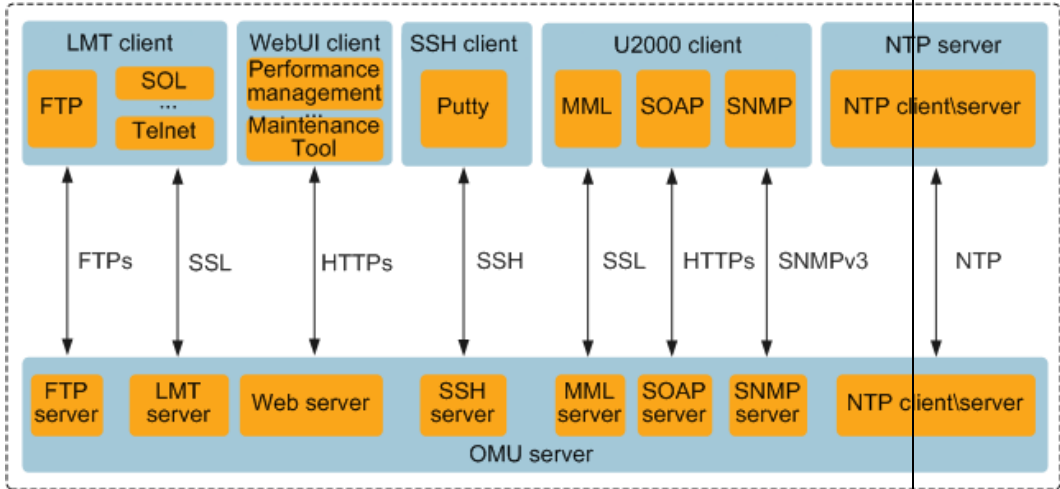
In addition, the performance management system provides the threshold alarm function that automatically monitors the network status and detects abnormal performance measurement data. Thresholds can be set by the measurement entity in a measurement task. If the measurement result of a measurement entity exceeds the threshold, the performance management system automatically reports a performance measurement task threshold alarm to the alarm system.

8.4 Security Management

The SE2900 operation and management (O&M) system is a multi-user system. This system manages user rights, logs, and user access to ensure that multiple users can securely and conveniently perform operations in the O&M system. Table 8-2 lists the security management functions.

Table 8-2 Security management functions

Function	Description
Rights management	Different levels of rights can be specified for operators and maintenance consoles. In the OMU O&M system, you can run an MML command only after gaining both operator rights and maintenance console rights.
Log manage	You can query man-machine language (MML) operation records using the SE2900 O&M system. You can check whether service-affecting operations are

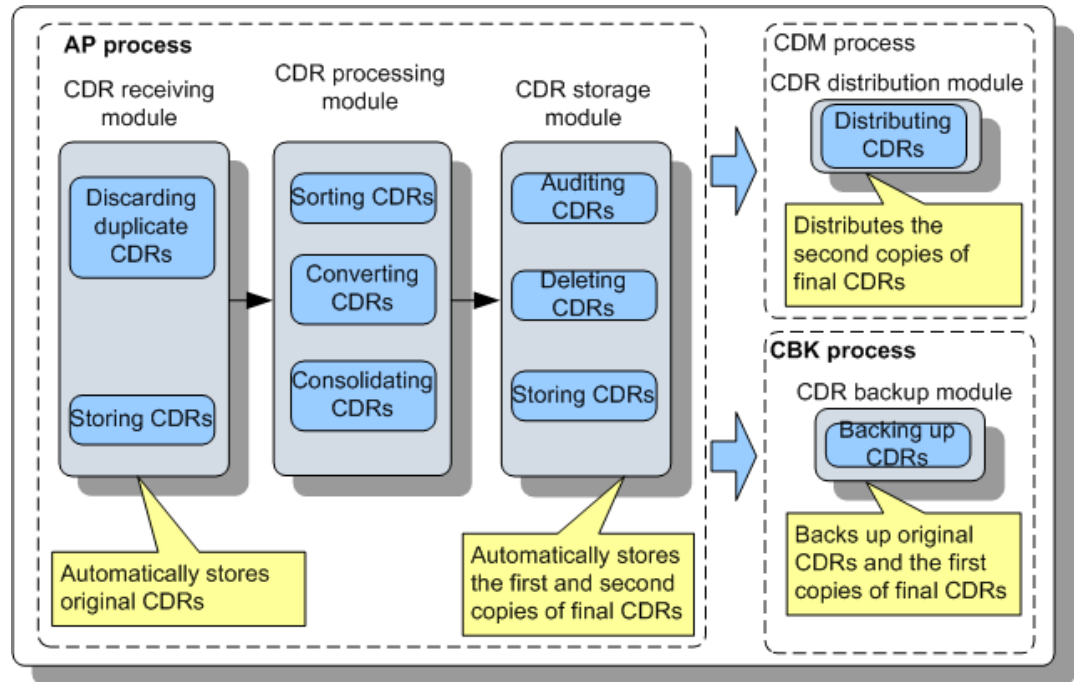
Function	Description
ment	performed on the SE2900 that cause a fault. The SE2900 O&M system provides security logs that record operations related to system security (for example, logging in to the LMT client). These logs help identify intrusions, restore the system, measure system resource usage, audit operations, and provide electronic evidence on operations.
Access management	<p>The OMU server provides multiple access interfaces for external devices, such as the LMT client, web user interface (WebUI) client, SSH client, EMS client, and NTP server. Terminals can access the OMU server of the SE2900 only after passing authorization and authentication.</p> <p>Figure 8-7 Access management</p> 

The OMU provides an access control mechanism: When the LMT, WebUI, or EMS client accesses the OMU server through different interfaces, the OMU server first verifies the account and password that are being used. If the account and password are correct and workstation management is enabled, the OMU server checks the IP address of the client. If the IP address is not contained in the accessible workstation list, the OMU server returns a login failure prompt "The accessible workstation list does not contain the IP address or port of the client."

8.5 Charging Management

The charging collection function (CCF) embedded in the SE2900 can generate and flexibly process charging data records (CDRs) to meet carriers' requirements. See Figure 8-8.

Figure 8-8 Processing CDRs



The access point process of the CCF handles CDRs, including receiving and sorting CDRs, as described in Table 8-3.

Table 8-3 Processing CDRs

Function	Description
Discarding duplicate CDRs	The iCG9815 performs online checks to discard duplicate original CDRs. This function is automatically implemented by the iCG9815 and does not require configuration.
Storing CDRs	CDRs are categorized as original and final CDRs. <ul style="list-style-type: none"> The iCG9815 saves accounting requests (ACRs) in files on a hard disk. These files are called original CDR files. The iCG9815 stores final CDRs in files on a hard disk. These files are called final CDR files. Configure CDR storage information as required, including storage time.
Sorting CDRs	The iCG9815 stores final CDRs in different channels based on sorting conditions, with each channel mapping to a level-1 or level-2 directory in the CDR storage path. This function is configurable. For example, users can configure sorting conditions.
Converting CDRs	The iCG9815 converts CDRs to the formats supported by a billing center (BC). During CDR conversion, CDRs in different formats are generated by invoking different format engine packages.

