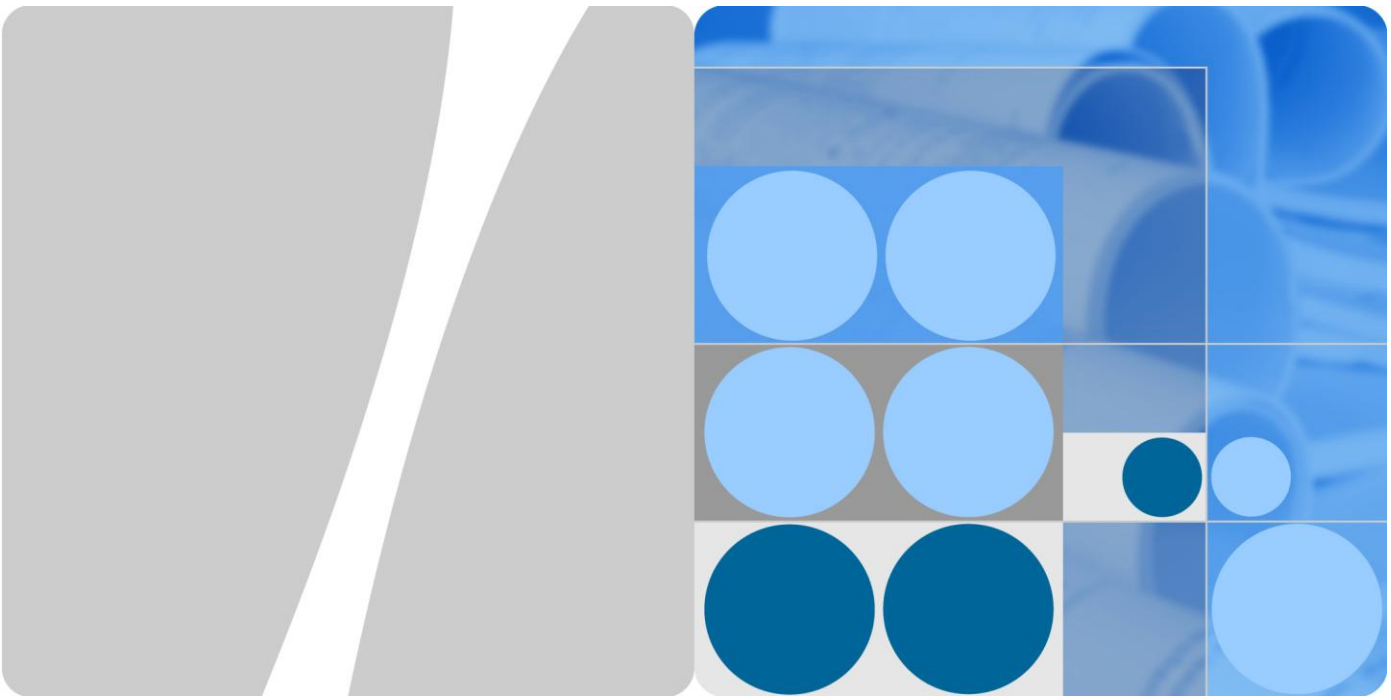


HUAWEI SeMG9811
Product Description

Issue 02

Date 2014-06-17

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 Introduction

About This Chapter

1.1 Positioning

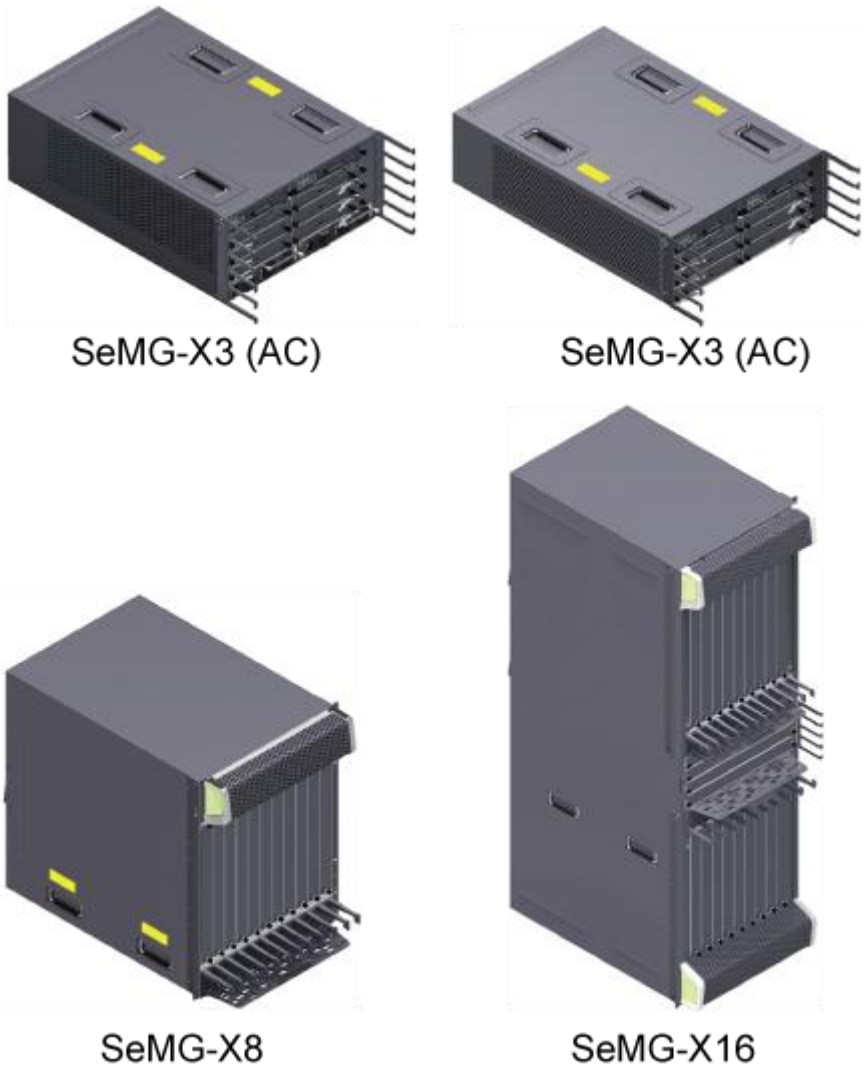
This document is for HUAWEI SeMG9811 V300R001C00.

