GGSN9811 Product Description

HUAWEI GGSN9811 Gateway GPRS Support Node
Product Description

Document Version 01 (2006-06-30)

Product Version V800R005

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,
Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Trademarks

and other Huawei trademarks are the trademarks or registered trademarks of Huawei Technologies Co., Ltd. in the People's Republic of China and certain other countries.

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

Notice

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

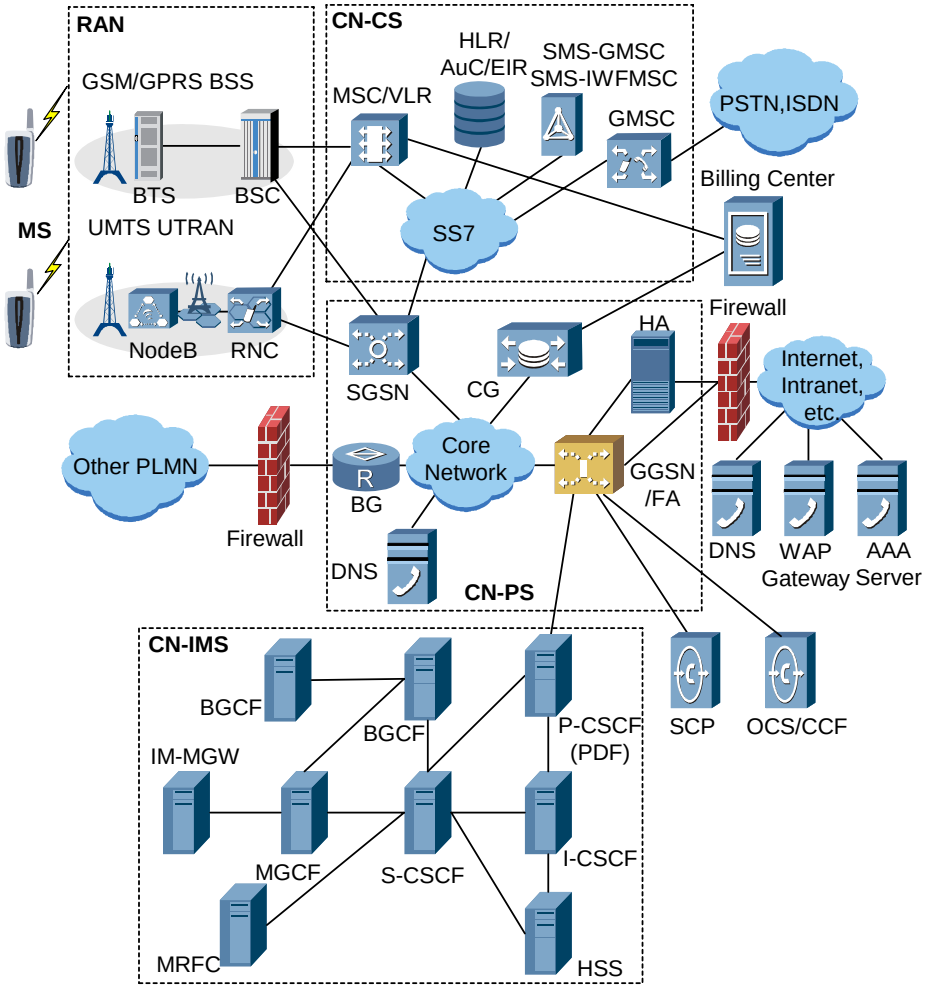
Table of Contents

Chapter 1 Introduction to the GGSN9811

1.1 GPRS/UMTS Network Architecture

The wireless technology sees the evolution from the 2G Global System for Mobile Communications (GSM) to the 2.5G General Packet Radio Service（GPRS), and then to the 3G Universal Mobile Telecommunications System (UMTS).

Mobile communications now cover wide areas, realize high-speed wireless data transmission, and access the Internet. It provides you with abundant multimedia services, such as voice, data and video, as well as the freedom and fun to communicate wherever and whenever.



MS: Mobile Station
CN-CS: Core Network-Circuit Switching
BSS: GSM Base Station Subsystem

BTS: Base Transceiver Station
NodeB: UMTS Base Station
SGSN: Serving GPRS Support Node

CG: Charging Gateway
BG: Border Gateway
AAA: Authentication, Authorization, Accounting Server
S-CSCF: Serving Call Session Control Function

BGCF: Breakout Gateway Control Function
MRFC: Multimedia Resource Function Controller

CN-IMS: Core Network-IP Multimedia Subsystem
OCS/CCF: Online Charging System/Credit Control Function

RAN: Radio Access Network
CN-PS: Core Network-Packet Switching
UTRAN: Universal Terrestrial Radio Access Network
BSC: Base Station Controller
RNC: Radio Network Controller
GGSN/FA: Gateway GPRS Support Node/Foreign Agent
HA: Home Agent
DNS: Domain Name System
I-CSCF: Interrogating Call Session Control Function
P-CSCF: Proxy Call Session Control Function

MGCF: Media Gateway Control Function
IMS-MGW: IMS Media Gateway Function
PDF: Policy Decision Function

SCP: Service Control Point

Figure 1-1 GPRS/UMTS network architecture

As shown in Figure 1-1, the GPRS/UMTS mainly consists of the following parts:

- Mobile Station (MS)
  An MS is a user's mobile equipment, being able to launch and receive calls through an air interface. To provide data service, the MS establishes a logic link with the PS domain.
- Radio Access Network (RAN)
  The RAN provides all the functions related to wireless access.
- Core Network-Circuit Switching (CN-CS)
  The CS domain provides circuit data services, connecting Public Switched Telephone Network (PSTN) or other external CS networks.
- Core Network-Packet Switching (CN-PS)
  The PS domain provides packet data services, connecting the Internet or other external Packet Data Networks (PDNs).
- Core Network-IP Multimedia Subsystem (CN-IMS)
  According to the 3GPP R5, the UMTS core network is divided into CS domain, PS domain and IMS domain.
  The IMS domain consists of the network elements that can realize such IP multimedia services as audio service, video service, text, chat and their combo. The PS domain bears the IMS domain for creating session and transmitting data in IP multimedia services.
  The Go interface is used for creating the association between the IMS session (SIP/SDP) and the PS bearer domain (PDP context).

Note:

During the evolution from the GPRS to the UMTS, the CN is changing smoothly, while the RAN has seen a total change as the air interfaces are so different.

1.2 Huawei GPRS/UMTS Packet Data Service Solutions

The GPRS/UMTS CN-PS of Huawei Technologies Co., Ltd (hereafter referred to as Huawei) consists of the following network entities: the SGSN, GGSN/FA, HA, CG and AAA Server. It makes an MS access the external PDN and provide packet data services and billing services (including prepaid service and postpaid service).

The functions of the main network entities of the Huawei GPRS/UMTS CN-PS are as follows:

I. SGSN

The Serving GPRS Support Node (SGSN) is a functional entity for providing packet data services. It forwards incoming and outgoing IP packets to MSs within the service area.

The SGSN provides the following functions:

- IP packet routing and forwarding for all mobile users within the service area of the SGSN
- Encryption and authentication
- Session management
- Mobility management
- Logical link management
- Call detail record (CDR) generation and output, reflecting the occupation of wireless resources

II. GGSN

The GGSN (Gateway GPRS Support Node) is a functional entity for providing packet data services. It is in charge of the routing and encapsulation of the packet data between the GPRS/UMTS network and the external PDN. The GGSN provides the following functions:

- Providing the interface to the external PDN.
  The GGSN functions as a gateway for an MS accessing an external PDN. For the external PDN, the GGSN exchanges routing information with each other, which actually serves as a router of all device IP addresses in the addressed GPRS/UMTS network.
- GPRS/UMTS session management.
  The GGSN undertakes communications between the MS and the external PDN.
- Receiving data from the MS and then routing to the external PDN, or receiving data from the external PDN and then sending to the SGSN according to the destination address by selecting a transport channel through the GRPR/UMTS network.
- Providing mobile IP service.
  To do this, the FA functionality is integrated into the GGSN. Now the GGSN/FA serves as both a gateway device and an FA of the network that the MS accesses.
- Postpaid service.
  The GGSN generates and outputs call bills, reflecting how users make use of the external network.
- Prepaid service.
  For general prepaid service, the GGSN serves as the service switching point (SSP). The GGSN serves as a connection point between a radio

communications network and an intelligent network, providing call control function and service switching function.
For content-based prepaid service, the 3GPP R6 explicitly defines the Traffic Plane Function (TPF) as the logical function of the GGSN. In content-based billing, the TPF is the core module for service differentiation and information statistics.

III. HA

The home agent (HA) is an entity that supports mobile IP. In fact, it is an enhanced router, being added with the function of maintaining the current location information.

The main functions of the HA are as follows:

- Sending HA advertisement messages, helping an MS know whether it is on the home network
- Handling the registration requests from an MS and replying to them. Establishing mobility binding records (MBRs) between the MS home address and care-of address
- Agency and forwarding. The HA announces the reachability of the network prefix of the MS home address so that the packets destined to the MS home address route to the home network. After encapsulating the packets destined to the MS, the HA tunnels them to the GGSN/FA. Finally, the packets are forwarded to the MS by the GGSN/FA.

IV. CG

The charging gateway (CG) is a device in the GPRS/UMTS network. It is in charge of collecting, merging, and pre-processing of the CDRs generated by the SGSN/GGSN, providing the interface to the billing center. The CDR will be generated from several network entities once the GPRS/UMTS user accesses the Internet. Each entity may generate several CDRs. The purpose for using CG is to reduce the workload of the billing center by merging and pre-processing the CDRs, and to provide an interface to the billing center. Therefore, the SGSN and the GGSN do not need to provide such interfaces.

V. AAA Server

The Authentication, Authorization and Accounting Server (AAA Server) is mainly used for authentication, authorization and accounting following the Remote Authentication Dial In User Service (RADIUS) protocol. It is not a special entity for the GPRS/UMTS system.

VI. DNS

There are two types of domain name systems (DNSs) in the GPRS/UMTS network.

One is the DNS between the GGSN and the external PDN. The main function is to resolve the domain name of the external PDN, just like the ordinary DNS on the Internet.

The other one is the DNS on the GPRS/UMTS CN. The main functions are:

- When the MS applies for accessing the external PDN, the DNS resolves the GGSN IP address from the Access Point Name (APN), so as to establish a communication channel from the MS to the GGSN.
- During the updating of the routing area between SGSNs, the DNS resolves the SGSN IP address from the old routing area code.

It is not specific to the GPRS/UMTS system.

VII. BG

The Border Gateway (BG) is, in fact, a router. It provides, apart from the security function, the routing function between SGSNs and GGSNs in different GPRS/UMTS networks. It is not a special entity for the GPRS/UMTS system.

Note:

The FA and HA are compulsory for the access of mobile IP. If mobile IP is not provided for the GPRS/UMTS packet service solution, the FA and HA are not needed.

1.3 Roles of the GGSN9811 in GPRS/UMTS

The GGSN9811 is a gateway GPRS support node that is independently developed by Huawei. As a gateway device for an MS to access the external PDN, the GGSN9811 is located at the joint between the packet CN of the GPRS/UMTS and the external PDN.

The hardware platform of the GGSN9811 is the Universal Switching Router (USR) of Huawei. The USR is a compact, carrier-class network switching device based on proven industry standards. The software of the GGSN9811 is developed on the Versatile Routing Platform (VRP) of Huawei. The GGSN9811 inherits the basic technologies of data communications, such as integrated routing technology, IP Quality of Service (QoS), Virtual Private Network (VPN) and security technology, greatly expands and improves the functions based on the wireless communication applications.