Function	Description
Consolidating CDRs	<p>The iCG9815 consolidates incoming accounting requests (ACRs) related to a session into a CDR supported by the BC.</p> <p>This function is automatically implemented by the iCG9815 and does not require configuration.</p>
Auditing CDRs	<p>The iCG9815 collects at 00:00 each day information about the second copies of final CDRs generated the previous day. The iCG9815 then generates logs based on the data and saves the logs in a path.</p> <p>This function is configurable. For example, users can configure the number of days that log files can be retained.</p>
Deleting CDRs	<p>The iCG9815 deletes CDRs when disk space is insufficient or when the CDRs are outdated.</p> <ul style="list-style-type: none"> • Deleting outdated CDRs Original and final CDRs are stored in files. Users can configure information about how long original and final CDRs can be retained. Before automatically deleting an outdated CDR, the iCG9815 checks whether the CDR has been processed. Unprocessed original CDRs are not deleted. • Automatically deleting CDRs in the case of insufficient disk space The iCG9815 monitors available disk space in real time. When the available disk space is less than 5% of the total disk space, the iCG9815 deletes the earliest CDRs to make room for new CDRs. <p>This function is configurable. For example, users can configure the number of days that CDRs can be retained.</p>

9 Technical Specifications

About This Chapter

- 9.1 Performance Specifications
- 9.2 Reliability Specifications
- 9.3 Power Consumption Specifications
- 9.4 Cabinet Specifications
- 9.5 Environment Specifications
- 9.6 EMC Specifications
- 9.7 Environment Requirements

9.1 Performance Specifications

Default traffic model (0.08Erl)

Table 9-1 lists the performance specifications of the SE2900 on the IMS.

Table 9-1 Performance specifications of the SE2900

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of registered audio	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
users supported by the A-SBC in the SIP over UDP scenario						
Maximum number of concurrent audio calls supported by the A-SBC in the SIP over UDP scenario	20,000	30,000	40,000	60,000	170,000	340,000
Maximum number of concurrent audio calls supported by the I-SBC in the SIP over UDP scenario	20,000	30,000	40,000	60,000	170,000	340,000
Maximum number of users for which SIP over TLS is	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
supported						
Maximum number of SRTP calls	10,000	15,000	20,000	30,000	85,000	170,000
Maximum number of calls for which MSRP proxy is supported	20,000	30,000	40,000	60,000	170,000	340,000
Maximum number of SIP over UDP users for which IMS-A KA/IPSec is supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000
Maximum number of SIP over TCP users for which IMS-A KA/IPSec is supported	125,000	175,000	250,000	350,000	1,000,000	2,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of concurrent audio calls for which SIP-H.323 interworking is supported (G.711A (20ms))	20,000	30,000	40,000	60,000	170,000	340,000
Number of concurrent audio/video calls for which SIP-H.323 interworking is supported (bandwidth: 500 kbit/s, video packet transmission rate: 60 pps)	10,000	15,000	20,000	30,000	85,000	170,000
Codec type	G.711 (including G.711A and G.711U), G.729 (including G.729A and G.729AB), G.723.1, G.722, internet low bit rate codec (iLBC), adaptive multirate (AMR), adaptive multirate wideband, and DTMF/2833					

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of VRF instances supported by the SE2900	4,095					
Maximum number of access-side IP addresses	6,000					



NOTE

The maximum number of VRF instances, maximum number of access-side IP addresses, and maximum number of ANs are independent of the number of subracks.

Table 9-2 shows the performance specifications of the SE2900 on the NGN

Table 9-2 Performance specifications of the SE2900 on the NGN

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of registered audio users supported by the	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
A-SBC in the SIP over UDP scenario						
Maximum number of concurrent calls supported by the A-SBC in the SIP over UDP scenario	20,000	30,000	40,000	60,000	170,000	340,000
Maximum number of concurrent calls supported by the I-SBC in the SIP over UDP scenario	20,000	30,000	40,000	60,000	170,000	340,000
Maximum number of users for which SIP over TLS is supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000
Maximum	10,000	15,000	20,000	30,000	85,000	170,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
number of SRTP calls						
Maximum number of concurrent audio calls for which SIP-H.323 interworking is supported (G.711A (20ms))	20,000	30,000	40,000	60,000	170,000	340,000
Number of concurrent audio/video calls for which SIP-H.323 interworking is supported (bandwidth: 500 kbit/s, video packet transmission rate: 60 pps)	10,000	15,000	20,000	30,000	85,000	170,000
Codec	G.711 (including G.711A and G.711U), G.729 (including G.729A and					

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
type	G.729AB), G.723.1, G.722, internet low bit rate codec (iLBC), adaptive multirate (AMR), adaptive multirate wideband, and DTMF/2833					
Maximum number of VRF instances supported by the SE2900	4,095					
Maximum number of access-side IP addresses	6,000					

Traffic model 1 (0.05Erl)

Table 9-3 lists the performance specifications of the SE2900 on the IMS.

Table 9-3 Performance specifications of the SE2900

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of registered audio users supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of concurrent audio calls supported by the A-SBC in the SIP over UDP scenario	12,000	18,000	24,000	36,000	102,000	204,000
Maximum number of concurrent audio calls supported by the I-SBC in the SIP over UDP scenario	12,000	18,000	24,000	36,000	102,000	204,000
Maximum number of users for which SIP over TLS is supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of SRTP calls	6,000	9,000	12,000	18,000	51,000	102,000
Maximum number of calls for which MSRP proxy is supported	12,000	18,000	24,000	36,000	102,000	204,000
Maximum number of SIP over UDP users for which IMS-A KA/IPSec is supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000
Maximum number of SIP over TCP users for which IMS-A KA/IPSec is supported	125,000	175,000	250,000	350,000	1,000,000	2,000,000
Maximum	12,000	18,000	24,000	36,000	102,000	204,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
number of concurrent audio calls for which SIP-H.323 interworking is supported (G.711A (20 ms))						
Number of concurrent audio/video calls for which SIP-H.323 interworking is supported (bandwidth: 500 kbit/s, video packet transmission rate: 60 pps)	6,000	9,000	12,000	18,000	51,000	102,000
Codec type	G.711 (including G.711A and G.711U), G.729 (including G.729A and G.729AB), G.723.1, G.722, internet low bit rate codec (iLBC), adaptive multirate (AMR), adaptive multirate wideband, and DTMF/2833					
Maximum number	4,095					

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
of VRF instances supported by the SE2900						
Maximum number of access-side IP addresses	6,000					



NOTE

The maximum number of VRF instances, maximum number of access-side IP addresses, and maximum number of ANs are independent of the number of subracks.