HUAWEI SeMG9811 series (the SeMG9811 for short) is a high-end 10-Gigabit compositive security gateway. The SeMG9811 is applicable to Internet backbone networks, IP dedicated backbone networks, IP metropolitan area networks (MANs), Internet data center (IDC) egress, and campus and large enterprises' network egress. It provides multiple powerful and all-round security solution with great flexibility.

The SeMG9811 comprises the SeMG9811-X3, the SeMG9811-X8, and the SeMG9811-X16.

In addition, the SeMG9811-X3 provides AC and DC models for users to select.

Figure 1-1 SeMG9811 series



1.2 Highlights

Industry No. 1 performance, ready to cope with surging traffic

The SeMG9811 performs best in the industry:

- The 10-Gigabit line-speed forwarding and the performance of up to 960 Gbit/s easily address the challenges brought by Web 2.0.
- With up to 960,000,000 concurrent connections per second and coordinated overall performance with connection quality, the SeMG9811 supports Web 2.0 applications.
- With up to 12,000,000 new connections per second, the SeMG9811 easily meets the challenges of burst problems such as surging traffic in rush hours and DDoS attacks to ensure a non-disruptive network.

With the overall penetration of wireless services, the number of mobile subscribers grows rapidly. The concurrent access of numerous mobile subscribers imposes a higher requirement for device performance. In addition, security problems in the transmission of wireless network

information become increasingly pressing. VPN devices are facing new challenges of stronger processing capability and larger capacity.

The SeMG9811 provides the best VPN performance in the industry:

- Up to 960,000 VPN concurrent tunnels
- Up to 768 Gbps (3DES/DES/AES) encryption performance

The SeMG9811 supports the IKE v2 protocol and enhances the functions of user authentication, packet authentication, and NAT traversal. Thus, the SeMG9811 eliminates the hidden hazards of man-in-the-middle attacks and DDoS attacks and supports wireless authentication protocols, such as EAP-SIM and EAP-AKA. In addition, the device supports PKI/CA, and can authorize and authenticate VPN access devices. All these features effectively safeguard wireless networks.

Distributed and scalable architecture, improving the return on investment (ROI)

The SeMG9811 adopts the distributed and scalable architecture with independent service processing units (SPUs) and line interface processing units (LPUs) which can be configured as per requirements. The flexible scalability satisfies the demand of increasing service traffic, and improves the investment return ratio.

The overall performance of the SeMG9811 including throughput, number of concurrent connections, number of connections established per second, and other indexes increases linearly as the number of SPUs grows.

Full redundancy and high reliability, ensuring service continuity

The SeMG9811 provides a comprehensive and reliable end-to-end solution. With high-end router level reliability, the SeMG9811 ensures service continuity:

- Device-level reliability
  - Dual-Main Processing Unit (MPU) backup supports a smooth switchover between MPUs.
  - N+1 backup of Switch Fabric Units (SFUs) enables inter-board data exchange and load balancing.
  - Load balancing and hot backup can be performed among SPUs of the SeMG9811. When a SPU is faulty, the system automatically switches services traffic to other SPUs to prevent the impact of SPU anomaly on services. This improves system reliability greatly.
  - The SeMG9811 has redundant components. In addition, the power modules and fan modules are hot-swappable.
- Network-level reliability
  - The SeMG9811 supports the dual-system hot backup based on the Huawei Redundancy Protocol (HRP), including active/standby backup and load balancing modes. The HRP backs up key configuration commands and the information about session table status from the active device to the standby device. In this manner, the standby device can smoothly take the place of the failed active device.
  - The SeMG9811 supports dedicated external bypass devices. When the SeMG9811 is faulty, network traffic can be forwarded by the Bypass device in a timely manner to ensure service continuity.
- Link-level reliability

- The SeMG9811 supports cross-board interface binding enabling balanced traffic forwarding, improving the link availability, and broadening total bandwidth.
- The SeMG9811 supports Bidirectional Forwarding Detection (BFD).

2 Architecture

About This Chapter

2.1 Hardware Structure

2.1.1 Product Appearance

The SeMG9811 uses an integrated chassis. The chassis can be installed in an N68E-22 cabinet or a standard International Electrotechnical Commission (IEC) 19-inch cabinet with a depth no less than 800 mm.

SeMG9811-X3 Chassis Overview

The SeMG9811-X3 chassis have both AC and DC models. Figure 2-1 shows a DC chassis, and the Figure 2-2 shows an AC chassis.

Figure 2-1 Appearance of a DC chassis

Figure 2-2 Appearance of an AC chassis

Figure 2-3 shows the slots of the SeMG9811-X3.

Figure 2-3 Diagram of the board slot area

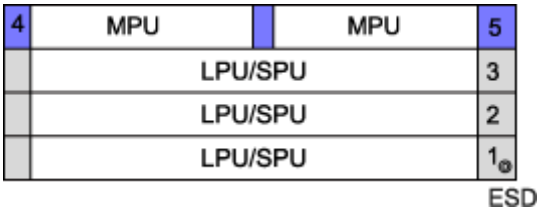


Table 2-1 Slot location of the SeMG9811-X3

Slot Number	Quantity	Slot Width	Remarks
1 to 3	3	41 mm (1.6 inches)	Indicates the slots for Line Processing Units (LPUs) and Service Processing Units (SPUs). The LPUs and SPUs can co-exist to suit your individual requirements. But at least one LPU and one SPU is needed.
4 to 5	2	41 mm (1.6 inches)	Indicates the slots that are dedicated for the Main Processing Unit (MPU). The slot can house two MPUs to form 1:1 backup.

SeMG9811-X8 Chassis Overview

Figure 2-4 shows the chassis of the SeMG9811-X8.

Figure 2-4 Appearance of the chassis of the SeMG9811-X8

Figure 2-5 shows the slots of the SeMG9811-X8.

Figure 2-5 Diagram of the board slot area

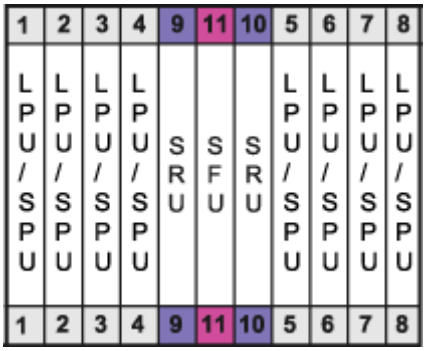


Table 2-2 Diagram of slot location

Slot Number	Quantity	Slot Width	Remarks
1 to 8	8	41 mm (1.6 inches)	Indicates the slots for LPUs and Service Processing Unit As (SPUAs). The LPUs and

Slot Number	Quantity	Slot Width	Remarks
			SPUAs can be inserted at the same time. Select the LPUs and SPUAs as required. But at least one LPU and one SPUA is needed.
9 to 10	2	36 mm (1.4 inches)	Indicates two slots that are dedicated for Switch Router Units (SRUs). The slots can house two MPUs to form 1:1 backup.
11	1	36 mm (1.4 inches)	Indicates the slot for the Switch Fabric Unit (SFU). The SFU interworks with the SFU integrated on the SRU to form 2+1 backup for load-balancing.