Based on both the hardware platform that is rendered by the USR, featuring high reliability and high data handling capability, and the software platform that integrates seamlessly wireless communications technologies and data communications

technologies, the GGSN9811 provides ideal and flexible solutions to wireless data communications for GPRS/UMTS network operators.

Chapter 2 Key Benefits

The GGSN9811 features high data handling capability, high reliability, rich and diversified services, easy operation and maintenance and smooth upgrade.

2.1 Large Capacity and High Performance

The hardware platform of the GGSN9811 is a Universal Switching Router (USR), which is the core router of the fifth generation. It is in a structure of separated signaling/control plane from the data plane. The signal/control plane consists of many universal processors of high performance; and the data plane consists of many network processors (NP) of high performance and high forwarding capability.

- Being fully configured, the GGSN9811 can activate 1,050,000 Packet Data Protocol (PDP) contexts at the same time, handling as much as 3 Gbit/s of data.
- When the GGSN9811 is expanded with new functions or carries out active/standby redundancy backup, it will not lead to dropdown in the overall capacity or in the performance.

2.2 Reliability of Carrier-Class

During the product design of the GGSN9811, the reliability design has been taken into full consideration in the three aspects of hardware, software and networking so that normal operation of the product is effectively guaranteed.

2.2.1 Hardware Reliability

The system adopts advanced network processor technology and supports the functions of online plugging and active/standby redundancy backup of key boards. It is powered by double-channel power supply system, which is protected by over-voltage/over-current measure.

2.2.2 Software Reliability

The system provides such functions as overload control, traffic control, resource check, and self fault detection. These functions ensure the system to operate stably. The special billing record buffer function guarantees a reliable billing system. The hot patch technology makes the upgrade of software not to impact normal operation of the equipment.

2.2.3 Networking Reliability

The router backup and router load sharing function can eliminate the single-point fault on the network so that a network of high reliability is guaranteed. The Eth-Trunk function can eliminate the bad effect that results from faults of a single port.

For details, refer to Chapter 6 "Reliability" of this manual.

2.3 Rich and Diversified Services and Functions

The GGSN9811 provides rich services and functions, able to satisfy users' diversifying networking and service demands. The system supports the following services and functions:

- IP over GTP and PPP over GTP
- Transparent access and nontransparent access to the PDN by MSs
- Mobile IP
- CAMEL prepaid service
- Prepaid service through the Gy interface
- Postpaid service
- Content-based billing
- Popular routing protocols, including static routing protocol, RIP, OSPF, IS-IS and BGP
- QoS based on Differentiated Services (Diff-Serv), including QoS marking, traffic classification, traffic policing, traffic shaping, queue scheduling, and congestion control
- VPN services, including GRE VPN, L2TP VPN and MPLS VPN
- Security solutions, including IPSEC, redirect technology, filtration technology and so on
- Access to the IP Multimedia Subsystem (IMS)

For details, refer to Chapter 4 "Services and Functions" of this manual.

2.4 Easy Operation and Maintenance

The GGSN9811 provides graphic operation and maintenance tools, making the operation and maintenance visualized, simple and easy.

- Providing several operation and maintenance networking approaches

The GGSN9811 provides such network management approaches as the Local Maintenance Terminal (LMT), the iManager 2000 and the integrated network management system based on the SNMP interface. Supported by the iManager 2000 CORBA interface, more management networking needs can be realized.

- Operation and maintenance approaches with the integration of MML and GUI

Network managers can still be benefited not only from the advantages of quick operation and easy access to network management of the Man Machine Language (MML), but also from that of visualization and less memory burden resulting from the graphical user interface (GUI).

- Strong functions of signaling tracing and message explanation

The GGSN9811 can trace all kinds of standard interfaces (such as Gn/Gp, Gi, Ga, Go, and Gy) and specified users. At the same time, it can explain and filter the traced messages.

- Rich online documentation

Help and guidance can be available at any time so that users feel convenient to operate and maintain the equipment.

For details, refer to Chapter 5 “Operation and Maintenance” of this manual.

2.5 Smooth Upgrade

The features of smooth system expansion, open standards and interfaces and future network-oriented design philosophy enable the GGSN9811 with lasting life and ability of smooth upgrade. In this way, user’s investment can be protected in a large extent.

- Smooth system expansion. You can deploy a proper capacity in early time and expand it with the increase of user quantity or service development. At that time, it is unnecessary for you to change the original hardware or the interface connection of the GGSN9811. The system expansion can be easily done by configuration of software parameters.
- The GGSN9811 is compliant to 3GPP and RFC protocols, providing open interfaces. This is convenient for the GGSN9811 to interwork with equipment made by other manufacturers. Moreover, it can connect directly with various service/content servers, carrying more diversified data services.
- In the design of the GGSN9811, the trend of future networks has been fully considered. New features will be added to the subsequent versions of the GGSN9811 to meet the trend of network development.

Chapter 3 System Architecture

3.1 Hardware Description of the GGSN9811

3.1.1 Hardware Configuration

The GGSN9811 system consists of the following components:

- GGSN subrack, LAN Switch, and Firewall Eudemon200
  They are mounted in Huawei N68-22 cabinet.
- No. 7 signaling access unit, including GSAU subrack, air deflector, GSAU BAM, KVM, LAN Switch and so on
  The No. 7 signaling access unit is mounted in another N68-22 cabinet and used to support CAMEL prepaid service.

Figure 3-1 shows the appearance of an N68-22 cabinet. Figure 3-2 shows a typical cabinet configuration.

Figure 3-1 An N68-22 cabinet

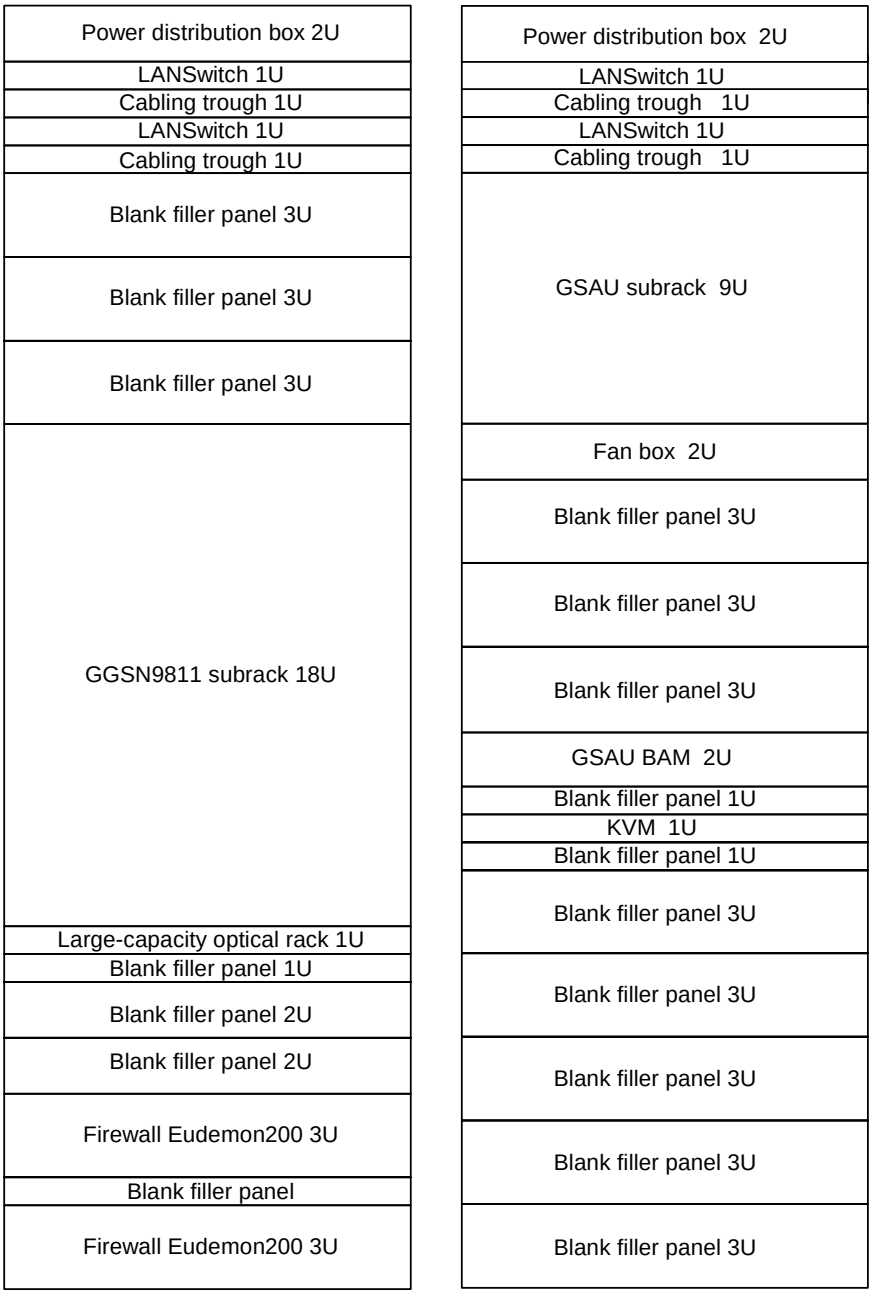


Figure 3-2 Schematic diagram of GGSN9811 cabinet configuration (right part is the GGSN No. 7 signaling access unit)

Of these components:

- GGSN subrack is mandatory. Main service boards (SRU, SPU, and LPU) of the GGSN9811 can be inserted in the GGSN subrack.

- LAN Switch is optional. In actual networking, the management channel of the device can be implemented by the LAN Switch (to improve reliability, you can select two LAN Switches as active/standby channels). When the GGSN9811 networks with other Huawei wireless devices (for example, an SGSN), it can share LAN Switch with other wireless devices without further separate configuration.
- Firewall Eudemon200 is optional. If you have special requirements, you can purchase it by separately.
- GGSN No.7 signaling access unit is optional. To support CAMEL prepaid service, you must configure the unit.

3.1.2 Boards of the GGSN9811

Typical board arrangement of the GGSN9811 is shown in Figure 3-3.

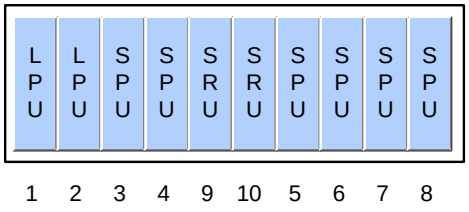


Figure 3-3 Boards of the GGSN9811

I. SRU

SRU is the core of the system management. SRU is active/standby redundancy backup. The system needs only two SRUs, of which one is active and one is standby. They are fixedly inserted in slots 9 and 10 of the GGSN subrack.

The main functions of SRU are as follows:

- SRU executes route protocol, collects route information, and produces routing table according to the network topology and user-define-scheme. Then it delivers the routing table to the LPUs and SPUs.
- SRU is the agent of O&M. It manages the system according to the operator's commands and collects the system running parameters for the operator.
- SRU is the datagram switching center. It receives datagram from LPUs and processes the datagram according to the control information taken by the datagram, and then it delivers the datagram to the SPUs.