Table 9-4 shows the performance specifications of the SE2900 on the NGN

Table 9-4 Performance specifications of the SE2900 on the NGN

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of registered audio users supported by the A-SBC in the SIP over	250,000	350,000	500,000	700,000	2,000,000	4,000,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
UDP scenario						
Maximum number of concurrent calls supported by the A-SBC in the SIP over UDP scenario	12,000	18,000	24,000	36,000	102,000	204,000
Maximum number of concurrent calls supported by the I-SBC in the SIP over UDP scenario	12,000	18,000	24,000	36,000	102,000	204,000
Maximum number of users for which SIP over TLS is supported	250,000	350,000	500,000	700,000	2,000,000	4,000,000
Maximum number of SRTP calls	6,000	9,000	12,000	18,000	51,000	102,000

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of concurrent audio calls for which SIP-H.323 interworking is supported (G.711A (20ms))	12,000	18,000	24,000	36,000	102,000	204,000
Number of concurrent audio/video calls for which SIP-H.323 interworking is supported (bandwidth: 500 kbit/s, video packet transmission rate: 60 pps)	6,000	9,000	12,000	18,000	51,000	102,000
Codec type	G.711 (including G.711A and G.711U), G.729 (including G.729A and G.729AB), G.723.1, G.722, internet low bit rate codec (iLBC), adaptive multirate (AMR), adaptive multirate wideband, and DTMF/2833					

Item	Specifications (One Subrack)				Specifications (Three-Subrack Cascading)	
	SPUA0 (Single-CPU Board)		SPUA1 (Dual-CPU Board)		SPUA0 (Single-CPU Board)	SPUA1 (Dual-CPU Board)
	ISU	ESU	ISU	ESU		
Maximum number of VRF instances supported by the SE2900	4,095					
Maximum number of access-side IP addresses	6,000					

9.2 Reliability Specifications

Table 9-5 shows the reliability specifications of the SE2900.

Table 9-5 Reliability specifications of the SE2900

Item	Specifications
Annual return and repair rate of replaceable units	≤ 1.5%
System availability	≥ 99.99953%
Fault detection rate	> 95%
MTTR	≤ 60 minutes
Downtime	< 3 minutes/year
MTBF	<ul style="list-style-type: none"> ≥ 24 years (in full configuration) ≥ 42 years (only one subrack)
SPU Board restart time	< 5 minutes
VPU Board restart time	< 5 minutes

Item	Specifications
Process switchover time	< 5s
Single-subrack startup time	< 10 minutes
System restart time (in full configuration)	< 10 minutes

9.3 Power Consumption Specifications

Power Supply

Rated voltage: -48 V/-60 V DC

Voltage range: -40 V DC to -57 V DC/-50 V DC to -72 V DC

System Power Consumption

Table 9-6 lists the power consumption specifications of the SE2900 when 9.5 Environment Specifications are met.



NOTE

The maximum power applies when the maximum CPU usage is 95%, and the typical power applies when the average CPU usage is 60%.

Table 9-6 Power consumption specifications of the SE2900

Item	Maximum Power (W)	Typical Power (W)
Cabinet (SPUA0 full configuration in three subracks)	3900	2815
Cabinet (SPUA1 full configuration in three subracks)	5100	3955
Subrack (with four pairs of SPUA0s and two pairs of VPUA0s installed)	3960	2875
Subrack (with four pairs of SPUA10s and two pairs of VPUA1s installed)	5320	4198
Subrack (with three pairs of SPUA0s and three pairs of VPUA0s installed)	3990	2905

Item	Maximum Power (W)	Typical Power (W)
Subrack (with three pairs of SPUA1s and three pairs of VPUA1s installed)	6840	5545
Subrack (SPUZ0 full configuration in a subrack)	1290	930
Subrack (SPUA0 full configuration in a subrack)	1290	930
Subrack (SPUA1 full configuration in a subrack)	1690	1310
Subrack (with one pair of SPUA0s and one pair of VPUA0s installed)	1320	960
Subrack (with one pair of SPUA1s and one pair of VPUA1s installed)	1800	1430
MXUA0	125	105
SPUZ0	190	170
SPUA0	190	170
SPUA1	290	265
VPUA0	205	185
VPUA1	345	325
Fan	140	20

9.4 Cabinet Specifications

Table 9-7 lists the N68E-22 cabinet specifications.

Table 9-7 N68E-22 cabinet specifications

Item	Specification or Model
Cabinet model	N68E-22
Cabinet dimensions (H x W)	2200 mm x 600 mm x 800 mm

Item	Specification or Model
x D)	
Subrack dimensions (H x W x D)	130.5 mm x 442 mm x 675 mm
Number of subracks in full configuration	3
Cabinet weight (vacant but with front and rear doors)	120kg
Cabinet weight (fully configured with SPUA0s/SPUA1s)	300kg
Cabinet weight (with four pairs of SPUA0s and two pairs of VPUA0s installed)	296kg
Cabinet weight (with four pairs of SPUA1s and two pairs of VPUA1s installed)	298kg
Cabinet weight (with three pairs of SPUA0s and three pairs of VPUA0s installed)	294kg
Cabinet weight (with three pairs of SPUA1s and three pairs of VPUA1s installed)	297kg
Subrack weight (fully configured with SPUZ0s)	47.8kg
Load-bearing capability of the floor in the equipment room	600 kg/m ²
Available height inside the cabinet	46U (1U = 44.45 mm)

9.5 Environment Specifications

The environment specifications of the SE2900 include environment adaptability specifications and noise specifications.

1. Environment adaptability specifications

Table 9-8 lists the long-term environment adaptability specifications of the SE2900.

Table 9-8 Environment adaptability specifications

Item	Value
------	-------

Item	Value
Altitude	≤ 4000 m
Atmospheric pressure	70 kPa to 106 kPa
Temperature	+5°C to +40°C
Relative humidity	5% RH to 85% RH
Quakeproof capability	Earthquakes measuring 7-9 on the Richter scale

2. Noise specifications

Table 9-9 lists the noise specifications of the SE2900.

Table 9-9 Noise specifications

Item	Value
Noise (acoustic power)	≤ 78 dBA (27°C)
	≤ 72 dBA (23°C ± 2°C)

9.6 EMC Specifications

The ElectroMagnetic Compatibility (EMC) specifications of the SE2900 include:

1. Electromagnetic interference (EMI) specifications
 - Conducted emission (CE)

Table 9-10 CE specifications of the -48 V or -60 V power supply port

Frequency Range	Limits	
	Average Limit	Quasi-Peak Limit
0.15 to 0.50 MHz	66 dBμV/m	79 dBμV/m
0.50 to 30 MHz	60 dBμV/m	73 dBμV/m
NOTE The CE specifications quantitatively indicate the interference signals conducted from the cable ports of the equipment.		

- Radiated emission (RE)

Table 9-11 RE specifications

Frequency Range	Quasi-Peak Limit
-----------------	------------------

Frequency Range	Quasi-Peak Limit
30 to 230 MHz	50 dB μ V/m
230 to 1000 MHz	57 dB μ V/m
NOTE <ul style="list-style-type: none"> The RE specifications quantitatively indicate the interference signals radiated from the ports on the shell of the equipment. The measurement point is three meters away from the equipment. 	

2. EMS specifications

- Conducted susceptibility (CS)

These specifications apply to -48 V or -60 V DC power cables and particular signal cables (the connection cable between the ports exceeds three meters).

Table 9-12 CS specifications

Tested Item	Frequency Range	Voltage	Performance Grade
DC power cable port	150 kHz to 80 MHz	10 V	A
Signal cable port	150 kHz to 230 MHz	10 V	A
NOTE The CS specifications quantitatively indicate the capability of the equipment in resisting the interference generated by coupling the ports of the cables.			

- Radiated susceptibility (RS)

Table 9-13 RS specifications

Frequency Range	Voltage	Performance Grade
80 MHz to 2.7 GHz	10 V/m	A
NOTE The RS specifications quantitatively indicate the capability of the equipment in resisting the interference generated by coupling ports on the shell of the equipment.		