SeMG9811-X16 Chassis Overview

Figure 2-6 shows the chassis of the SeMG9811-X16.

Figure 2-6 Appearance of the chassis

Figure 2-7 shows the slots of the SeMG9811-X16.

Figure 2-7 Diagram of the board slot area

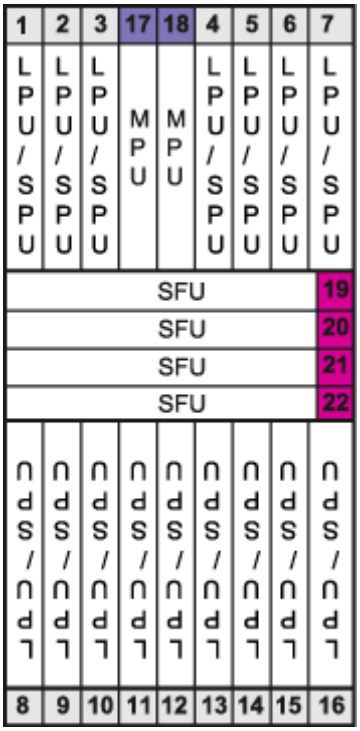


Table 2-3 Diagram of slot location

Slot Number	Quantity	Slot Width	Remarks
1 to 16	16	41 mm (1.6 inches)	Indicates the slots for LPUs and SPUAs. The LPUs and SPUAs can be inserted at the same time. Select the LPUs and SPUAs as required. But at least one LPU and one SPUA is needed.
17 to 18	2	41 mm (1.6 inches)	Indicates the slots that are dedicated for MPUs. The slots can house two MPUs to form 1:1 backup.
19 to 22	4	41 mm (1.6 inches)	Indicates the slots for SFUs. The slots can house four SFUs to form 3+1 backup for load balancing.

Power and Heat Dissipation Systems of the SeMG9811

Table 2-4 shows the overview of the power and heat dissipation systems of the SeMG9811 of different models.

Table 2-4 Overview of the power and heat dissipation systems of the SeMG9811 of different models

Component	SeMG9811-X3	SeMG9811-X8	SeMG9811-X16
Power supply system	Supports AC or DC power supplies.		
	The power supply system consists of 1+1 redundant AC or DC power supply frames. Both the AC and DC power supply frames support power alarming.	• In DC mode, four Power Entry Modules (PEMs) reside on the back panel to provide 2+2 backup. • In AC mode, an AC power supply frame resides externally, and connects to the power input ports of the PEMs through a rectifier that suits the total power of the integrated chassis.	• In DC mode, eight PEMs reside on the back panel to provide 4+4 backup. • In AC mode, two AC power supply frames reside externally, and connect to the power input ports of the PEMs through a rectifier that suits the total power of the integrated chassis.
Heat dissipation system	• Air enters the chassis from the left and exits from the back. • The air intake vent is on the left of the chassis, and the air exhaust vent is on the back of the chassis. • The fans reside on the air exhaust vent. The two fan frames back against each other, each having two fans. The fan frame extracts air from the system for dissipation.	• Air enters the chassis from the front and exits from the back. • The air intake vent is above the front board slot area, and the air exhaust vent is above the rear board slot area. • The fans reside on the air exhaust vent. The two fan frames back against each other. Each fan frame has one fan. The fan frame extracts air from the system for dissipation.	• The two fan frames reside respectively on the upper and lower parts of the chassis. Air enters the chassis from the front and exits from the back. • For the upper fan frame, the air intake vent resides above the front board slot area, and the air exhaust vent resides above the rear board slot area. For the lower fan frame, the air intake vent resides above the rear board slot area, and the air exhaust vent resides above the front board slot area. The upper and lower fan frames function independently. • The board slot area for the SFU resides on the middle part of the device. The area

Component	SeMG9811-X3	SeMG9811-X8	SeMG9811-X16
			intake vent for this slot area is on the left of chassis. To dissipate the SFUs in the two upper slots, the air enters from the left, and goes up on the right to converge with the air from the upper fan frame. To dissipate the SFUs in the two lower slots, the air enters from the left, and goes down on the right to converge with the air from the lower fan frame.

2.1.2 System Configuration

Table 2-5 lists the system configuration of the SeMG9811 Series.

Table 2-5 SeMG9811 Series System Configuration

Item	SeMG9811-X3	SeMG9811-X8	SeMG9811-X16	Remarks
Processing unit of the MPU	Main frequency: 1 GHz	Main frequency: 1.5 GHz	Main frequency: 1.5 GHz	-
BootROM capacity of the MPU	1 MB	8 MB	8 MB	-
SDRAM capacity of the MPU	2 GB	2 GB	2 GB	-
NVRAM capacity of the MPU	512 KB	4 MB	4 MB	-
Compact Flash (CF) card	2 GB	2 GB	2 GB	Two 1 GB CF cards
Number of MPU slots	2	2	2	1:1 backup
Number of SFU slots	-	1	4	• The independent SFUs on the SeMG9811-X8

Item	SeMG9811-X3	SeMG9811-X8	SeMG9811-X16	Remarks
				interwork with the SFU integrated on the SRU to form 2+1 backup for load balancing. • The independent SFUs of the SeMG9811-X16 form 3+1 backup for load balancing.
Number of LPU slots	3	8	16	Each LPU slot can house an SPU. In normal cases, the SPU and the LPU need to be carried out in accordance with the capacity of the closest configuration.
Switching capacity	1.08 Tbit/s	1.44 Tbit/s	2.56 Tbit/s	Bidirectional
Interface capacity	40 Gbit/s	120 Gbit/s	240 Gbit/s	–
Maximum throughput of each SPU	160 Gbit/s			
Maximum port rate of each LPU	100 Gbit/s			

2.1.3 Board

MPU

The MPU on the SeMG9811 performs system control and the learning of route information.