II. SPU

SPU provides all service processing functions of the GGSN9811, including the GTP-U and GTP-C functions. A GGSN9811 can be configured with up to three pairs of SPUs, with each pair being in active/standby backup design, located at slots 3 and 4, slots 5 and 6, and slots 7 and 8. The capacity of the GGSN is up to the processing capability of SPUs. The processing capability of one pair of SPU is 350,000 PDP contexts. The maximum processing capability of the GGSN9811 is 1,050,000 PDP contexts.

The GTP-U processing functions include:

- Encapsulating data packets from an external PDN into GTP data packets according to activated PDP contexts and sending them to the corresponding SGSN through the LPU.
- Decapsulating the GTP data packets sent from the SGSN according to activated PDP contexts and then routing and forwarding them by the LPU.

The GTP-C processing functions include:

- Processing the GTP-U signaling such as a path-check signaling
- Processing the GTP-C signaling
- Processing the billing information

Optionally, an SPU can also be added with a Compression Service Processing Card (CSPC) so as to enable such complicated functions as content-based billing, IPv6 user plane, lawful interception, and IPSec encryption/decryption.

III. LPU

LPU provides physical interfaces to the external network (such as the SGSN, PDN, AAA Server, and CG), including the following types of interface:

- Fast Ethernet (FE, 10/100 Mbit/s) interface
- Gigabit Ethernet (GE, 1,000 Mbit/s) interface

The GGSN9811 is designed with two LPUs, which are in slots 1 and 2 and are used to cooperate with remote networking devices. LPU is in charge of only packet forwarding, not any service processing. All service processing functions are performed by SPUs. The routing table information of LPUs is issued by SRUs.

3.2 Software Description of the GGSN9811

Architecture of the GGSN9811 software is shown in Figure 3-4.

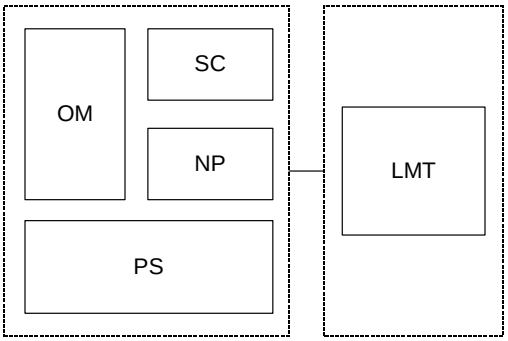


Figure 3-4 Architecture of the GGSN9811 software

- Operation and maintenance (OM): Its main function is operation and maintenance management, such as equipment management, data configuration management, alarm management, and command line resolution.
- Network service process (NP): This module undertakes the functions of GTP-U, including forwarding packets from an MS to the PDN or from the PDN to an MS.
- Service control (SC): This module undertakes the functions of GTP-C, including processing GTP signaling, GTP-U signaling, billing signaling and so on. The signaling packets that have been processed by the SC will be delivered to NP for forwarding.
- Software platform service (PS): This module provides the platform service of the whole GGSN9811 software system, including IP address assignment, communication with AAA, security, QoS, VPN and so on.
- LMT: This module provides users with graphic user interface (GUI).

3.3 Protocol Interface

As shown in Figure 3-5, the GGSN9811 implements interfaces as follows:

- Gn/Gp: interface between the SGSN and the GGSN (or GSN for short)
- Gi: interface between the GGSN and the PDN
- Ga: interface between the GGSN and the CG
- Ge: interface between the GGSN and the SCP
- Gy: interface between the GGSN and the OCS/CCF
- Go: interface between the GGSN and the PDF

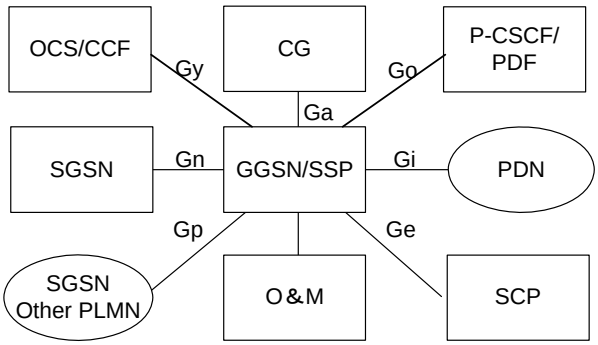


Figure 3-5 GGSN protocol interfaces

3.3.2 Interface Gn/Gp

Gn is the interface between the SGSN and the GGSN, if both the SGSN and the GGSN belong to one PLMN. Gp is the interface between the SGSN and the GGSN, if the SGSN and the GGSN belong to different PLMNs. Gn and Gp have the same protocol stack, as shown in Figure 3-6.

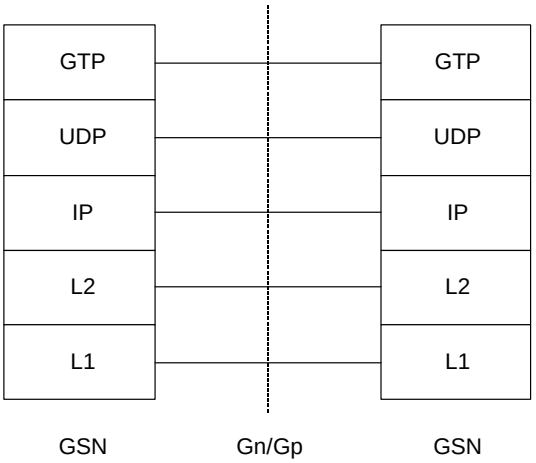


Figure 3-6 Gn/Gp protocol stack

The GPRS Tunneling Protocol (GTP) includes GTP control plane (GTP-C) and GTP user plane (GTP-U).

- On the control plane, the signaling is used to create, modify and delete tunnels.
- On the user plane, the tunneling mechanism is used to transport users' packets.

There are two versions of GTP, GTP version 0 and GTP version 1 (In addition, there is a GTP' which is used for billing). The former belongs to 3GPP Release 98, which is used in GPRS network; the latter belongs to 3GPP Release 99, which is used in 3G network. GTP Version 0 is compatible with GTP Version 1. They are differentiated by

value in the version field of the GTP packet header. The GGSN9811 supports GTP version switching at Gn and Gp.

3.3.3 Gi Interface

Gi is the interface between GGSN and PDN. Gi's protocol stack is shown in Figure 3-7 and Figure 3-8 (transparent access and nontransparent access).

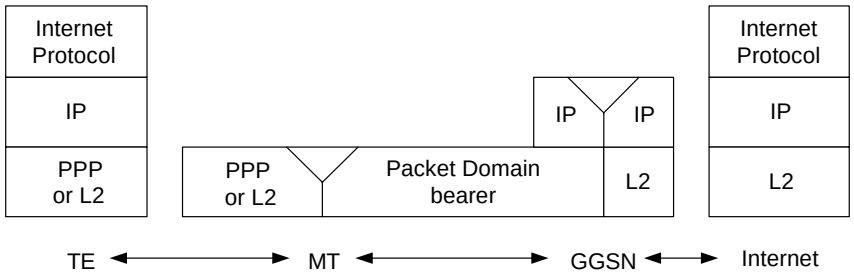


Figure 3-7 Gi interface protocol stack (transparent access)

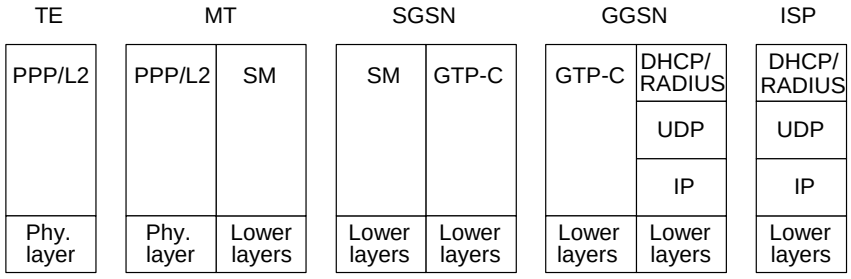


Figure 3-8 Gi interface protocol stack (nontransparent access)

3.3.4 Ga Interface

Ga is an interface between the GSN (including SGSN and GGSN) and the Charging Gateway Functionality (CGF), running GTP'. GTP' is a protocol that is used to send CDRs generated by a network unit or functional entity to the CGF.

The Ga protocol stack is shown in Figure 3-9.

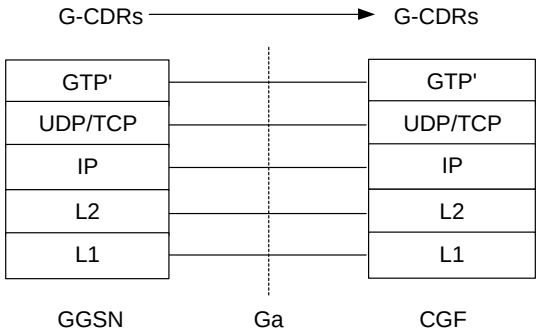


Figure 3-9 Ga interface protocol stack

3.3.5 Ge Interface

Ge is the interface between the GGSN SS7 Signaling Access Unit and the SCP. It communicates over the CAP (CAMEL Application Part) signaling protocol. Currently it is mainly used for general prepaid service.

The Ge interface protocol stack is shown in Figure 3-10.

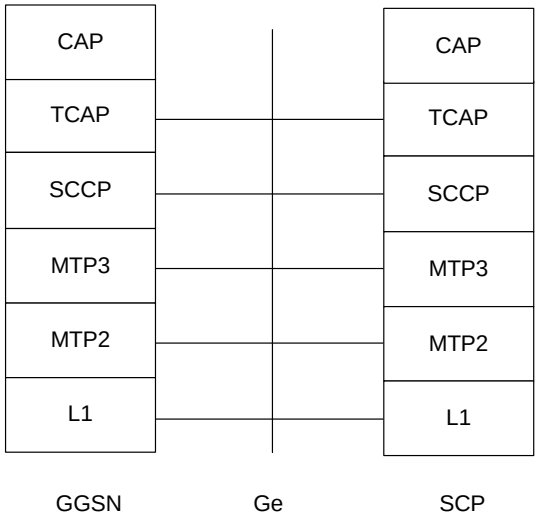


Figure 3-10 Ge signaling interface protocol stack

3.3.6 Gy Interface

Gy is the interface between the GGSN and the Online Charging System/Credit Control Function (OCS/CCF). It communicates based on the Diameter Base Protocol and is used for prepaid service control.

The Gy interface and the OCS interact to realize content-based prepaid service and general prepaid service.

Figure 3-11 shows the protocol stack of the Gy interface.

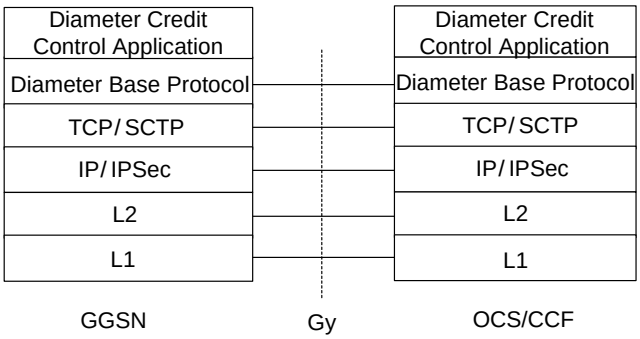


Figure 3-11 Protocol stack of the Gy interface

3.3.7 Go Interface

Go interface is used for creating relationship between the IMS session (SIP/SDP) and the PS bearer domain (PDP context). Go is the interface between the GGSN and PDF. It is used for session policy control. That is to say, for multimedia services, the QoS policy for specified PDP contexts is delivered by the PDF and the GGSN only implements access control and forwards data based on the policy made by the PDF. Therefore, the Go interface is in fact a signaling port. It communicates in accordance with the Common Open Policy Service Protocol（COPS).