- Electrostatic discharge (ESD)

These specifications apply to the ESD sources, including human activities, which may damage the components (such as boards, subracks, and cabinet enclosure) of the equipment.

Table 9-14 ESD specifications

Tested Item	Voltage	Performance Grade
Air discharge	8 kV	B
	15 kV	R
Contact discharge	6 kV	B
	8 kV	R
NOTE The ESD specifications quantitatively indicate the capability of the equipment in resisting the ESD, including contact discharge and air discharge.		

- Electrical fast transient (EFT)

These specifications are applicable to DC power cables and particular signal cables (the connection cable between the ports exceeds three meters).

Table 9-15 EFT specifications

Tested Item	Voltage	Performance Grade
DC power cable port	1 kV	B
Signal cable port	1 kV	B
NOTE The EFT specifications quantitatively indicate the impact of the high-frequency low-energy impulse generated by an inductive load changeover on the equipment.		

- Surge

These specifications apply to DC power cables and certain signal cables, such as indoor signal cables and E1 lines.

Table 9-16 Surge specifications

Tested Item	Voltage	Performance Grade
DC power cable port	1 kV (wire to wire), 2 kV (wire to ground)	B
Signal cable port	Indoor cables (cables inside the system) 1 kV	B

9.7 Environment Requirements

The environment requirements consist of requirements related to the storage environment, transportation environment, and operating environment. The requirements are defined on the basis of the following standards:

- Storage environment: ETS 300 019-1-1 Class 1.2
- Transportation environment: ETSI EN 300 019-1-2 Class 2.3
- Operating environment: ETSI EN 300 019-1-3 Class 3.1

9.7.1 Storage Environment

1. Climatic requirements

Table 9-17 lists the climatic requirements for storing the SE2900.

Table 9-17 Climatic requirements

Item	Scope
Temperature	-40°C to +70°C
Temperature change rate	≤ 1°C/min
Relative humidity	10% RH to 95% RH
Altitude	≤ 5000m
Atmospheric pressure	70 kPa to 106 kPa
Solar radiation	≤ 1120 W/m ²
Heat radiation	≤ 600 W/m ²
Wind speed	≤ 30 m/s

2. Waterproofing requirements

Table 9-18 lists the waterproofing requirements for storing the SE2900.

Table 9-18 Waterproofing requirements

Location	Description
Stored inside the equipment room	There must not be any water on the ground or any other place in the equipment room to prevent water from dampening the equipment. The equipment must be placed away from fire-extinguishing devices and heating pipes that may damage the equipment.
Stored outside the equipment room	The package must be preserved properly. Waterproof measures should be taken to protect the package against rainfall. No water should be found on the ground where the package is placed and water must not seep into the package.

Location	Description
	The package is not exposed to sunlight.

3. Biological requirements
 - There is no any propagation of fungus, mildew or other microorganism.
 - There are no rodents, such as mice, in the equipment room.
4. Air cleanliness requirements
 - The equipment room is free of explosive, conductive, magneto conductive, or corrosive dust.
 - Table 9-19 lists the density requirements for mechanically active substances.

Table 9-19 Density requirements for mechanically active substances

Mechanically Active Substance	Content	Unit
Suspended dust	≤ 5.00	mg/m ³
Deposited dust	≤ 20.0	mg/m ² ·h
Sand	≤ 300	mg/m ³
NOTE <ul style="list-style-type: none"> • Suspended dust: diameter $\leq 75 \mu\text{m}$ • Deposited dust: $75 \mu\text{m} \leq \text{diameter} \leq 150 \mu\text{m}$ • Sand: $150 \mu\text{m} \leq \text{diameter} \leq 1000 \mu\text{m}$ 		

- Table 9-20 lists the density requirements for chemically active substances.

Table 9-20 Density requirements for chemically active substances

Chemically Active Substances	Content	Unit
SO ₂	≤ 0.30	mg/m ³
H ₂ S	≤ 0.10	mg/m ³
NO ₂	≤ 0.50	mg/m ³
NH ₃	≤ 1.00	mg/m ³
Cl ₂	≤ 0.10	mg/m ³
HCl	≤ 0.10	mg/m ³
HF	≤ 0.01	mg/m ³
O ₃	≤ 0.05	mg/m ³

5. Mechanical stress requirements

Table 9-21 lists the mechanical stress requirements for storing the SE2900.

Table 9-21 Mechanical stress requirements

Item	Subitem	Vibration Frequency for the Fixed Shift	Vibration Frequency for the Fixed Acceleration
Sinusoidal vibration	Offset	≤ 7.0 mm	-
	Acceleration	-	≤ 20.0 m/s ²
	Frequency range	2 Hz to 9 Hz	9 Hz to 200 Hz
Non-stable impulse	Shock response spectrum (SRS) II	≤ 250 m/s ²	
	Static payload	≤ 5 kPa	
<p>NOTE</p> <ul style="list-style-type: none"> • SRS Refers to the response curve of the maximum acceleration generated by the device under the specified impulse motivation. SRS II means that the duration of half-sine impulse response spectrum is 6 ms. • Static payload Refers to the capability of the equipment in package to bear the pressure from the top in normal pile-up method. 			

9.7.2 Transportation Environment

1. Climatic requirements

Table 9-22 lists the climatic requirements for transporting the SE2900.

Table 9-22 Climatic requirements

Item	Scope
Temperature	-40°C to +70°C
Temperature change rate	≤ 3°C/min
Relative humidity	5% RH to 100% RH
Altitude	≤ 5000 m
Atmospheric pressure	70 kPa to 106 kPa
Solar radiation	≤ 1120 W/m ²
Heat radiation	≤ 600 W/m ²
Wind speed	≤ 30 m/s

2. Waterproofing requirements

The waterproofing requirements for transporting the SE2900 are as follows:

- The package is intact.
- Waterproofing measures should be taken in transportation vehicles to prevent rainwater from leaking into the package.
- There is no water inside the transportation vehicles.

3. Biological requirements

- There is no any propagation of fungus, mildew or other microorganism.
- There are no rodents, such as rats.

4. Air cleanliness requirements

- The transportation environment is free of explosive, conductive, magneto conductive, or corrosive dust.
- Table 9-23 lists the density requirements for mechanically active substances.

Table 9-23 Density requirements for mechanically active substances

Mechanically Active Substance	Content	Unit
Suspended dust	Not applicable	mg/m ³
Deposited dust	≤ 3.0	mg/m ² ·h
Sand	≤ 100	mg/m ³
NOTE <ul style="list-style-type: none"> • Suspended dust: diameter ≤ 75 μm • Deposited dust: 75 μm ≤ diameter ≤ 150 μm • Sand: 150 μm ≤ diameter ≤ 1000 μm 		

- Table 9-24 lists the density requirements for chemically active substances.

Table 9-24 Density requirements for chemically active substances

Chemically Active Substances	Content	Unit
SO ₂	≤ 0.30	mg/m ³
H ₂ S	≤ 0.10	mg/m ³
NO ₂	≤ 0.50	mg/m ³
NH ₃	≤ 1.00	mg/m ³
Cl ₂	≤ 0.10	mg/m ³
HCl	≤ 0.10	mg/m ³
HF	≤ 0.01	mg/m ³

Chemically Active Substances	Content	Unit
O ₃	≤ 0.05	mg/m ³

5. Mechanical stress requirements

Table 9-25 lists the mechanical stress requirements for transporting the SE2900.