The SeMG9811 MPU uses the 1:1 backup mechanism. When the active MPU is faulty, the standby immediately takes over the work. The backup mechanism ensures the normal running of the system.

SFU

The SFU in the SeMG9811 is in charge of data exchange among boards.

- The SeMG9811-X8 is equipped with three switch network units, two of which together with two main control units are integrated on two MPUs respectively. The third one is placed on an independent SFU.
  - Enables 2+1 load balancing backup in the switching network

  - Four SFUs work simultaneously to share the service data. When one of them is faulty, the service data is automatically balanced to the other two with on service interruption.
- The SeMG9811-X16 equips with four switch network units.
  - Enables 3+1 load balancing backup in the switching network
  - Four SFUs work simultaneously to share the service data. When any SPU is faulty, the service data is automatically balanced to the other three with no service interruption.

SPU

The SPU in the SeMG9811 is a core component which is in charge of processing every security service.

The SPU in the SeMG9811 comes with high-performance multi-core central processing units (CPUs). A service processing card (SPC) can be installed on each SPU.

The SeMG9811 comes with multiple SPUs. The system performance n terms of the throughput and the number of new connections per second will increase in a linear fashion with multiple SPUs support mutual backup. When one SPU is faulty, all its traffic is immediately balanced to other SPUs with no service interruption.

LPU

The SeMG9811 supports LPUF-21 with FPIC for expansion and LPUF-40 with FPIC for expansion.

The LPUF-21 has two slots, each applicable to one FPIC. The entire LPUF-21 provides a maximum bandwidth of 20 Gbit/s.

The LPUF-21 supports the following cards:

- 1-port 10GBase LAN/WAN-XFP optical interface FPIC (one half-width slot)
- 4-port 10GBase LAN/WAN-XFP optical interface FPIC (two half-width slots, convergence)
- 12-port 100Base FX/1000Base-X-SFP optical interface FPI C (one half-width slot)
- 12-port 10Base-T/100Base-TX/1000Base-T electrical interface FPIC (one half-width slot)
- 1-port OC-192c/STM-64c POS-XFP optical interface FPIC (one half-width slot)

The LPUF-40 has two slots, each applicable to one FPIC. The entire LPUF-40 provides a maximum bandwidth of 40 Gbit/s.

The LPUF-40 supports the following cards:

- 2-port 10GBase LAN/WAN-XFP optical interface FPIC (one half-width slot)
- 4-port 10GBase LAN/WAN-XFP optical interface FPIC (one half-width slot, convergence)
- 20-port 100Base-FX/1000Base-X-SFP optical interface FPIC (one slot)

2.1.4 Physical Hardware Architecture

The SeMG9811 consists of the following subsystems:

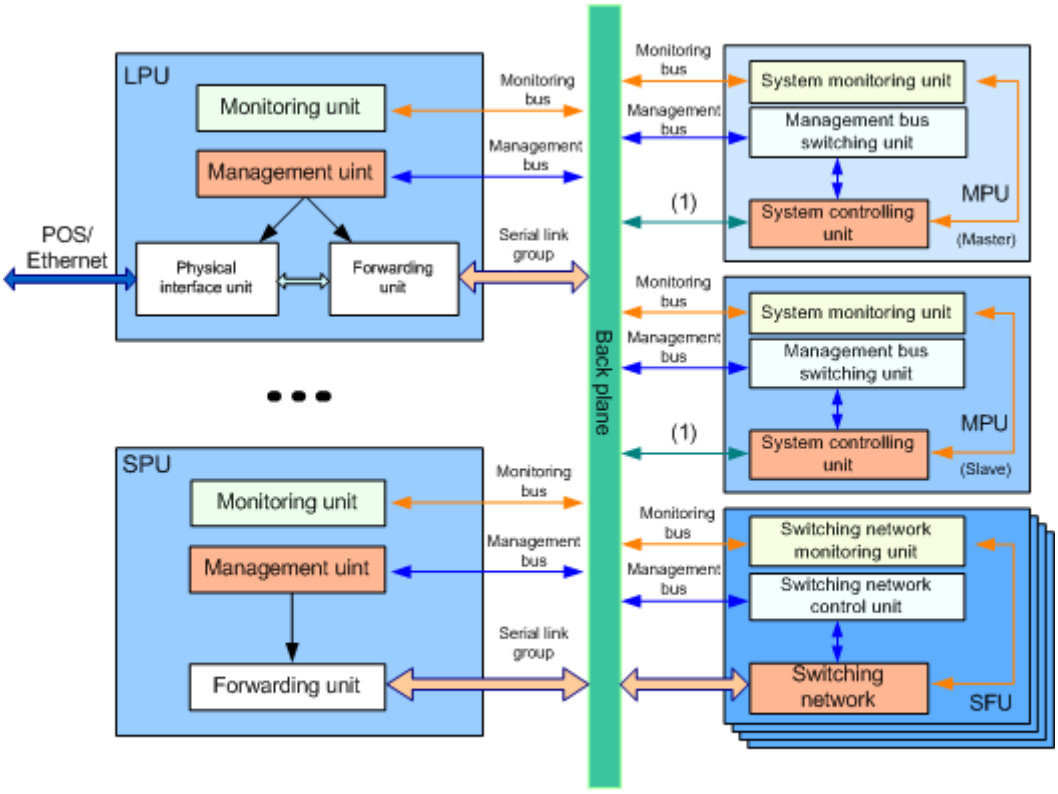
- Power supply system

- Heat dissipation system
- Functional host system
- Network Management (NM) system

Except the NM subsystem, all subsystems are placed in the integrated chassis. Among them, the power supply system works in 1+1 backup mode.

- The NM system, independently deployed on the server, serves for configuring and managing the SeMG9811.
- For details about the functions of the power supply system (in 1+1 backup mode) and the heat dissipation system, see SeMG9811Power Supply and Heat Dissipation Systems
- The functional host subsystem consists of system backplane, MPU, LPU, SPU, and SFU. This subsystem mainly performs data processing function. In addition, the subsystem monitors and manages all devices in the system, including power modules and fan modules. The functional host system can be connected to Network Management System (NMS) through NMS interface. The diagram of functional host is shown in Figure 2-8.