Figure 3-12 shows the protocol stack of the Go interface.

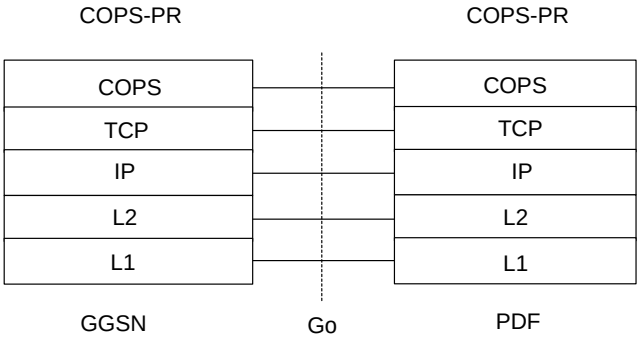


Figure 3-12 Protocol stack of the Go interface

Chapter 4 Services and Functions

The GGSN9811 is one of the indispensable network entities in the UMTS or the GPRS backbone network. Its main function is to forward packets between a mobile network (UMTS or GPRS) and a packet network. The 3GPP does not define application services for the GGSN; therefore, services on the application layer need to be provided by the ISP. The GGSN provides only carrying function for the application layer.

4.1 Routing

From the viewpoint of the PDN, as a gateway device between the GPRS/UMTS and the PDN, the GGSN is equivalent to a router that can address all users' IP on the GPRS/UMTS.

The GGSN9811 supports the key routing protocols, including:

- Static routing
- RIP
- OSPFv2
- IS-IS
- BGP-4
- Routing policies
- Active/Standby routing

4.2 Access to the PDN

The main function of the GGSN is to connect a Mobile Station (MS) to the external PDN, providing users with Internet/Intranet access services. An MS is connected to the PDN through Access Points (APs).

There are two ways for an MS to access the PDN, namely, transparent access and nontransparent access.

I. Transparent Access

The transparent access mode means that the operator serves as the data network service provider and directly provides services to subscribers, such as E-mail, Web browsing and so on.

Figure 4-1 shows an example of the transparent access mode.

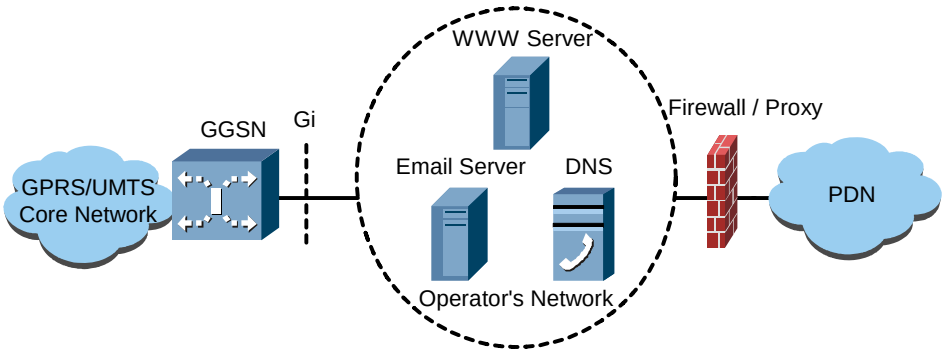


Figure 4-1 Example of transparent access to IP network

Equipment such as WWW server, E-mail server, DNS server is provided in the IP network of the operator. At the joint with the external network, a firewall is set up to shield unauthorized access.

In this mode, the IP address assigned to the mobile subscriber belongs to the address space of the operator. It can be one of the following:

- IP address given when the services are subscribed, for example, the static address saved in the subscription data of the subscriber
  When the PDP context is activated, this IP address is carried by the request message. The GGSN saves this IP address to the PDP context to provide routing information for data transmission.
- IP address obtained during the activation of the PDP context, for example, the dynamic address

The dynamic IP address assigned to the MS by the GGSN can be either the IP address in the internal IP address pool assigned to the AP through data configuration or the dynamic IP address assigned by the AAA server or DHCP server.

When the PDP context is activated, the MS may not carry the subscriber identity information and the GGSN may not conduct subscriber identity authentication and verification.

II. Nontransparent Access

This access mode is applicable to the detached mode of mobile operator and ISP. Figure 4-2 shows an example of the nontransparent access mode.

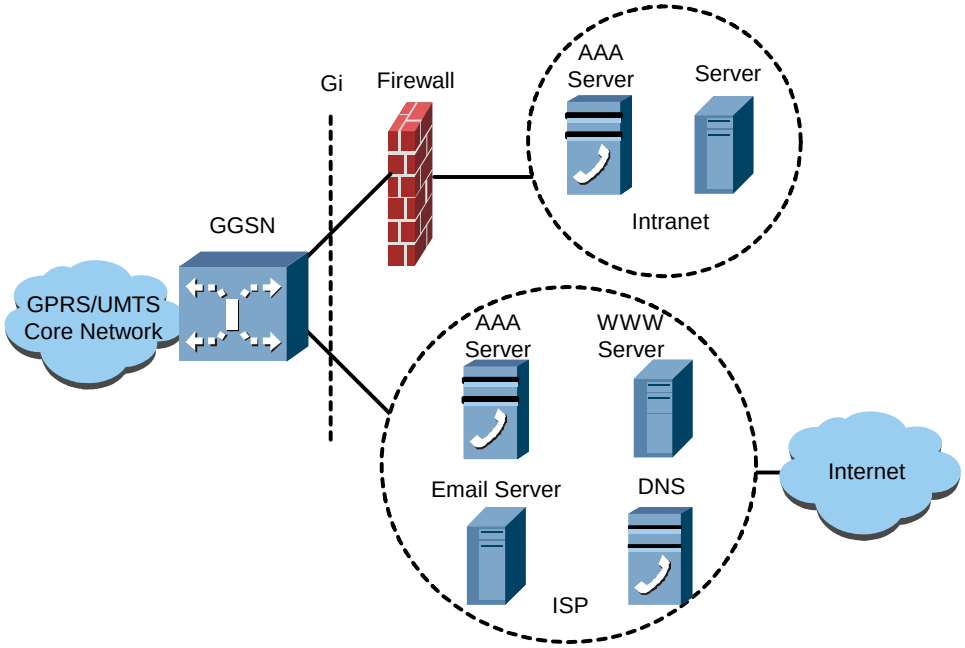


Figure 4-2 Example of nontransparent access to ISP/enterprise network

In this mode, the IP address assigned to the mobile subscriber belongs to the address space of the ISP or the Enterprise network. The IP address can either be the IP address (static address) given when subscribing services or the IP address (dynamic address) obtained during the activation of the PDP context.

The dynamic IP address assigned to the MS by the GGSN can either be the IP address in the internal IP address pool assigned to the AP through data configuration or the dynamic IP address assigned by the AAA server or DHCP server.

When the PDP context is activated, the MS carries the subscriber identity and verification information. After receiving the activation request, the GGSN conducts subscriber identity authentication and authorization through the AAA server.

4.3 GTP Functionality

4.3.1 GTP Tunneling

The GTP tunneling functionality enables data forwarding between the SGSN and the GGSN. Data packets from the PDN are given GTP encapsulation at the GGSN and then forwarded to the SGSN through the GTP tunnel between the SGSN and the GGSN. Data packets from the SGSN reach the GGSN through the GTP tunnel. At the GGSN, the packets are given GTP decapsulation and then forwarded to the PDN.

A GTP tunnel is in bidirectional point-to-point connection. It is defined jointly by the tunnel ID of the node at the two ends of a tunnel, the UDP port number and the IP address.

4.3.2 Signaling

GGSN signaling functionality includes creating, updating and deleting PDP contexts from the GGSN and maintaining part of mobility management. When an MS that is doing data service launches the flow of routing area update between the old and new SGSNs, the GGSN moves the tunnel endpoint to a new SGSN so that the data service of the MS remains uninterrupted.

The GGSN signaling entity manages the activated PDP contexts. It also takes care of GTP signaling in the UMTS/GPRS backbone and allocates dynamic IP addresses for the MSs during the PDP Context Activation phase.

4.3.3 IP and PPP over GTP

As shown in Figure 4-3, the GGSN9811 supports two types of PDPs, namely, IP (IPv4 or IPv6) over GTP and PPP over GTP. When GTP bears PPP, PPP can be terminated on the GGSN9811, or delivered to the LNS through an L2TP tunnel.

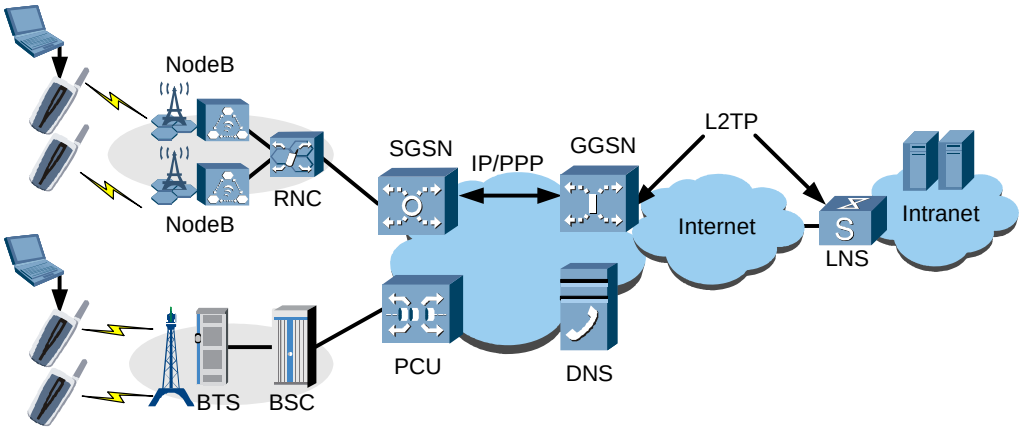


Figure 4-3 Example of GTP over IP and PPP

When GTP bears PPP, the compression function is used to improve link transmission efficiency. In enterprise networking applications, PPP over GTP can enable the enterprise to exploit the original fixed-line VPN gateway devices without the need of modifying configurations and networking information. In this case, fixed users and mobile users can be managed uniformly. In addition, for PPP over GTP, L2TP tunnels can be established or removed in real time. However, in present enterprise networking applications, because GTP bears IP, you can use only the GRE protocol to

build VPN tunnels. In this case, it is necessary that VPN gateways in the enterprise network establish tunnels with all the GGSNs in advance.