Table 9-25 Mechanical stress requirements

Item	Subitem	Vibration Frequency for the Fixed Shift	Vibration Frequency for the Fixed Acceleration	Vibration Frequency for the Fixed Acceleration
Sinusoidal vibration	Offset	≤ 7.5 mm	-	-
	Acceleration	-	≤ 20.0 m/s ²	≤ 40.0 m/s ²
	Frequency range	2 Hz to 9 Hz	9 Hz to 200 Hz	200 Hz to 500 Hz
Random vibration	Acceleration spectral density (ASD)	10 m ² /s ³	3 m ² /s ³	1 m ² /s ³
	Frequency range	2 Hz to 9 Hz	9 Hz to 200 Hz	200 Hz to 500 Hz
Non-stable impulse	Shock response spectrum (SRS) II	≤ 300 m/s ²		
	Static payload	≤ 10 kPa		
<p>NOTE</p> <ul style="list-style-type: none"> • SRS Refers to the response curve of the maximum acceleration generated by the device under the specified impulse motivation. SRS II means that the duration of half-sine impulse response spectrum is 6 ms. • Static payload Refers to the capability of the equipment in package to bear the pressure from the top in normal pile-up method. 				

9.7.3 Operating Environment

1. Climatic requirements

Table 9-26 lists the climatic requirements for operating the SE2900.

Table 9-26 Climatic requirements

Item	Scope
Temperature	+5°C to +40°C
Relative humidity	5% RH to 85% RH
Altitude	≤ 4000 m
Atmospheric pressure	70 kPa to 106 kPa
Temperature change rate	≤ 15°C/h
Solar radiation	≤700 W/m ²
Heat radiation	≤ 600 W/m ²
Wind speed	≤ 1 m/s

2. Biological requirements

- There is no any propagation of fungus, mildew or other microorganism.
- There are no rodents, such as rats.

3. Air cleanliness requirements

- The operating environment is free of explosive, conductive, magneto conductive, or corrosive dust.
- Table 9-27 lists the density requirements for mechanically active substances.

Table 9-27 Density requirements for mechanically active substances

Mechanically Active Substance	Content	Unit
Dust particles	≤ 3 x 10 ⁴ (No visible dust accumulates on the desktop within three days.)	Particles/m ³
NOTE Dust particle: diameter ≥ 5 μm		

- Table 9-28 lists the density requirements for chemically active substances.

Table 9-28 Density requirements for chemically active substances

Chemically Active Substances	Content	Unit
SO ₂	≤ 0.20	mg/m ³
H ₂ S	≤ 0.006	mg/m ³
NH ₃	≤ 0.05	mg/m ³

Chemically Active Substances	Content	Unit
Cl ₂	≤ 0.01	mg/m ³

4. Mechanical stress requirements

Table 9-29 lists the mechanical stress requirements for operating the SE2900.

Table 9-29 Mechanical stress requirements

Item	Subitem	Vibration Frequency for the Fixed Shift	Vibration Frequency for the Fixed Acceleration
Sinusoidal vibration	Offset	≤ 3.5 mm	-
	Acceleration	-	≤ 10.0 m/s ²
	Frequency range	5 Hz to 9 Hz	9 Hz to 200 Hz
Non-stable impulse	Shock response spectrum (SRS) II	≤ 100 m/s ²	
	Static payload	0	
<p>NOTE</p> <ul style="list-style-type: none"> • SRS Refers to the response curve of the maximum acceleration generated by the device under the specified impulse motivation. SRS II means that the duration of half-sine impulse response spectrum is 6 ms. • Static payload Refers to the capability of the equipment in package to bear the pressure from the top in normal pile-up method. 			

10 Differences Between the SE2900 and SE2600

The following tables describe the differences between the SE2900 and the SE2600 in key specifications, hardware, and software. The differences between the SE2900 and the SE2600 in features and functions are not covered in this topic. For detailed features and functions of the SE2900, see 4.1 Feature Matrix and .

Key Specifications

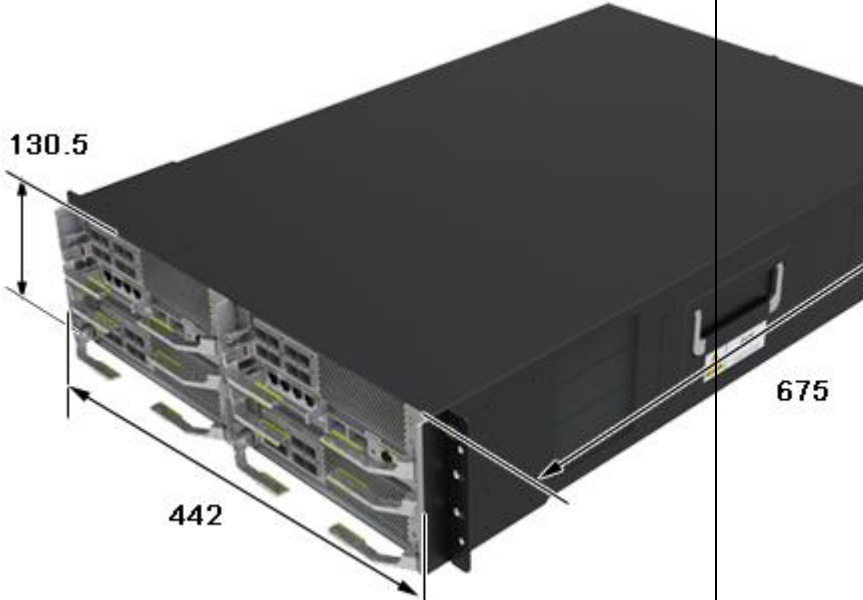
Table 10-1 lists only the maximum number of registered users and maximum number of concurrent calls. For specifications of other key counters, see 9.1 Performance Specifications.

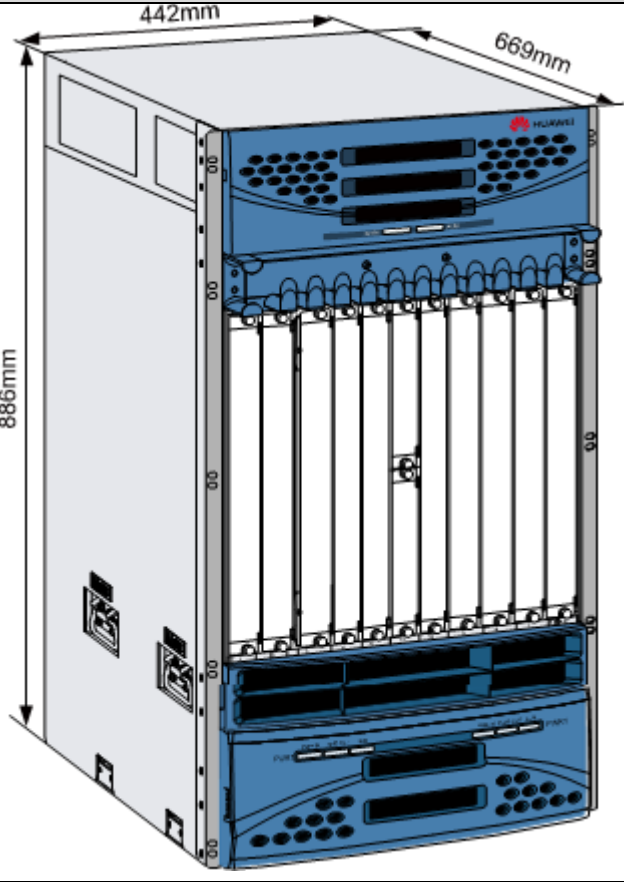
Table 10-1 Key specifications comparison