Figure 2-8 Diagram of functional host



NOTE

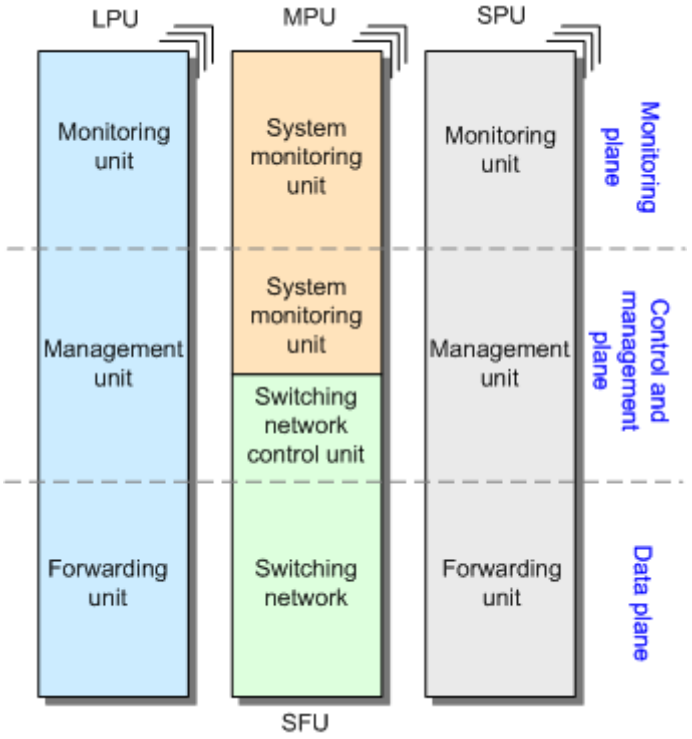
Figure 2-8 applies only to the SeMG9811-X8 and SeMG9811-X16. The SeMG9811-X3 uses Full Mesh Architecture, and it has no switch network unit.

2.1.5 Logical Hardware Architecture

The logical architecture of the SeMG9811 consists of the following planes:

- Data plane
- Control and management plane
- Monitoring plane

Figure 2-9 Diagram of logical hardware architecture



- The data plane is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, processes security services, forwards IPv4/IPv6 packets, performs QoS and scheduling, completes inner high-speed switching, and collects statistics.
- The control and management plane is the core of the entire system. It controls and manages the system. The control and management unit processes protocols and signals, configures and maintains the system status, and reports and controls the system status.
- The monitoring plane monitors the system environment. It detects the voltage, controls power-on and power-off of the system, and monitors the temperature and controls the fan. In this manner, the security and stability of the system are ensured. It can isolate the fault promptly in the case of a unit failure to guarantee the operation of other parts.

The SeMG9811 is based on the dedicated modular security software platform, and implements the separation of the forwarding and control functions. The control function of the SeMG9811 is based on the MPU; the forwarding function is based on the LPU and SPUA.

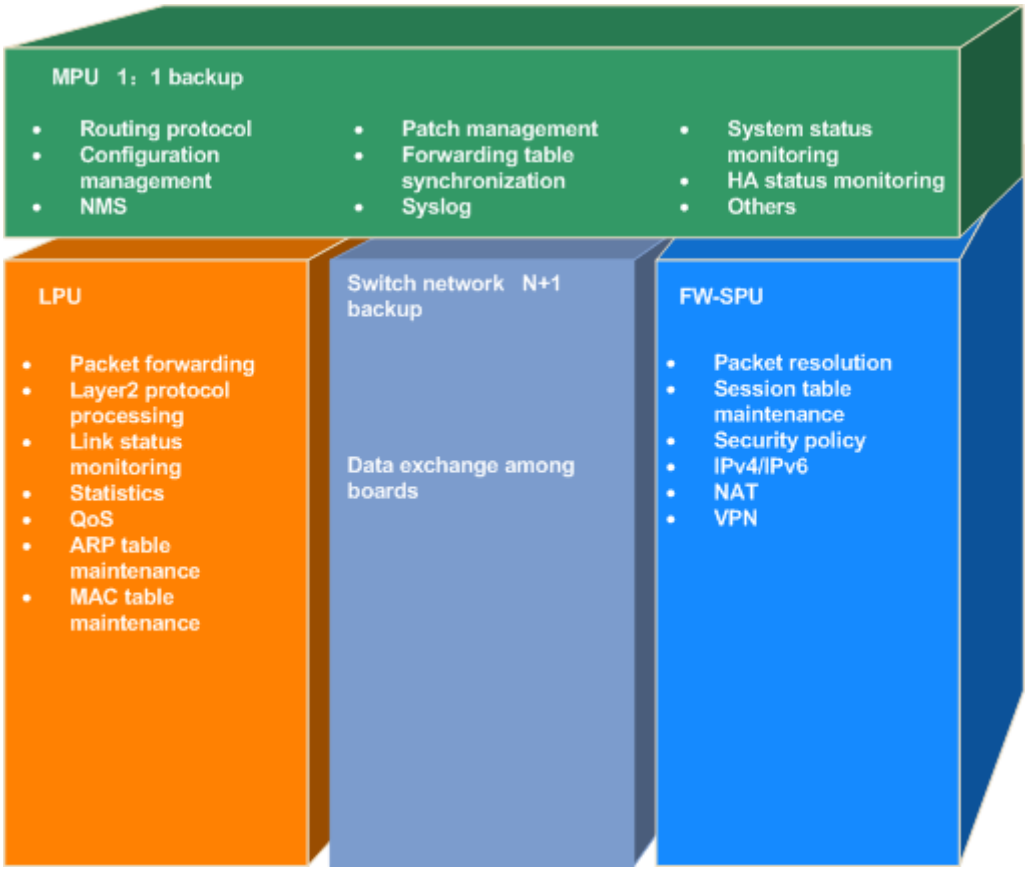
2.2 Software Structure

2.2.1 Logical Software Architecture

The SeMG9811 adopts the flexible and sophisticated versatile routing platform (VRP). Based on the component technology, the VRP supports the distributed architecture and improves security features and reliability.

Figure 2-10 shows the logical diagram of the software architecture.