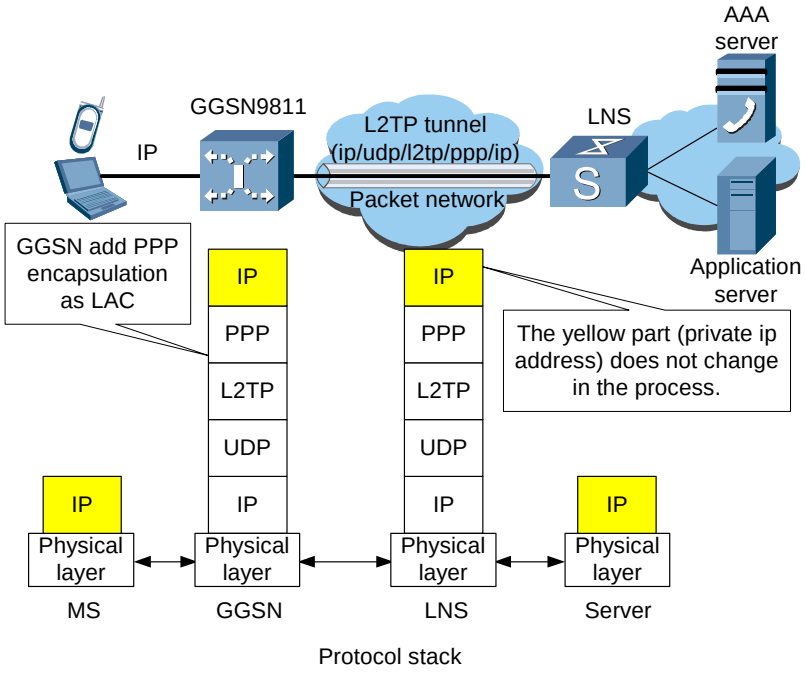


Figure 4-4 Example of PPP regeneration

GTP over IP and PPP are two basic functions of 3GPP. However, GTP over PPP is only supported by a few parts of mobile phones. Therefore, it comes to be a problem when enterprise customers tend to access their enterprise network depending on their present LNS and AAA devices without having to changing network constructer and configuration.

The GGSN9811 provides PPP regeneration, as shown in Figure 4-4, to solve the said problem. The GGSN can negotiate with the LNS device and set up PPP sessions according to the user information, such as user name and password, in user activation requests. After setting up PPP sessions, the GGSN encapsulates IP packets with PPP protocol for further transmission between the GGSN and the LNS device.

4.4 Mobile IP and Foreign Agent

4.4.1 Mobile IP

The above methods for an MS to access the PDN can support only packet services that are initiatively launched by the MS. However, when the MS moves from one network to another or it switches from one GGSN to another, the existing packet

service will be interrupted and the IP address must be reassigned or renegotiated. To solve the problem of more and more frequent MS mobility, Huawei GPRS/UMTS packet service solution has enabled mobile IP (or MIP).

The mobile IP technology is a solution for providing mobility on the IP network. This solution enables a node to keep its available communication free of interruption even if the node switches from one network to another and makes the IP address (or a home address) a permanent one for connecting with any other nodes. That is, when an MS switches from one GGSN to another, the original IP address and session are still kept and the ongoing packet service remains uninterrupted.

Under MIP architecture, in addition to the GGSN and the AAA Server, the HA is also one of the networking entities of the packet-switched core network. The GGSN is also integrated with the FA functionality.

The MIP service flow of the GGSN falls into two stages:

- Stage one: before the MS switches from one GGSN to another
- Stage two: after the MS switches from one GGSN to another

I. Stage One

Note:

The GGSN/FA mentioned in stage one refers to the GGSN/FA before the MS switches from one GGSN to another.

In stage one, the MIP service flow of the GGSN is as follows:

1 A mobile subscriber (MS) launches a packet service request, accessing the core network through the RAN. The MS then sets up a link with the GGSN/FA through the GTP tunnel between the SGSN and the GGSN/FA.

2 GGSN/FA sends agent advertisement messages, declaring its FA services. Such a message carries certain IP address of the GGSN/FA.
This IP address serves as the foreign agent care-of address of the MS.

3 The MIP-enabled MS sends a registration request to the HA through the GGSN/FA, advertising the information of the HA that the MS belongs to.
The information cannot indicate which HA the MS belongs to.

4 The GGSN/FA assigns a dynamic HA for the MS based on the information of the HA contained in the registration request. By means of the authentication message between the GGSN/FA and the AAA Server, the GGSN/FA verifies whether the MS is legal.
When the MS has passed the authentication, the GGSN/FA then will forward the registration request message of the MS to the HA.

5 The HA checks the validity of the registration request, assigning a home address for the MS (the IP address can be assigned through the local address pool, the RADIUS or the DHCP), creating a mobile binding table (that is, the mapping relation between the home address and the foreign agent care-of address), setting up a tunnel to the GGSN/FA, and then sending registration reply message to the GGSN/FA. The GGSN/FA then forwards the registration reply message to the MS.

6 The HA announces the reachability of the network prefix of the MS home address so as to attract the packets destined to the MS home address to route to the home network. The HA delivers these packets to the GGSN/FA through the tunnel. The original packets are singled out from the tunnel at the GGSN/FA and forwarded to the MS.

7 In the reverse direction, the data packets which are sent from the MS follow only the simple IP forwarding flow; instead of the HA, they go directly to the destination node on the PDN through the GGSN/FA, a default router. However, if a reverse tunnel has been applied for, the packets can also reach the HA through the reverse tunnel between the GGSN/FA and the HA and then are forwarded through the HA.

II. Stage Two

Note:

The GGSN/FA mentioned in stage two refers to the GGSN/FA after the MS switches from one GGSN to another.

In stage two, the MIP service flow of the GGSN is as follows:

1 Since the MS switches from one link to another, the MS sets up a link with the GGSN/FA through the GTP tunnel between the SGSN and the GGSN/FA.

2 This step is identical with step 2 in stage one.

3 The MS sends another registration request to the HA through the GGSN/FA, advertising the actual IP address of the HA that the MS belongs to.

4 By means of the authentication message between the GGSN/FA and the AAA Server, the GGSN/FA verifies whether the MS is legal. If legal, the GGSN/FA forwards the registration request sent from the MS to the HA.
When the MS has passed the authentication, the GGSN/FA then will forward the registration request message of the MS to the HA.

5 The HA checks the validity of the registration request, updates the mobile binding table, and then sends a registration reply message to the GGSN/FA. The GGSN/FA then forwards the registration reply message to the MS.

6 This step is identical with step 6 in stage one.

7 This step is identical with step 7 in stage one.

4.4.2 Foreign Agent

Under MIP architecture, the GGSN not only serves as a gateway device between the GPRS/UMTS and the PDN, but also integrates with FA functionality. The FA provides an MS with a foreign agent care-of address, be in charge of routing of a registered MS and forward the packets from the HA through the tunnel to the MS.

The FA functionalities that are supported by the GGSN9811 are as follows:

- Sending agent advertisements
  By sending agent advertisement messages, the FA helps an MS know whether it has moved away from its home network and provides the MS with foreign agent care-of address and other information.
- Handling registration messages
  The FA judges whether the registration message contains legal contents in the fields of registration message of an MS. If it is necessary, the FA can also send the registration message to the AAA Server for authentication and forward the legal registration message to the HA for further treatment.
- Authentication extension
  The registration is a process vulnerable for being attacked. This demands a compulsory authentication to the registration messages between an MS and the HA. The GGSN/FA supports the authentication extension of registration messages, including the authentication between an MS and the FA and that between the FA and the HA.
- Supporting both forward tunneling and reverse tunneling
  The GGSN/FA carries the IP traffic between an MS and the HA through a tunnel. At the forward tunnel (a tunnel with the HA as the start point and the FA as the end point), the FA decapsulates the IP packets from the HA and sends them to an MS. At the reverse tunnel (a tunnel with the FA as the start point and the HA as the end point), the FA encapsulates the packets from an MS and forwards them to the HA through the tunnel. The GGSN/FA supports three types of tunnel encapsulation: IP in IP encapsulation, minimum encapsulation and GRE encapsulation.
- Packet delivery
  The FA obtains packets that are forwarded from the HA through the forward tunnel and delivers them to an MS. It can also forward the packets from an MS by following the simple IP forwarding procedure or through a reverse tunnel.

4.5 Normal Billing and Hot Billing

The GGSN9811 provides rich billing functions, enabling you to exercise flexible billing policies to subscribers. The GGSN generates the GGSN Call Detail Record (G-CDR) and sends it to the CGF for handling through interface Ga. Then the processed CDR is sent to the billing center for billing process.

The G-CDR is a data service billing record generated by the GGSN side, which records the billing information relating to the PDN occupation. The billing begins after a mobile user activates the PDP context, and then a billing record is created. When the PDP context is deactivated, the billing record is closed and the billing stops. Each activated PDP context is corresponding to a G-CDR billing record.

The billing features of the GGSN9811 are as follows:

- Periodic G-CDR Generation
- G-CDR Generation Based on Traffic
- G-CDR Generation Based on the Times of Billing Condition Changes
- G-CDR Generation Based on the Times of SGSN Changes
- Multiple Charging Rate Periods
- CG Selection Function
- Hot Billing

I. Periodic G-CDR Generation

If a subscriber occupies a data connection for a long time, the CDR function will generate a CDR at specified intervals. The billing interval can be pre-configured.

II. G-CDR Generation Based on Traffic

The CDR function will generate a CDR after the subscriber transmits certain volume of data. The traffic threshold can be configured.

III. G-CDR Generation Based on the Times of Billing Condition Changes

If the times of billing conditions such as QoS and charging rate reach a certain number, the CDR function will be triggered to generate a CDR. The times of billing condition changes can be configured.

IV. G-CDR Generation Based on the Times of SGSN Changes

During the connection, if the changes of SGSN address reach a certain number (the number can be configured), the CDR function will generate a CDR.

V. Multiple Charging Rate Periods

The GGSN supports flexible setting of the billing time segment. The traffic measurement will be conducted according to specific billing rate period.

VI. CG Selection Function

The GGSN supports the CG selection function.

- If multiple CGs are configured as the same level, when multiple PDP contexts are activated, the idler CG of the same level can be selected to send the CDRs for different PDP contexts so as to realize load-sharing of the CGs.
- If multiple CGs are configured as different levels, the CG of higher level will be selected to send the CDRs so as to realize the active and standby CDR delivery relationship of CGs.

VII. Hot Billing

Hot billing is almost the same as normal billing with the exception that it generates CDR more frequently.

4.6 Content-Based Billing

The 3G technology brings speedy development of wireless data service. In contrast, the simple charging mode based on traffic or time does not keep pace with such momentum. Operators are trying to obtain more benefits from the services offered and integrate different service schemes. They set their hope on the charging model which features more diversified and dynamic granularity.

Content-based billing, or Flow Based bearer charging (FBC) as the 3GPP defines it, is a critical step toward value-based charging model. FBC enables you to charge various content and applications as well as the access. Extra benefits are thus realized.

According to the 3GPP R6, the TPF is the logic function of the GGSN. With this function, the GGSN not only differentiates the services that are charged based on content, but also implements information statistics.

At present, major operators accept the enhanced GGSN (eGGSN) as the content-based billing solution. In this solution, the GGSN on current network is upgraded to the enhanced GGSN and then directly implements content-based billing.

The GGSN9811 realizes the TPF defined in the FBC framework in the 3GPP R6. That is to say, the GGSN9811 supports both online charging (prepaid service in this manual) and offline charging (postpaid service in this manual).

The Diameter Credit Control Application is extended on the basis of the Diameter Base Protocol. It defines the charging mechanism based on the credit of prepaid service subscribers. Credit control makes the billing mode based on session and event come true. It meets the charging requirement for prepaid service.

In the GGSN9811, the Gy interface is compliant with the Diameter Base Protocol. It interacts with the OCS to offer prepaid service.

The GGSN9811 provides the CDRs defined by the 3GPP, that is, G-CDR and eG-CDR.

The G-CDR includes statistics for all services uplink and downlink traffic of a subscriber.

The eG-CDR provides separated statistics on uplink traffic and downlink traffic of various services. The eG-CDR is also able to provide statistics over the traffic of a service which is actually a combo of several services.