Item	Subitem	SE2900 V300R001C10		SE2600 V200R009C30
		One Subrack	Three-Subrack Cascading	
Platform and performance	Maximum number of SIP over UDP registered users	1,200,000	4,000,000	600,000
	Maximum number of SIP over UDP concurrent calls	100,000	340,000	60,000

Hardware

Table 10-2 Hardware comparison

Item	Subitem	Comparison
Product form	Subrack (Height x Width x Depth)	<ul style="list-style-type: none"> • SE2900: 130.5mm×442mm×675mm  <ul style="list-style-type: none"> • SE2600 V200R009C30: 886mm×442mm×669mm

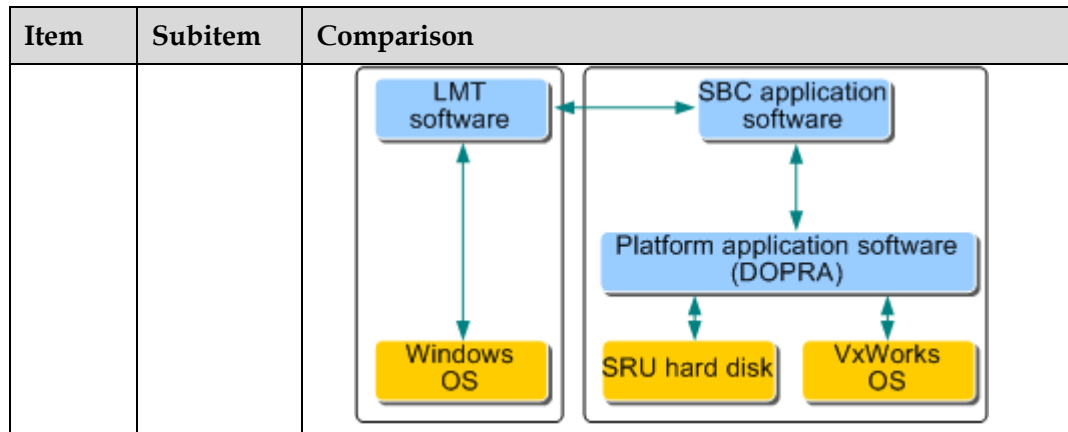
Item	Subitem	Comparison
		
	Number of SPUs (in one subrack)	<ul style="list-style-type: none"> • SE2900: 2 pairs • SE2600 V200R009C30: 3 pairs
	Cascading capability	<ul style="list-style-type: none"> • SE2900: Three-subrack cascading • SE2600 V200R009C30: Not supported
Hardware platform	Hardware platform	<ul style="list-style-type: none"> • SE2900: OSTA5.0 hardware platform <p>NOTE For detailed specifications, see Table 3-1.</p> <ul style="list-style-type: none"> • SE2600 V200R009C30: Packet gateway platform (PGP)
Subrack parameters	Weight of a fully configured subrack	<ul style="list-style-type: none"> • SE2900: 47.8kg • SE2600 V200R009C30: 147kg

Item	Subitem	Comparison
	Power consumption of the fully configured subrack	<ul style="list-style-type: none"> SE2900: 1310w SE2600 V200R009C30: 1700w

Software

Table 10-3 Software comparison

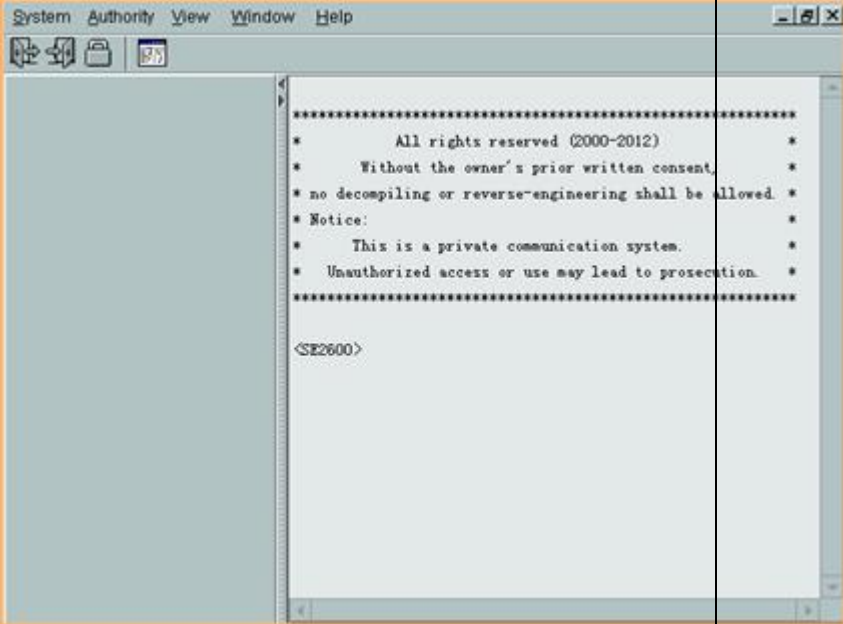
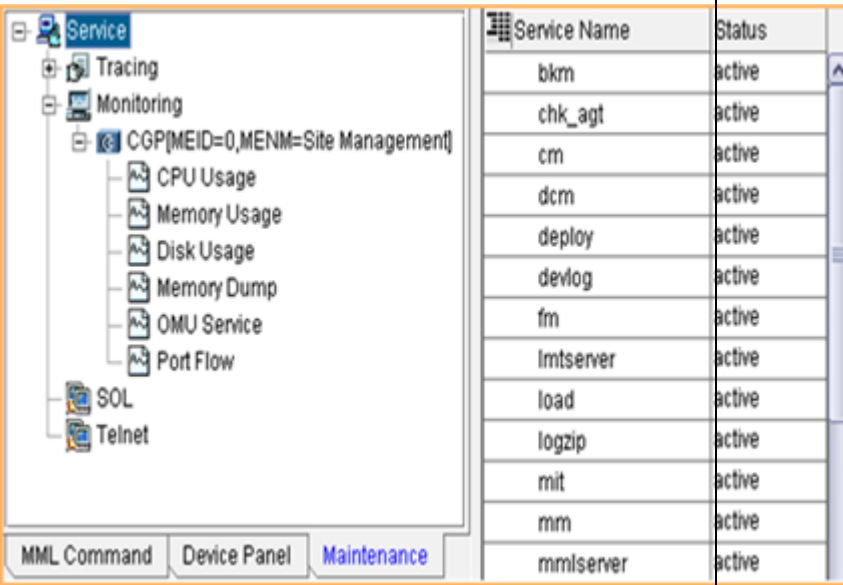
Item	Subitem	Comparison
Software platform	Software platform	<ul style="list-style-type: none"> SE2900: <p>The operating system (OS) of host software is Linux, a real-time OS. Middleware technology DOPRA_C is used between the OS and application software, which ensures that upper-layer service software is independent of the platform. For details, see Table 3-2.</p> <p>The OMU application software provides unified maintenance and operation to separate service application and operation management and enhance device maintainability.</p> SE2600 V200R009C30: <p>The OS of host software is VxWorks. Middleware technology DOPRA_C is used between the OS and application software, which ensures that upper-layer service software is independent of the platform.</p> <p>Application software implements operation and maintenance and service application.</p>