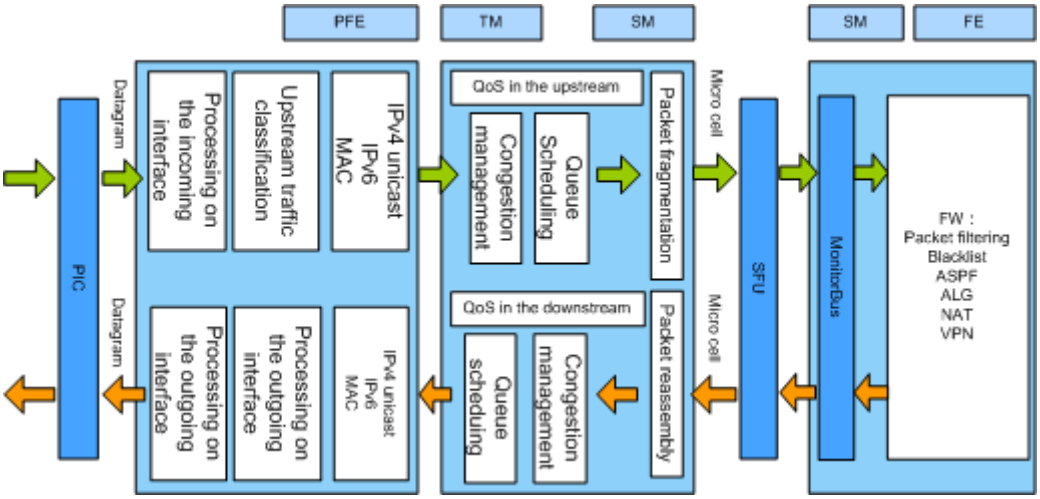
Figure 2-10 Diagram of the logical software architecture



2.2.2 Data Forwarding Process

SeMG9811 shows the flowchart of forwarding data.

Figure 2-11 Flowchart of forwarding data



According to data direction, data forwarding can be divided into the following three processes:

- Upstream process

  A packet is encapsulated in a frame on the Physical Interface Card (PIC) and then sent to the Packet Forwarding Engine (PFE). On the incoming interface, the packet is decapsulated and the packet type is identified. Then, traffic is classified according to the configurations on the incoming interface. Subsequently, scheduling priorities are generated and added to the packet. Then the packet is sent to the Traffic Manager (TM) where the scheduling for Quality of Service (QoS) is completed.

- Process in the SPU

  After the upstream process in the LPU, the SFU sends the packet to the forwarding engine in the SPU. Then the forwarding engine searches the session table. If the search succeeds, the packet is sent for security process according to the matched session entries. If the search fails, the packet is the first packet in the session. The forwarding engine searches the Forwarding Information BASE (FIB) according to the destination IP address of the packet. By searching the FIB, the forwarding engine obtains the outbound interface and the next hop of the packet, and then sends the packet for security services, such as the firewall.

- Downstream process

  After the process in the SPU is complete, the packet is sent through the SFU to the downstream LPU. In the LPU, the packet is processed for downstream QoS and downstream traffic classification. Finally, according to the configurations on the outgoing interface, the packet is encapsulated with the new Layer-2 header, and is then sent to the PIC.

3 Functions

About This Chapter

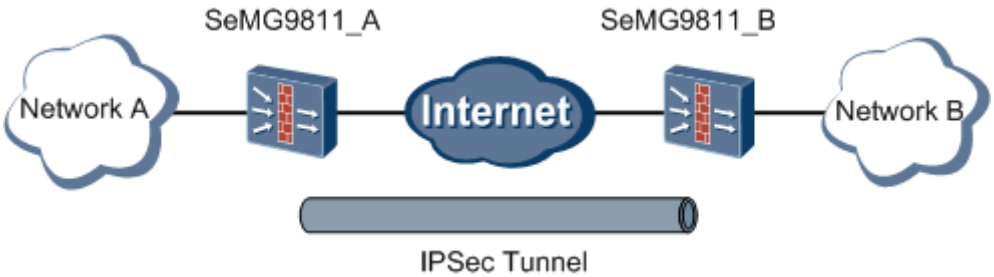
3.1 Virtual Private Network (VPN)

IPSec

As shown in Figure 3-1, the SeMG9811 provides the IP Security (IPSec) mechanism to perform the following for both parties of communications:

- Access control
- Connectionless integrity
- Data source authentication
- Anti replay and encryption
- Encryption of categorized data streams

Figure 3-1 IPSec tunnel



The SeMG9811 also supports the IPSec tunnel negotiation by using the IKE V2 protocol. The IKE V2 protocol reserves the basic functions of IKE and overcomes the problems found during IKE study. Moreover, for considerations of simplicity, efficiency, security, and robustness, relevant IKE documents are replaced by RFC 5996. By minimizing core functions

and default password algorithms, IKE V2 greatly improves the interoperation capability among different IPSec VPNs.

Compared with IKE, IKE V2 has the following advantages:

- After four messages, one IKE SA and a pair of IPSec SAs can be created through negotiation. Thus, the negotiation efficiency is improved.
- Data structures that are difficult to understand and likely to be confusing are deleted, including DOI, SIT and domain identifier.
- Many cryptographic loopholes are closed, and thus security is improved.
- IKE V2 can choose payloads of specific traffic to protect. In this way, IKE V2 takes over certain functions of the former ID payload and becomes more flexible.
- IKE V2 supports EAP authentication, and thus the authentication is improved in flexibility and expansibility.

Through IPSec, the SeMG9811 provides secure transmission tunnels of high reliability for users. In addition, the SeMG9811 supports the combination of the IPSec, L2TP, and GRE to construct multiple VPN applications as follows:

- L2TP over IPSec VPN
- GRE over IPSec VPN
- IPSec Dual-System Hot Backup

Digital Certificate

A certificate, short for a digital certificate, ensures the mutual trust between communications parties, and guarantees the security, integrity, and non-repudiation of information during transmission. The certificate file, usually issued by a third party, that is, a digital Certificate Authentication (CA) center, contains the device information, public key, and signature of the issuer.

Public Key Infrastructure (PKI) is a system that employs the public key technology and digital certificate to secure system information and authenticate the identity of the digital certificate owner. As the collection of software and hardware systems and security policies, PKI provides a set of security mechanisms. PKI provides a secure network environment where users can conveniently use encryption and digital signature technologies in various application scenarios

The SeMG9811 provides a PKI-based certificate authentication mechanism. The certificate mechanism can provide a centralized key management mechanism for the IPSec network and enhances the expansibility of the entire IPSec network. On the IPSec network that employs the certificate mechanism, every device has a certificate issued by the CA. When two devices communicate with each other, they only need to exchange certificates to authenticate the other device , and then get the public key of the other side from the certificate. In this case, when a new device needs to communicate with other devices, it only needs to apply for a certificate rather than modify the configurations of other devices.

SeMG9811 supports three modes of certificate application from CA server: SCEP online application, CMPv2 online application and offline application. And it also sopports the certificate auto-updating function, which gets rid of the service interruption situation result from forgeting to manually update certificate.