In the GGSN9811 system, you can specify the server for each user and monitor port traffic and duration so as to make a price and charge according to different application-layer protocols. Presently, the GGSN9811 supports such application-layer protocols as FTP, HTTP, TELNET, SMTP, POP3, and WAP.

For HTTP, WAP1.x, WAP2.0 and RTSP service traffic, this control can also be implemented based on Uniform Resource Locator (URL) address. Rules can be configured for the URL content. Once a user accesses the Web page matching a specific URL rule, you can obtain the information and billing.

You can define a special service charging rate (from zero charging rate through full charging rate) for a specific content-based billing rule based on service market policy, price mechanism, and relations with the Internet content provider. CDRs generated by content-based billing can be delivered through G-CDR extension attribute over the Ga interface, or directly generate billing records according to charging rate information set by the user on the GGSN.

4.7 Intelligent Prepaid Service

The GGSN9811 prepaid system is developed based on the mobile network and combined with an intelligent network to form a mobile intelligent network.

Mobile intelligent network calls are implemented by Service Control Point (SCP) and Service Switching Point (SSP).

- The SCP is a core component in an intelligent network. Its major function is to start different service logics based on call events reported by the SSP, and then to issue call control instruction to the relevant SSP according to service logic to implement various intelligent calls.
- The SSP is a joint point between a communication network and an intelligent network. SSF can accept and identify intelligent service calls, and report them to the SCP. In addition, the SSF is also responsible for accepting control commands sent by the SCP.

The GGSN9811 provides GPRS Service Switching Function (gprsSSF), that is, it acts as the SSP in the mobile intelligent network. In this case, it can support intelligent prepaid service in a GPRS/UMTS network. The gprsSSF interworks with the SCP to

implement the control of PDP context activation of current users from the SCP. In addition, the SCP can monitor current PDP when you perform data communication.

Based on the information in the user database, the SCP judges whether the account balance of the user is sufficient, whether the requested service is allowed, and then controls user activation process in turn. After intelligent user service is activated, the gprsSSF reports charging information to the SCP for charging.

The traditional mobile intelligent network is based on the CAP3 scheme of the SGSN/SSF. In this case, the SGSNs in the entire network need to be upgraded to support gprsSSF and HLRs in the entire network need to be upgraded to support GPRS-CSI. However, the CAP3 scheme based on the GGSN/SSF does not require upgrading the SGSNs and the HLRs. This network scheme simplifies network configuration and is easy to deploy service quickly. In addition, it solves the problem with roaming of prepaid users.

Note:

Presently, the prepaid function based on the SGSN has some difficulties in roaming:

- The SGSN in the roaming area cannot be guaranteed to also support gprsSSF.
- Even if the support is allowed, according to the stipulation in the CAMEL protocol, a user in one PLMN roams into a new SGSN in another PLMN, and the new SGSN needs to connect to the SCP in the original PLMN. But for the purpose of security, the operator will not provide SCP open interface to other operators.

In present applications, there is no successful case for PPS user roaming based on the SGSN/SSF.

For the reason of IP address assignment and management, the general practice in the industry is to enable roaming users to access through the home GGSN. Therefore, the PPS scheme based on the GGSN/SSF can solve the above problem.

4.8 Mobile VPN

The Mobile Virtual Private Network (MVPN) is a mobile data network on which VPN services are enabled. By setting up a private network based on the public packet switching network, the MVPN can make remote mobile users access an enterprise network under security. This can save a large sum of money used to spend on renting expensive private lines. It also features high security, reliability and manageability.

Based on a GPRS/UMTS network, you can make an MS access an enterprise network securely and reliably by setting up a private tunnel between the GGSN and the enterprise VPN gateways, and by applying remote user authentication and tunnel data encryption technologies.

The GGSN9811 supports tunneling technologies such as MPLS, GRE and L2TP. The operator can provide customers flexibly with a most suitable secure solution in the establishment of a VPN.

I. MPLS L3 VPN

MPLS L3 VPN provides VPN technology on the IP backbone network of the service provider. It distributes VPN routes through BGP on IP backbone networks to separate traffic between different VPN members, and then uses MPLS LSP to forward data packets on IP backbone networks.

The GGSN9811 supports MPLS L3 VPN and conforms to IETF RFC 2547.

II. L2TP VPN

L2TP tunnel is a kind of layer 2 tunneling technology. It uses IP networks to establish an L2TP tunnel and encapsulates data into PPP for delivery through the L2TP tunnel. The GGSN9811 has L2TP Access Concentrator (LAC) function and supports building VPN through L2TP tunnel for transporting PDP PDU. L2TP tunnel conforms to the definition in RFC 2661 regardless of whether the type of PDP PDU is PPP or IP.

III. GRE VPN

GRE tunnel is a kind of layer 3 tunneling technology, enabling encapsulation of any network layer protocol over another network layer protocol. The GGSN9811 supports GRE tunneling. IP network protocol can be used by GRE to transmit upper layer protocols so as to provide VPN functionality. The GRE tunnel must conform to the definitions in RFC 1702 and RFC 1701.

Figure 4-5 shows an example of network interconnection with GRE to create VPN.

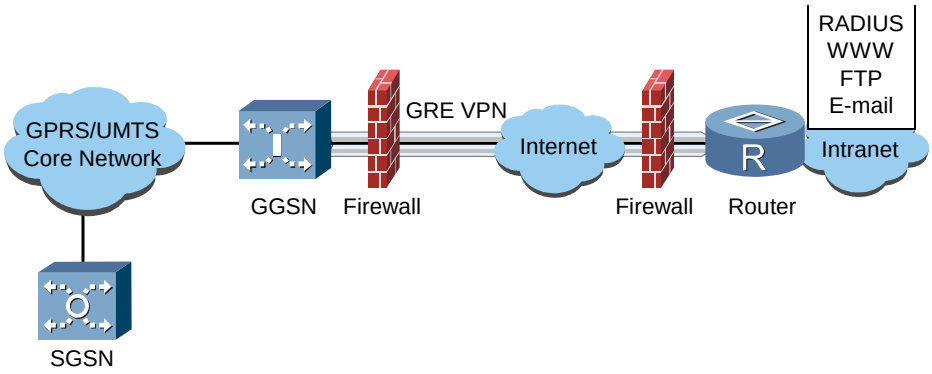


Figure 4-5 GGSN realizes VPN through GRE

For subscribers using the GRE function, when a subscriber message is sent, the GRE encapsulation of the subscriber message will be conducted first and then the message will be sent out from the Gi interface. When the peer router receives the

message, it firstly conducts GRE decapsulation and then sends the message to the destination equipment. When the destination equipment completes the relevant processing, it sends a response message, which is then given GRE encapsulation by the peer router and sent to the GGSN. When the Gi interface receives the message with GRE encapsulation, it conducts GRE decapsulation first and then the GGSN will perform GTP encapsulation. Finally it is forwarded to the SGSN where the mobile station is.

4.9 Security

The design of GGSN9811 has fully considered the implementation of the security policies.

4.9.1 Protocol Security Authentication

The GGSN9811 supports the following protocol security authentication:

- When in simple IP connection, the GGSN9811 carries out authentication and authorization to an MS by interacting with the AAA Server.
- When mobile IP connection, the GGSN9811 needs to carry out authentication to the registration message between an MS and the HA. The GGSN/FA supports authentication extension of the registration message, including authentication between an MS and the FA, and that between the FA and the HA.
- The GGSN9811 provides more than one authenticating methods such as plain text authentication, MD5 and HMAC-MD5, for important routing protocols such as RIP v2, OSPF, IS-IS, and BGP.

4.9.2 IPSec

IP Security (IPSec) protocol family is a series of protocols defined by the IETF. It provides high-quality, interoperable and cryptology-based security for IP data packets. The two sides of communication perform encryption and data source authentication on IP layer to assure confidentiality, data integrity, data origin authentication and anti-replay for packets when they are being transmitted on networks.

IPSec implements the above aims by Authentication Header (AH) security protocol and Encapsulating Security Payload (ESP) security protocol. Moreover, Internet Key Exchange (IKE) provides auto-negotiation key exchange and Security Association (SA) setup and maintenance services for IPSec so as to simplify the use and management of IPSec.

The GGSN9811 supports IPSec on interfaces Gn and Gp, interface Gi, interface Ga, physical interfaces and operation and maintenance interfaces. It can set up IPSec tunnel to the following entities of the SGSN, AAA Server, CG, HA, router and

maintenance host, authenticate or encrypt the data stream going between them so as to ensure security of the data.

The GGSN9811 supports the following IPSec functions:

- Implementing MD5 and SHA-1 authentication algorithms
- Implementing DES, 3DES and AES encryption algorithms
- Supporting two IPSec modes: the transmitting mode and the tunneling mode
- Implement AH and ESP protocols and supporting binding of AH and ESP
- Manually Configuring security associations or automatically negotiating security associations through IKE
- Realizing IPSec VPN by binding VRF to the interface where the IPSec situates

The above features are implemented by means of a hardware encryption card so as to ensure high performance.

4.9.3 Packet Filtering and ACL

The GGSN9811 provides packet filtering and ACL mechanism, filtering each packet according to the defined conditions (for example, by comparing whether the source address of a packet, or the destination address of it or other items conform to the rules). This can effectively prevent illegal invasion or ill-intentioned attacks.

4.9.4 Gi Redirection

Generally, the GGSN carries out routing search to the inner layer of IP datagrams that are obtained by decapsulation of the packets from an MS. If the IP addresses in the packets are destined to other MSs in the same GGSN, the GGSN will directly encapsulate and forward the downlink datagrams rather than letting them go through the interface Gi. This has brought about an issue of security: the datagram attacks among the mobile users in the same GGSN cannot be prohibited.

The Gi redirect function of the GGSN9811 can solve the above problem. When forwarding uplink packets from users, the GGSN9811 is requested to redirect datagrams to Gi even if the datagrams are destined to other mobile users under its administration. After being filtered by the firewall that connects the interface Gi, the datagrams are retransmitted to the GGSN9811 and then encapsulated and forwarded by the GGSN9811.

4.10 Accessing the IMS Domain

The GGSN9811 supports access to the IMS domain.

The IMS is a new added subsystem in 3GPP R5 on the WCDMA network. It functions on the control plane and is borne by the PS domain.

The PS bearer domain creates sessions for IP multimedia services and transfers data. The Go interface is used for creating relationship between the IMS session (SIP/SDP) and the PS bearer domain.

The introduction of IMS in PS domain inherits the idea of separating the bearer function from the control function in the CS of R4. The IMS enables all mobile subscribers to be offered with the Internet services irrespective of time and place.

In the preceding UMTS version, real time multimedia services are provided by the PS domain. The PS, however, only provides the service within its capacity without QoS. This means that the quality of the real time multimedia sessions is not guaranteed.

The IMS proposed in R5 is improved in the aspects of QoS, charging and integration of different services. This provides a favorable platform for developing further services on the PS domain.

4.11 QoS

GRRS/UTMS criterion specifies the QoS from MS to 3G gateway, which is actually an end-to-end QoS. Down to earth, the end-to-end QoS depends on the QoS features of every node on the transmission path. Thus, when the traffic is passing through the IP-based GPRS/UMTS core network, the QoS negotiated in the PDN context activation should be mapped to the DSCP field or ToS field in the IP header according to a certain mapping rule. The queue scheduling is completed by IP QoS to provide the end-to-end QoS.