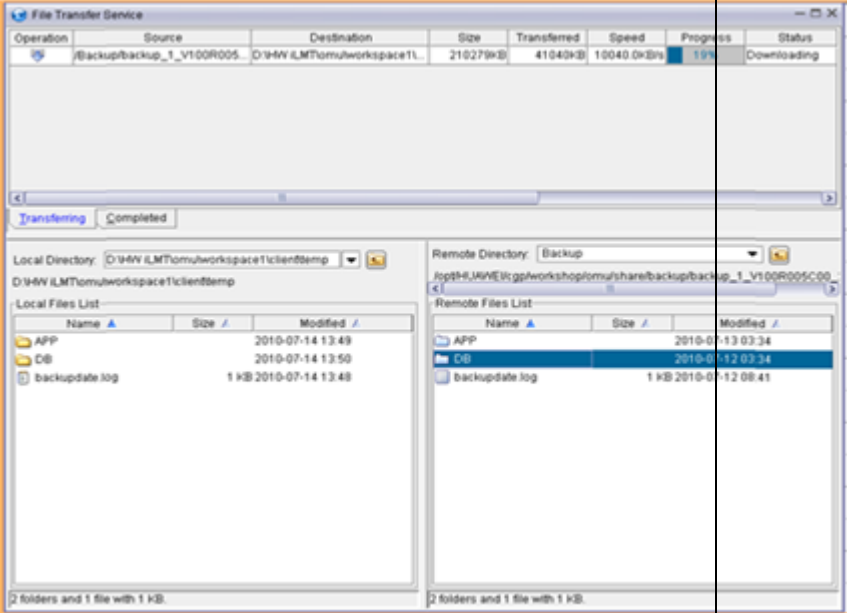


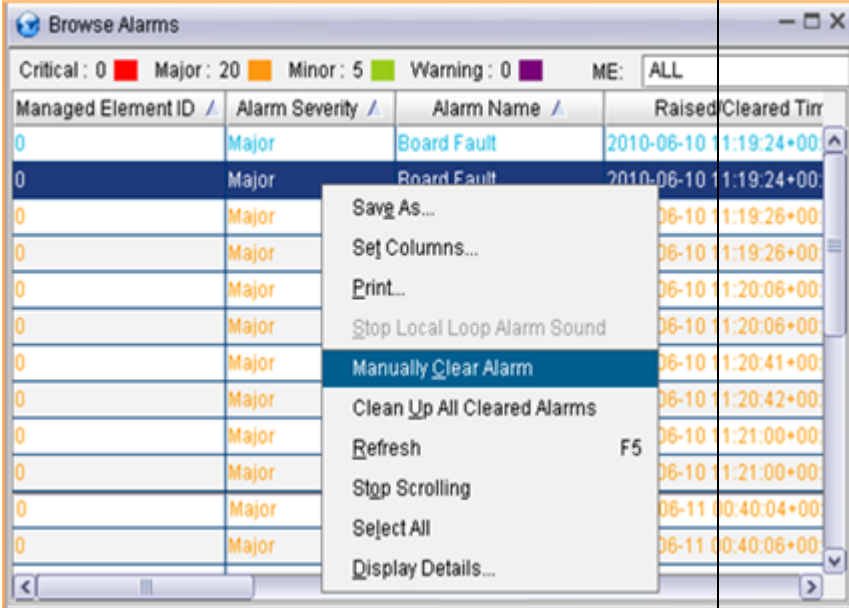
Configuration management

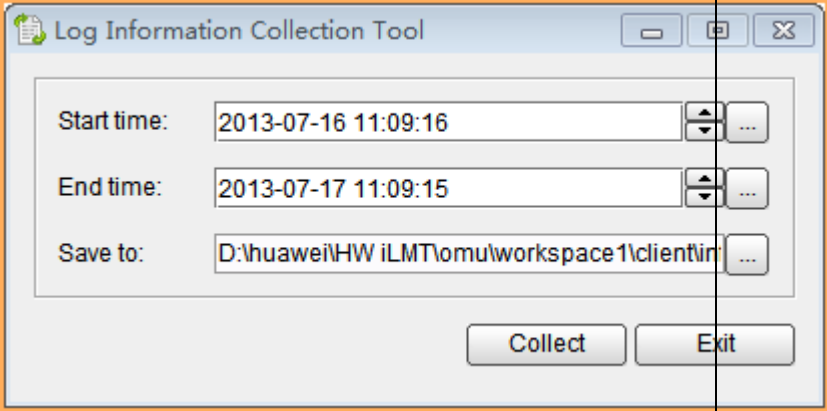
Table 10-4 Configuration management comparison


Item	Subitem	Comparison
GUI	Command	<ul style="list-style-type: none"> SE2900: Man-machine language (MML) command The SE2900 uses the OMU client that supports command searching, automatic command line completion, command navigation tree, batch command execution. <ul style="list-style-type: none"> SE2600 V200R009C30: Command-line interface (CLI) command

Item	Subitem	Comparison																												
																														
	<p>Operation and maintenance</p>	<ul style="list-style-type: none"> <p>SE2900:</p> <p>You can view the operating status of the SE2900 and perform operations on the simulated device panel.</p> <p>The SE2900 provides the display of message trace results and fault locating, and status monitoring of CPU usage, memory usage, and port traffic on the GUI.</p>  <table border="1" data-bbox="1204 1153 1572 1736"> <thead> <tr> <th>Service Name</th> <th>Status</th> </tr> </thead> <tbody> <tr><td>bkm</td><td>active</td></tr> <tr><td>chk_agt</td><td>active</td></tr> <tr><td>cm</td><td>active</td></tr> <tr><td>dcm</td><td>active</td></tr> <tr><td>deploy</td><td>active</td></tr> <tr><td>devlog</td><td>active</td></tr> <tr><td>fm</td><td>active</td></tr> <tr><td>lmtserver</td><td>active</td></tr> <tr><td>load</td><td>active</td></tr> <tr><td>logzip</td><td>active</td></tr> <tr><td>mit</td><td>active</td></tr> <tr><td>mm</td><td>active</td></tr> <tr><td>mmserver</td><td>active</td></tr> </tbody> </table> <p>SE2600 V200R009C30:</p> <p>The SE2600 provides CLI command-based management.</p> <pre data-bbox="686 1825 1428 1993"> <SE2600> display cpu-usage CPU Usage Stat. Cycle: 60 (Second) CPU Usage : 21% Max: 79% CPU Usage Stat. Time : 2012-09-04 10:52:21 </pre> 	Service Name	Status	bkm	active	chk_agt	active	cm	active	dcm	active	deploy	active	devlog	active	fm	active	lmtserver	active	load	active	logzip	active	mit	active	mm	active	mmserver	active
Service Name	Status																													
bkm	active																													
chk_agt	active																													
cm	active																													
dcm	active																													
deploy	active																													
devlog	active																													
fm	active																													
lmtserver	active																													
load	active																													
logzip	active																													
mit	active																													
mm	active																													
mmserver	active																													

Item	Subitem	Comparison
	File management	<ul style="list-style-type: none"> SE2900: The SE2900 provides GUI-based remote file management, for example, file upload and download.  <ul style="list-style-type: none"> SE2600 V200R009C30: The SE2600 provides FTP-based file management. The following is example file transfer between a PC and the SE2600: <pre>put local-filename remote-filename</pre> <pre>[ftp] put /soft/b/bam/cfg/vrpcf.cfg c:\download\backup.cfg</pre> <pre>200 Port command okay.</pre> <pre>150 "c:\download\backup.cfg" file ready to receive in ASCII mode.</pre> <pre>226 Transfer complete.</pre> <p>The file is transferred to a specified path and named backup.cfg.</p>
	Alarm management	<ul style="list-style-type: none"> SE2900: The SE2900 uses the alarm box to report and prompt alarms in real time. Operators can use the OMU client to view, print, and clear alarms.