SeMG9811 supports the certificate validity check through OCSP. Compared with the CRL, OCSP provides more timely information regarding the revocation status of certificates

SeMG9811 also supports the imports and exports of RSA Key Pairs, according to the PEM and PKCS12 standards. In that, RSA based identify information and trust relationship can be transferred between different devices and even different systems. The ease in transferring and sharing the in formation structure reduces the occurrence of relevant problems and risks.

L2TP

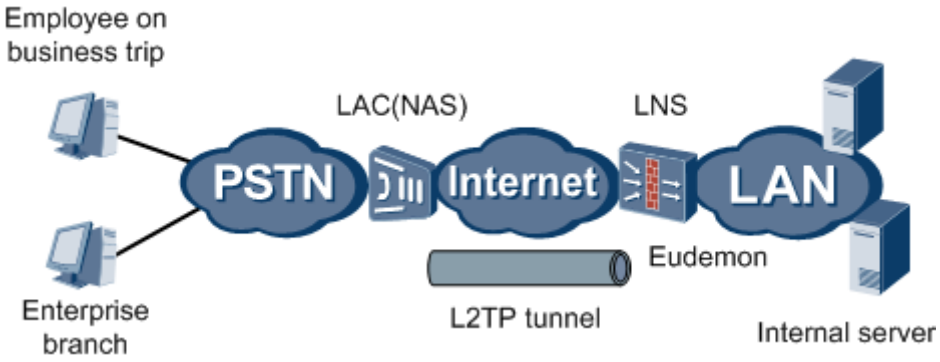
The SeMG9811 supports constructing a virtual private dial network (VPDN) by using the Layer Two Tunneling Protocol (L2TP) and a VPN by using the access network and the dial function of public networks such as ISDN and PSTN. This provides access services for enterprises, small ISPs, and mobile business personnel.

The SeMG9811 can be used as an L2TP network server (LNS) in two typical tunnel modes as follows:

- NAS-Initialized Mode

  As shown in Figure 3-2, the remote system connects to the LAC through the PSTN or the ISDN. The LAC sends a request to the LNS for setting up a tunnel connection through the Internet. Dial user addresses are allocated by the LNS. The agent on the LAC or LNS can perform authentication on the remote user.

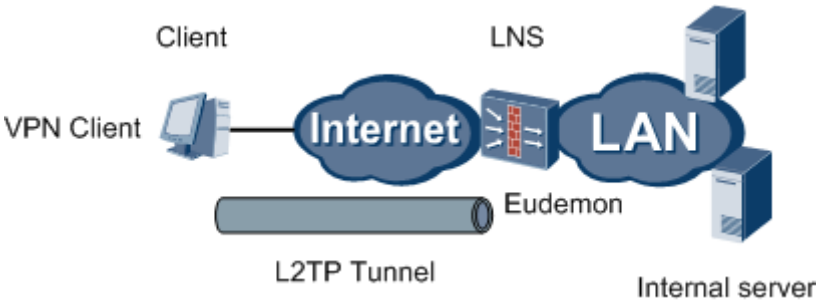
Figure 3-2 L2TP tunnel in the NAS-initialized mode



- Client-Initialized Mode

  As shown in Figure 3-3, the LAC client can directly send a request to the LNS for setting up a tunnel rather than through a single LAC device. According to the user name and password, the LNS authenticates this received request and allocates a private IP address to the LAC user.

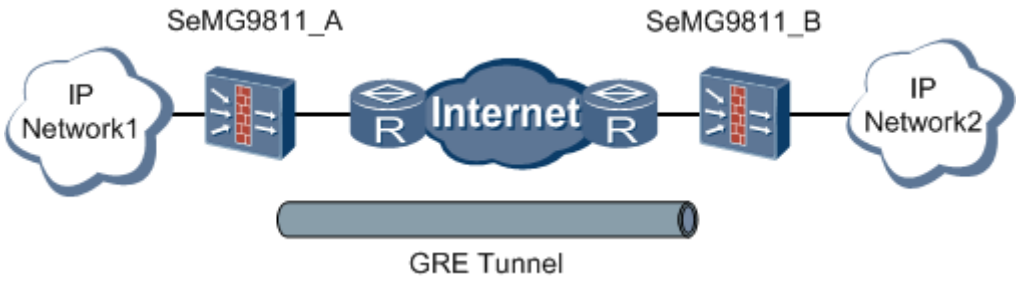
Figure 3-3 L2TP tunnel in the client-initialized mode



GRE

As shown in Figure 3-4, the SeMG9811 supports encapsulating certain network layer protocol packets by using the Generic Routing Encapsulation (GRE) protocol. In this manner, the encapsulated packets are transmitted in another network layer protocol.

Figure 3-4 GRE tunnel



3.2 Security Mechanism

Security Policy

SeMG9811 supports the IPv4/IPv6 security policy. The security policy checks the device traffic, and allows only the legitimate traffic to pass. The major applications are as follows:

- Controlling the cross-device network access

  Such as controlling the rights to access extranets from intranets and the mutual access rights between the subnetworks of different security levels on intranets.
- Controlling the device access

  Such as controlling IP addresses for Telnet or Web login and the mutual access between NMSs or NTP servers and devices.

Application Specific Packet Filter

Application Specific Packet Filter (ASPF) is the packet filter based on the application layer, that is, the status-based packet filter. It cooperates with the common static firewall to carry out

the security policy of internal network. ASPF can detect the application layer protocol session to prevent the unmatched data packet from passing the firewall.

Malicious Host Blacklisting and Filtering

The SeMG9811 can blacklist the source IP addresses of suspicious packets. The system can discard the packets of blacklist users to effectively avoid attacks by malicious hosts.

The SeMG9811 provides the following blacklist maintenance modes:

- Manually adding entries to the blacklist to implement proactive defense.
- Automatically adding entries to the blacklist with the help of attack defense to implement intelligent defense.

In addition, by applying ACL rules in the blacklist, the SeMG9811 can filter the packets that are denied by the ACL rules, but allow the permitted packets to pass through.

Varied Authentication Modes

The SeMG9811 provides authentication and authorization schemes and can work with the accounting server and the record server to manage the network access security in a centralized manner.