The GGSN9811 supports QoS negotiation and mapping. The context activating request message of an MS carries the QoS Requested. The GGSN9811 implements QoS negotiation according to this QoS information and its own configuration, maps the negotiated QoS parameter into the differentiated service priority of the IP network, fills it into the ToS field or DSCP field at the head of datagrams and finally forwards the datagrams to the external PDN. Relying on this, the external network implements IP QoS queue scheduling so as to guarantee the QoS of packet service.

The GGSN9811 supports differentiated QoS and the QoS for streaming service.

I. Differentiated QoS

The GGSN9811 supports differentiated service, which is mandatory in the UMTS 6.0. In other words, graded services are provided for subscribers who have different demands.

Technically, the Allocation/Retention Priority (ARP) in the activation request controls the subscriber’s access and bearer priority.

For the subscribers of different grade, the GGSN9811 provides QoS of different levels.

II. QoS In Streaming Service

In the 3GPP R6, the peer-to-peer QoS architecture in the UMTS poses a strict requirement on the terminal, which is supposed to be able to sense and negotiate service QoS.

Huawei's solution resolves two problems. The first problem is that the bearer network is unable to sense service QoS requirement. The second is the over waste and insufficient utilization of airborne wireless resources.

Huawei's UTMS streaming solution achieves QoS dynamic policy control based on the network PUSH mode. In the solution, the network completely controls the process of QoS sensing and application. The GGSN supports the QoS refreshment according to PDF delivery policy. This realizes the E2E QoS stipulated in the 3GPP R6 without making any change in the terminals.

In addition, as an enhanced router, the GGSN9811 supports the following QoS features such as traffic policing, traffic shaping, queue scheduling and congestion control. They are implemented by hardware, which results in high performance.

4.12 IPv6

IPv6 is developed on the basis of IPv4. To cope with the shortcomings of IPv4, IPv6 has adopted many measures and been enhanced with many new features, including more adequate address spaces, higher security and better support of mobility and QoS and so on. IPv6 has laid a solid foundation for the sustainable development of the IP network.

IPv6 is introduced to 3GPP in phase R5. In phase R5, the IMS is carried by IPv6. The RNC, SGSN and GGSN are interconnected by IPv4 or IPv6. Users' terminals have dual IPv4/IPv6 stacks so that they can access IPv4/IPv6 services.

Currently, the GGSN9811 supports basic IPv6 access services: it supports IPv6 carrying on the users' plane rather than the IPv6 features on the signaling plane. That is, the GGSN9811 is still in the IPv4 networks. With the interconnection of the IPv4 network with the SGSN and the PDN, the uplink IPv6 datagrams from a mobile user, after being encapsulated in the IPV4+GTP datagrams by the SGSN, are sent to the GGSN9811. The GGSN9811 decapsulates the GTP datagrams and singles out IPv6 datagrams from them. Then the IPv6 datagrams are forwarded according to the configuration of the system to the IPv6 gateway through the IPv4 tunnel. The IPv6 gateway finally implements the routing forwarding or protocol transform (IPv6/IPv4 transform) of the IPv6 datagrams. For downlink datagrams, when the GGSN9811 find out that a user is of IPv6, it decapsulates the datagrams, singles out the IPv6 datagrams, and then carries out GTP encapsulation and deliver them to the SGSN.

This function enables the following services:

- Mobile terminals of IPv6 accessing IPv6 services
- Mobile terminals of IPv6 accessing IPv4 services

4.13 Others

The GGSN9811 also supports the following services and functions:

- Supporting more than one IP address assigning mode

Under simple IP connection, the IP address that is assigned to an MS can either be a static IP address or a dynamic IP address. A dynamic address can be assigned either from the local address pool of the GGSN9811, or by the RADIUS or DHCP on the request of the GGSN9811. The IP address assigned to an MS can be either a public IP address or a private IP address. If it is a private IP address, it must be transformed by the NAT server.

Under mobile IP connection, the home address of an MS is assigned by the HA. This IP address can be either a public IP address or a private IP address. If it is a private IP address, a reverse tunnel must be set up between the GGSN9811 and the HA.

- Enabling Network Time Protocol (NTP)

As the NTP client, the GGSN9811 can enable network time synchronization with the NTP Server.

- Supporting SNMP V1and SNMP V2 and SNMP V3

Chapter 5 Operation and Maintenance

The GGSN9811 provides easy operation and maintenance (O&M) management system. It includes the following functions:

- Local Maintenance Terminal (LMT) provides MML and GUI for operation and maintenance.
- Access to HUAWEI M2000 and OMC network management system.
- Rich online help.

5.1 LMT

The LMT consists of:

- O&M System
- Alarm Forwarding System
- Monitor Reviewer
- Performance Browser
- Tracing Reviewer

The functions of the LMT of the GGSN9811 are detailed in the following sections:

- Alarm Management
- Equipment Management
- Message Tracing
- Data Configuration Management
- Centralized User Management
- Log Management
- Performance Management

5.1.1 Alarm Management

The alarm system of the GGSN9811 is responsible for monitoring the system operation and notifying the detected fault or disturbance to the maintenance personnel through audio and visual alarms.

The GGSN9811 alarm system mainly provides the following alarms:

- GRE tunnel fault
- Software fault
- CPU load fault
- Board fault
- Board switchover fault
- Hard disk space fault

- Hard disk fault
- GTP path fault
- Database fault
- AAA server fault
- Software loading fault

The GGSN9811 provides the following two alarm output modes:

- Alarm box
  This is the main equipment for audio and visual alarms in the GGSN9811 system. When an alarm is sent to the alarm box, the alarm indicator of a certain level on the alarm box will be on and alarm sound will be given out in the meantime.
- Alarm client
  This can observe the real-time alarm generated by the system at the alarm client. In addition, you can conduct history alarm query, alarm information print, alarm box control and so on.

5.1.2 Equipment Management

The equipment management function refers to the functions of monitoring, control, and test of the system hardware and software.

I. Information Query Function

The following information can be queried:

- Board information, such as state and version
- Subscriber information, such as context and number of subscribers
- APN information, such as address pool
- Various types of GTP-C/GPT-U information, such as number of paths and path state
- Data backup process information
- Fan state
- Power state
- Subrack temperature
- Time information of the system and the NTP Server

II. Control Function

The control functions are as follows:

- Board switchover
- Component reset
- Activated subscriber bandwidth modification
- Subscriber deactivation
- CPU occupancy report control
- System time setting

III. Test Function

The test functions are as follows:

- Context self-test
- Self-loop test of Ga interface
- GTP communication test of GTP-U
- GTP signaling path communication test
- PING function test
- Tracert function test

IV. Patch Management Function

The patch management functions are as follows:

- Activation
- Deactivation
- Deletion
- Running
- Loading
- Information query

V. Loading Function

The loading function includes functions such as the management of board software loading version, forced board software loading.

5.1.3 Message Tracing

The GGSN9811 provides the message tracing function for Ga, Gn/Gp, Gi, Gy, and Go interfaces. Furthermore, it provides the message tracing function for subscribers of the specified IMSI or MSISDN.

The tracing management mainly implements functions such as tracing task creation/deletion, message browsing, message explanation, message storage and tracing message review.

- Tracing task control

The tracing task start/stop function is provided. Each control console can simultaneously start multiple tracing tasks. Furthermore, to guarantee the system overhead, the maximum number of tracing tasks that can be started simultaneously is limited to 16.

- Message browsing

With this function, you can browse the tracing messages. Different tracing tasks generate corresponding message browse windows which display the messages

returned by the OM. Message browsing supports the functions of automatic scroll display and stopping scroll display.

- Message storage

With this function, you can store the tracing messages, and can also save files automatically and manually. Furthermore, user-defined file name is supported.

- Message explanation

This function provides the content and explanation of the tracing messages. The message contents are shown in the message explanation window.

- Tracing review

This function supports the browsing and explanation of historical tracing messages. You can select the tracing message file to be viewed and browse it.

5.1.4 Data Configuration Management

The data configuration management includes operations such as system data addition, deletion, modification, and query. The GGSN9811 data configuration includes hardware data configuration, system information configuration, GTP protocol related configuration, charging configuration, FA configuration, VPN configuration, QoS configuration, and security configuration.

5.1.5 Centralized User Management

The GGSN9811 enables centralized management of user accounts. In this management mode, there are two types of account as follows:

- Domain account
  A domain account is the user account which is centrally managed by the M2000. This type of account is created, modified, authenticated and authorized by the M2000.
- Local account
  A local account is managed by the GGSN9811 independently. It can be managed through system installation and network element login.
  The GGSN9811 manages local accounts by limiting the operation commands set for users of different levels. This ensures the safe and reliable operation of the system.

5.1.6 Log Management

Based upon the contents, the log can be divided into user operation log and system operation log. The former records information such as user name, commands executed and execution time, and facilitates the fault analysis and responsibility division. The latter records some state information during system operation for the

convenience of system maintenance and fault locating. The system also provides the User Operation Log query function.

5.1.7 Performance Management

The GGSN supports the statistics and measurement of varied services and objects.

The analysis of the statistic data is helpful for understanding the operation of the gateway device. It also provides basic data for the planning and design of telecommunication network as well as its operation, management and maintenance.

The system provides the function of performance measurement. This enables you to configure the object to be measured, change the measurement period, query the measurement state and browse the result.

5.2 Access to the M2000 and the OMC

The GGSN9811 can access HUAWEI M2000 and OMC network management system. Though the M2000 or the OMC, you can perform centralized configuration management, centralized alarm management and centralized performance management.

5.3 Online Help

The GGSN9811 provides rich online help documents so that you can easily learn and use the equipment. The online help provides reasonable retrieval mode so that you can conveniently obtain required information online.

The GGSN9811 online help documents include the O&M system, alarm management system and command line help. An example of the GGSN9811 online help is shown in Figure 5-1.

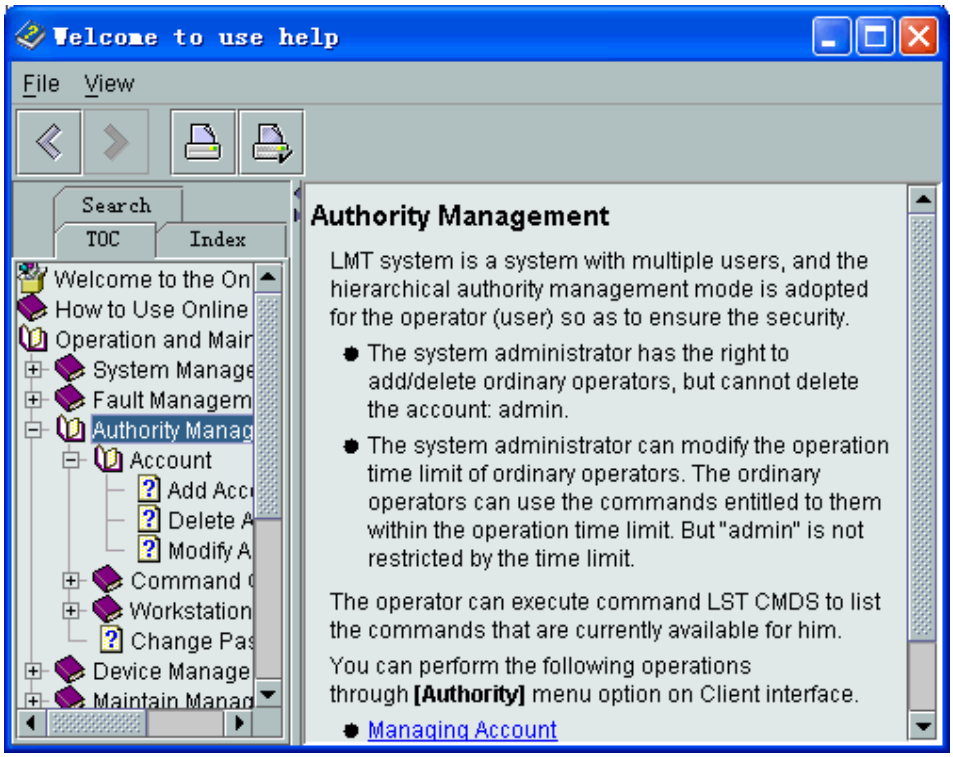


Figure 5-1 GGSN9811 online help

Chapter 6 Reliability

During the product design of the GGSN9811, the reliability design has been taken into full consideration in the three aspects of hardware, software and networking so that normal operation of the product is effectively guaranteed.