Item	Subitem	Comparison
		 <ul style="list-style-type: none"> SE2600 V200R009C30: The SE2600 provides CLI command-based alarm management. <pre data-bbox="683 1025 1433 1438"> <SE2600> system-view [SE2600] om-view [SE2600-om-view] display alarm active counts 1 ALARM 76239 Fault Critical SBC 3509 Running Sync serial No. = 152333 Alarm name = License expired Alarm raised time = 2011-12-19 02:00:36 Location info = Feature=all features Cleared state = Not cleared (Number of results = 1) </pre>
	Log management	<ul style="list-style-type: none"> SE2900: The SE2900 provides log collection tools to collect log information by period. Operators can use the OMU client to view or print logs.

Item	Subitem	Comparison
		 <ul style="list-style-type: none"> SE2600 V200R009C30: The SE2600 provides CLI command-based log management. <pre data-bbox="683 795 1433 1303"> <SE2600> system-view [SE2600] om-view [SE2600-om-view] display operlog Query operation log ----- No. = 1 Date = 2008-02-15 Time = 17:16:56 User ID = 0 User name = admin Terminal IP address = 10.110.56.22 Operation Result = Execution succeeded Return code = 0 Command = language-mode chinese (Number of results = 1) </pre>
Maintenance tools	Maintenance tools	<ul style="list-style-type: none"> SE2900: The SE2900 provides the performance and management system, patch and upgrade tool, and maintenance tool through the WebUI, which simplify maintenance or configuration modification on the live network.

Item	Subitem	Comparison
		 <p>• SE2600 V200R009C30: Not supported</p>

11 Acronyms and Abbreviations

Digits	
3GPP	The 3rd Generation Partnership Project
A	
AAC-LD	Advanced Audio Coding with Low Delay
ACL	Access Control List
ACR	Apply Charging Report
AG	Access Gateway
AH	Authentication Header
AN	Access Network
AMR-NB	Adaptive MultiRate NarrowBand
AMR-WB	Adaptive MultiRate WideBand
ANSI	American National Standards Institute
API	Application Platform Interface
AS	Application Server
A-SBC	Access side Session Border Controller
ATS	Avanced Tlephony Srver
AUTN	Authentication TokeN
B	
B2BUA	Back-to-Back User Agent
BFD	Bidirectional Forwarding Detection
BGF	Border Gateway Function
BMC	Baseboard Management Controller
C	

CAC	Connection Admission Control
CAR	Committed Access Rate
CCF	Charging Collection Function
CDB	Central Database
CDR	Call Detail Record
CRC	Cyclic Redundancy Check
CSCF	Call Session Control Function
D	
DBMS	Database Management System
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DOPRA	Distributed Object-oriented Programmable Realtime Architecture
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DNS	Domain Name System
DSP	Digital Signal Processing
DTMF	Dual Tone Multiple Frequency
E	
EC	Echo Cancellation
E-CSCF	Emergency-Call Session Control Function
ECM	Entitlement Control Message
EFT	Electrical Fast Transient
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electromagnetic Shielding
ESD	Electrostatic Discharge
ESP	Encapsulating Security Payload
ETS	European Telecommunication Standards
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVRC	Enhanced Variable Rate Codec

G	
GE	Gigabit Ethernet
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support node
GPRS	General Packet radio System
GUI	Graphical User Interface
H	
HDMI	High Definition Multimedia Interface
HF	High Frequency
HTTP	Hypertext Transfer Protocol
HSS	Home Subscriber Server
I	
I-CSCF	Interrogating-Call Session Control Function
IBCF	Border Control Function
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
iLBC	Low Bitrate Codec
IK	Integrity Key
IKE	Internet Key Exchange
IM	Instant Message
IMS	IP multimedia Subsystem
IMU	I/O Board Management Unit
I-SBC	Interconnection Session Border Controller
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
IUA	ISDN Q.921-User Adaptation layer
L	
LACP	Link Aggregation Control Protocol
LAN	Local Area Network

LC	Line Card
LMT	Local Maintenance Terminal
LTE	Long Term Evolution
M	
M2UA	MTP2-User Adaptation layer
M3UA	MTP3-User Adaptation layer
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MIME	Multipurpose Internet Mail Extensions
MME	Mobility Management Entity
MML	Man-Machine Language
MON	Process Monitor Service
MOS	Mean Opinion Score
MPO	Maximum Power Output
MSRP	Message Session Relay Protocol
MTBF	Mean time Between Failures
MTTR	Mean Time to Repair
MXUA0	Multi-Function and Switch Unit
N	
NAT	Network Address Translation
NEBS	Network Equipment Building System
NFS	Network File Server
NGN	next generation network
NTP	Network Time Protocol
O	
OAM	Operation, Administration and Maintenance
OM	Object Dimension
OMU	Operation and Maintenance Unit
OPEX	Operating Expense
OSPF	Open Shortest Path First
OSTA	Open Standards Telecom Architecture
P	

PABX	Private Automatic Branch eXchange
PBX	Private Branch eXchange
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy-call Session Control Function
PCU	Packet Control Unit
PDN	Packet Data Network
PEM	Power Entry Module
PS	Packet Switched
Q	
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
R	
RAN	Radio Access Network
RAND	RANDom challenge
RCS	Rich Communication Suite
RDIMM	Registered Dual In-line Memory Module
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
S	
S-CSCF	Serving-Call Session Control Function
SAS	Serial Attached SCSI
SBC	Session Border Controller
SCU	Session Control Unit
SDP	Session Description Protocol
SFP	Small Form-factor Pluggable
SFP+	Enhanced Small Form-factor Pluggable
SIP	Session Initiation Protocol
SMU	Service Management Unit
SNMP	Simple Network Management Protocol
SPU	Service Processing Unit

SRMU	System Reliability Management Unit
SRTP	Secure Real-time Transport Protocol
SRVCC	Single Radio Voice Call Continuity
SSD	Shared Secret Data
SSH	Secure Shell
STUN	Session Traversal Utilities for NAT
SYN	Synchronize Sequence Number
T	
TCP	Transmission Control Protocol
TLS	Transport Layer Security
U	
UAC	User Agent Client
UAS	User Agent Server
UDIMM	Unbuffered Dual in-line Memory Module
UE	User Equipment
UDP	User Datagram Protocol
V	
VoBB	Voice over Broad Band
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution
VOS	Virtual Operating System
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
W	
WebUI	Web User Interface