The SeMG9811 provides the following modes of authentication:

- Local authentication
- Standard Remote Authentication Dial-In User Service (RADIUS)
- Huawei RADIUS+ authentication
- Huawei Terminal Access Controller Access Control System (HWTACACS) authentication

The SeMG9811 can also provide plain text and Message-Digest Algorithm 5 (MD5), and other means of authentication. It can also support local user management. The SeMG9811 can authenticate the validity of users, and authorize legal users while deny illegal users

Robust GTP Protection Function

The SeMG9811 supports the GTP solution, which can be used to interwork with GPRS Support Node (GSN) products. This solution secures the data transmitted on the General Packet Radio Service (GPRS) network. On a GPRS network, the SeMG9811 can be deployed on Gn, Gp, and Gi interfaces to realize the following applications.

- When working on the Gn interface, the SeMG9811 filters out malicious packets, thus securing NEs on the same PLMN.
- When the SeMG9811 works on the Gp interface, and a PLMN connects to other PLMNs, the SeMG9811 filters out malicious packets from other PLMNs, thus securing NEs on the PLMN.
- When the SeMG9811 works on the Gi interface, and a PLMN connects to an external IP network, the SeMG9811 filters out malicious packets from the external IP network, thus securing NEs on the PLMN.
- The SeMG9811 defends against GTP charging overflow attacks.

4 Operation and Maintenance

About This Chapter

4.1 Maintenance Features and Functions

4.1.1 System Configuration Mode

The SeMG9811 provides the following three configuration modes:

- Command line configuration
- Web configuration
- NMS configuration

The command line configuration supports:

- Local configuration through the Console port
- Remote configuration through the AUX port with a Modem
- Remote configuration through Telnet or SSH
- Configuration management through Web pages

The NMS configuration supports Huawei NMS that is based on SNMP.

4.1.2 System Management and Maintenance

The SeMG9811 provides the following system management and maintenance functions:

- Board-in-position detection, hot-swap detection, board reset, control over running and debugging indicators, fan monitoring, power monitoring, active/standby switchover control, and version query

- Local and remote software upgrading and data loading, version rollback, backup, storage, and removal
- Hierarchical user authority management, operation log management, online help and comment for command line
- Multi-user operation
- Collection of multi-layer information, including interface information, Layer 2 information, and Layer 3 information
- Hierarchical management, alarm classification and alarm filtering

4.1.3 System Service and Status Tracking

The SeMG9811 can track the system service and status as follows:

- Monitor the migration of state machines related to the route protocol
- Monitor the migration of state machines related to VPN
- Monitor the types of protocol packets that are sent by the NP and display details about the packets with the debugging function
- Monitor and count abnormal packets
- Display notification when abnormality handling processing takes effect
- Monitor and collect statistics on the resources that are occupied by each system feature

4.1.4 System Test and Diagnosis

The SeMG9811 provides debugging for services. It can in service record information on key events, packet processing, packet resolution, and state switchover during the period specified by the customer.

The SeMG9811 provides the trace function on system operation. It can in service record the key events such as service switchover, service interruption, queue read-and-write, and system abnormity.

The CPU usage of the MPU, the SPU and the LPU can be queried in real time.

The debugging and trace messages can be classified into different levels. According to the configuration, the messages with different levels can be redirected to various output destinations such as the console display, Syslog server, and SNMP Trap trigger alarm.

4.1.5 Online Upgrade

The SeMG9811 supports online software upgrade. If the upgraded software is faulty, you can restart the system and switch to the original software version. Meanwhile, the SeMG9811 also supports online software patching, that is, you only need to upgrade certain necessary features. If the patched software is faulty, you can switch to the original software version.

Board program upgrade downloads programs online. During the upgrade, you need to reset only the board to be upgraded. For upgrading LPU programs, you can upgrade multiple concurrent LUP programs at the same time. After that, original programs are backed up on the device. Online program downloading does not affect the normal running of the system.

4.1.6 Miscellaneous

The SeMG9811 provides the following additional features:

- Hierarchical commands, ensuring that the unauthorized users cannot access the device

- Online help available if you type a "?"
- Various debugging information for troubleshooting
- DosKey-like function for running a historical command
- Fuzzy search for command lines, for example, you can enter the non-conflicting key words "**disp**" for the **display** command

4.2 Network Management

The SeMG9811 uses the system for network management. This network management system supports the SNMP(V1/V2c/V3) protocol and the client/server architecture and can run on multiple operating systems independently. The supported operating systems include Windows NT/2000 and UNIX (SUN, HP, and IBM).

4.3 WEB Configuration and Management

The SeMG9811 provides the Web Graphic User Interface (GUI)-based management interface, and user-friendly configuration and management interfaces. On GUIs, you can configure features such as security zones, ACLs, NAT, ASPF, attack defense, blacklists, and view various statistics parameters.

The Web browser communicates with the SeMG9811 over the HTTP Security (HTTPS) protocol. HTTPS employs the SSL security encryption mechanism to establish an encrypted channel between the client and server, ensuring that data is protected from being intercepted. The encryption function ensures the security of user information.

4.4 Security

Data System Security

The system takes the backup and recovery policy to ensure data security. Save the data (the system software, configuration file, log file, and database data) at a certain time spot to other storage devices. When the system becomes faulty, import the backup data to the system to restore the normal operation of the system.

Operation and Maintenance Security

The SeMG9811 provides a security mechanism to ensure the security of the operation and maintenance from multiple dimensions such as the device management, application, and log.

- Hierarchical-based management

  The SeMG9811 supports hierarchical-based management for administrators. The available permissions vary with the administrators. To log in to the system, the administrator must provide a correct user name and password. After successfully logging in to the system, the administrator can perform operations with the assigned permissions.
- Access channel control

  The SeMG9811 provides a dedicated out-of-band management port instead of using the service ports for management.

The device supports the ACL and policy mechanism to ensure the security of access control over the device.

The communication between the SeMG9811 and the third-party NMS is implemented using security protocols. You can enable the services of the security protocols, such as HTTPS. You can disable the services of insecure protocols, such as Telnet.

- Security logging

  The system can log important operations such as login and logout for future audit.

- Protection mechanism for the sensitive user information

  The system authenticates users through password and identity authentication, and protects the sensitive user information using the advanced encryption algorithm. Every user is allocated with a password for the verification before the system provides services for the user, protecting the security of user information. When the administrator logs in to the device, the system forces the administrator to change the default password to enhance security management.

- Anti-brute-force mechanism

  Some unauthorized users attempts to hack into the system by conjecturing the administrator's user name and password. The SeMG9811 supports the maximum number of login attempts. Once the number of login attempts exceed the specified threshold, the system adds the user's IP address to the isolated IP address list and blocks the user from accessing the device within the lockout period.