6.1 Hardware Reliability

- The hardware platform of the GGSN9811 is based on the USR, which is the core router of the fifth generation. It uses the advanced NP technology. Most of the functions can be realized with one or two chipset, which greatly reduces the influence to the system that results from unstable chipset operation.
- All key boards support online plugging and active and standby redundancy functions. When an active board is abnormal or unplugged, the standby one will automatically take over instantly and become the active, making the service flow free of interruption.
- The double-channel –48 V power supply mode is adopted, providing the load sharing function.
- Over-voltage/over-current protection measure is adopted for the board power input and external interfaces. The applied measures satisfy requirements of the ITU-T G.703 Recommendation Annex B and relative specifications.
- The flash memory element is used so that both the programs and static data can be saved permanently, convenient for quick recovery of both the programs and data.

6.2 Software Reliability

- System overload control
  When the CPUs are overloaded, the system can shut down some less necessary functions by means of the overload control function, or adjust the access volume of users to prevent the system from breaking down due to overload. The threshold for overload control can be dynamically configured.
- Traffic control
  The GGSN9811 automatically checks whether system load is greater than the expected, and then takes different traffic control measures according to load extents. By this function, the system is guaranteed not to break down while running overlarge traffic or suffering from malicious attack. Even if in such case, the system can be restored to a normal and stable status in a short time.

- System resource check
  This function can compare data in the system database with the current running data, if inconsistent, the data can be restored with this function.
- Self fault detection and recovery
  When the system (either software or hardware) is faulty, some detection measures should be taken to find the faults for fault isolation and system recovery from faults. The system can take certain measures (such as automatic switchover with normal boards, automatic reset of abnormal board) to remove some malfunctions
- Billing reliability measures
  The GGSN9811 supports bill buffer function. When a communication problem occurs between the GGSN9811 and the CG, if the CG still fails to respond even though the billing records have been re-sent for many times, the GGSN9811 will make a buffer area on the hard disk to store the billing records. As soon as the communication to the CG returns to normal status, the buffered billing records will be re-sent to the CG.
- Board LOCK and system SHUTDOWN
  With this function, the services that are processed by either the boards or the system can cease in a gradual way, rather than stopping suddenly.
- Hot patch technology
  Such a technology that is provided by the GGSN9811 can guarantee that upgrade of software will not influence the normal operation of the equipment.

6.3 Networking Reliability

Networking reliability is guaranteed by the following functions:

- Router backup and router load sharing: In networking, single-point fault on the network can be eliminated so that a network of high reliability is guaranteed.
- Eth-Trunk: The GGSN9811 can bundle many Ethernet ports into one Eth-Trunk port, which works as an ordinary Ethernet port. The bundled port can send data in active/standby mode. Even if one port fails to work, the service can still go without interruption.

6.4 Reliability Specifications

The reliability specifications of the GGSN9811 are as follows:

- System availability: Equal to or larger than 99.99978%
- Mean Time Between Failures (MTBF): Equal to or larger than 461,000 hours
- Mean Time To Repair (MTTR) of the system: Equal to or smaller than one hour (preparation time excluded)
- Yearly board repair ratio: Equal to or smaller than 3%

Chapter 7 Technical Specifications

7.1 Capacity Specifications

Capacity specifications of the GGSN9811 are listed in Table 7-1.

Table 7-1 GGSN9811 capacity specifications

Parameter	Specification
Maximum PDP contexts	1,050,000 (A whole system can be configured with three pairs of SPUs, with each pair of SPUs supporting 350,000 PDP contexts at most.)
Maximum packet handling capacity	1,000,000 PPS
Maximum data throughput	3 Gbit/s
IPSec throughput	600 Mbit/s (A whole system can be configured with three pairs of SPUs, with each pair of SPUs supporting up to 200 Mbit/s.)
Maximum number of APNs	1,000
Maximum number of GRE tunnels	4,000
Maximum number of L2TP tunnels	6,000
Maximum number of IPSec tunnels	5,000

7.2 Physical Dimensions and Power Supply

7.2.1 Physical Dimensions

The GGSN9811 is mounted on a Huawei N68-22 cabinet with the following physical dimensions:

- Height: 2,200 mm
- Depth: 800 mm
- Width: 600 mm
- Weight: less than 300 kg (single cabinet); less than 500 kg (double cabinets required in CAMEL prepaid service)

7.2.2 Power Supply

DC input: –48 V to –60 V

7.2.3 Total Power Consumption

- Less than 1,400 W maximum (single cabinet)
- Less than 2,000 W (double cabinets required in CAMEL prepaid service)

7.3 Environment Requirements

7.3.1 Temperature

- Long-term operation: 5ºC to 40ºC
- Short-term operation: –5ºC to +50ºC

7.3.2 Relative Humidity

- Long-term operation: 5% to 85%
- Short-term operation: 5% to 90%

7.3.3 Storage Condition

- Complies with the storage condition standard of 1.3E equipment defined in ETS 300 019-1-1.
- The floor load should be greater than 600 kg/m^2.
- The relative humidity of storage is 8% to 100%.
- The storage temperature is –40ºC to +70ºC.

7.3.4 EMC

The GGSN9811 complies with the following EMC standards:

- EN300386-2
- EN55022
- EN50082-1
- EN61000-3-2
- EN61000-3-3

7.3.5 Safety

The GGSN9811 complies with the following safety standards:

- UL1950
- CE Mark
- CUL/CSA 22.2 NO 950–M93

- IEC950
- TUV EN60950

Chapter 8 Installation

Installation of the GGSN9811 includes hardware installation and software installation.

8.1 Introduction to Hardware Installation

Figure 8-1shows a regular hardware installation flow of the GGSN9811.

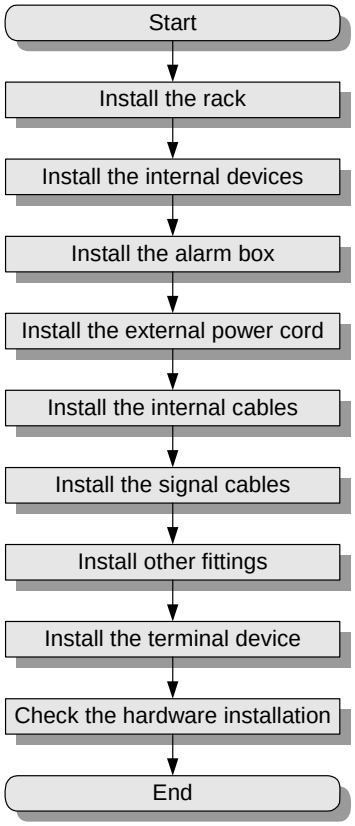


Figure 8-1 GGSN9811 hardware installation flow

8.2 Introduction to Software Installation and Upgrade

The GGSN9811 has been installed with host software before delivery. You only need to install the LMT software of the Windows system to provide services and data configurations.

You can upgrade host software through the LMT.

Chapter 9 Acronyms and Abbreviations

3

3GPP	3rd Generation Partnership Project

A

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AH	Authentication Header
AP	Access Point
APN	Access Point Name
ARP	Address Resolution Protocol

B

BG	Border Gateway
BGCF	Breakout Gateway Control Function
BGP-4	Border Gateway Protocol 4
BSC	Base Station Controller
BSS	Base Station Subsystem

C

CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CCF	Call Control Function
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CG	Charging Gateway
CGF	Charging Gateway Functionality
CN-CS	Core Network-Circuit Switching
CN-IMS	Core Network-IP Multimedia Subsystem
CN-PS	Core Network-Packet Switching

COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
CS	Circuit Switched (CS) domain
CSA	Canadian Standards Association
CSPC	Compress Service Processing Card

D

DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSCP	DiffServ Code Point

E

E2E	End to End
eG-CDR	enhanced GGSN Call Detail Record
EMC	Electromagnetic Compatibility
ESP	Encapsulating Security Payload
ETS	European Telecommunication Standards

F

FA	Foreign Agent
FBC	Flow Based Charging
FE	Fast Ethernet
FTP	File Transfer Protocol

G

G-CDR	GGSN Call Detail Record
GE	Gigabit Ethernet
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPRS-CSI	GPRS-CAMEL Subscriber Information

gprsSSF	GPRS Service Switch Function
GRE	Generic Routing Encapsulation
GSAU	GGSN9811 Signaling Access Unit
GSM	Global System for Mobile Communications
GSN	GPRS Support Node
GTP	GPRS Tunneling Protocol
GTP-C	Control plane part of GPRS tunneling protocol
GTP-U	User plane part of GPRS tunneling protocol
GUI	Graphic User Interface

H

HA	Home Agent
HLR	Home Location Register
HTTP	Hyper Text Transport Protocol

I

I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMS-MGW	IMS Media Gateway Function
IP	Internet Protocol
IPSec	IP Security Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermedia System-Intermedia System
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector

K

KVM	Keyboard&Video&Mouse

L

L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LMT	Lifecycle Management Team; Local Maintenance Terminal
LNS	L2TP Network Server
LPU	Line interface Processing Unit
LSP	Label Switching Path

M

MBR	Mobility Binding Record
MGCF	Media Gateway Control Function
MIP	Mobile IP
MML	Man-Machine Language
MPLS	Multi-Protocol Label Switching
MRFC	Multimedia Resource Function Controller
MS	Mobile Station
MSISDN	Mobile Station International ISDN Number
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MVPN	Mobile Virtual Private Network

N

NAT	Network Address Translation
NP	Network Processing
NTP	Network Time Protocol

O

OCS	Online Charging System
OM	Operation and Maintenance
OMC	Operation & Maintenance Center
OSPF	Open Shortest Path First

P

P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PDN	Public Data Network
PDP	Packet data protocol
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PPS	Prepaid Service
PS	Packet Switching
PSTN	Public Switched Telephone Network

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial in User Service
RAN	Radio Access Network
RFC	Request for Comments
RIP	Routing Information Protocol
RNC	Radio Network Controller
RTSP	Real-Time Streaming Protocol

S

SC	Service Control
SCP	Service Control Point
S-CSCF	Serving Call Session Control Function
SDP	Service Data Point
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPU	Service Processing Unit

SRU	Switching and Routing Unit
SSF	Service Switching Function
SSP	Service Switching Point

T

ToS	Type of Service
TPF	Traffic Plane Function

U

UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USR	Universal Switching Router
UTMS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network

V

VPN	Virtual Private Network
VRF	Virtual Route Forward
VRP	Versatile Routing Platform

W

WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WWW	World Wide Web