



HUAWEI NIP6000

V500R001C80

Product Description

Issue 01

Date 2017-11-03

Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.

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

Trademarks and Permissions



HUAWEI 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://e.huawei.com>

About This Document

Related Version

The documents are applicable to the following product versions:

| Product Name | Version |
|--|-------------|
| The NIP6300/6600 series have the following models: <ul style="list-style-type: none">● NIP6300<ul style="list-style-type: none">- NIP6320- NIP6330● NIP6600<ul style="list-style-type: none">- NIP6610- NIP6620- NIP6650- NIP6680 | V500R001C30 |

Intended Audience

This document describes the product positioning and highlights, typical networking and application scenarios, software and hardware architecture, functions and features, standards, and technical specifications of the NIP6000. This document helps you to quickly familiarize yourself with the product.

This document is intended for administrators who configure and manage NIP6000. The administrators must have good Ethernet knowledge and network management experience.






Feature Conventions

Antivirus and IPS support packet capture to analyze data packets for viruses or intrusions. However, the packet capture process may involve the collection of user's communication content. The device provides dedicated audit administrators to obtain captured packets. Other administrators do not have such permissions. Please keep the audit administrator account safe and clear the packet capture history in time.

Huawei alone is unable to collect or save the content of users' communications. It is suggested that you activate the user data-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

| Symbol | Description |
|---|---|
|  DANGER | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|  WARNING | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|  CAUTION | Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. |
|  NOTICE | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury. |
|  NOTE | Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration. |

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 01 (2016-08-19)

Initial commercial release.

Contents

| | |
|---|-----------|
| About This Document..... | ii |
| 1 Product Positioning and Features..... | 1 |
| 1.1 Product Positioning..... | 1 |
| 1.2 Highlights..... | 1 |
| 2 Product Architecture..... | 4 |
| 2.1 System Components..... | 4 |
| 2.2 Hardware Architecture..... | 5 |
| 2.2.1 NIP6320..... | 5 |
| 2.2.2 NIP6330..... | 7 |
| 2.2.3 NIP6610..... | 9 |
| 2.2.4 NIP6620..... | 12 |
| 2.2.5 NIP6650..... | 14 |
| 2.2.6 NIP6680..... | 16 |
| 2.2.7 NIP6830..... | 20 |
| 2.2.8 NIP6860..... | 21 |
| 2.3 Software Architecture..... | 23 |
| 3 Product Functions..... | 25 |
| 3.1 Product Function List..... | 25 |
| 3.2 Virtual Patch..... | 28 |
| 3.3 Web Application Protection..... | 28 |
| 3.4 Security Posture Awareness..... | 29 |
| 3.5 SSL Traffic Detection..... | 30 |
| 3.6 Antivirus..... | 30 |
| 3.7 Application Identification and Control..... | 31 |
| 3.8 URL Filtering..... | 32 |
| 3.9 Abnormal Traffic Prevention..... | 32 |
| 3.10 Logs and Reports..... | 33 |
| 3.11 Availability..... | 35 |
| 4 Application Scenarios..... | 37 |
| 4.1 Internet Border..... | 37 |
| 4.2 IDC/Server Upstream..... | 38 |
| 4.3 Network Border..... | 39 |

| | |
|---|-----------|
| 4.4 Out-of-Path Detection..... | 40 |
| 5 Operation and Maintenance..... | 42 |
| 5.1 Configuration and Management..... | 42 |
| 5.2 System Maintenance..... | 42 |
| 5.3 Security..... | 43 |
| 6 Technical Specifications..... | 45 |
| 6.1 Hardware Specifications..... | 45 |
| 6.1.1 NIP6320..... | 45 |
| 6.1.2 NIP6330..... | 47 |
| 6.1.3 NIP6610..... | 50 |
| 6.1.4 NIP6620..... | 52 |
| 6.1.5 NIP6650..... | 55 |
| 6.1.6 NIP6680..... | 58 |
| 6.1.7 NIP6830..... | 60 |
| 6.1.8 NIP6860..... | 63 |
| 6.2 Standards and Protocols..... | 65 |

1 Product Positioning and Features

1.1 Product Positioning

The NIP6000 series is an intrusion prevention product developed by Huawei Technologies Co., Ltd. (Huawei for short). It provides application and traffic security for enterprise networks, Internet Data Centers (IDCs), and campus networks.

The NIP6000 extends the functions of traditional intrusion prevention products to provide better application and service security. Details are as follows:

- Standard intrusion prevention functions
The NIP6000 provides vulnerability- and threat-facing signature databases for detecting and blocking attacks.
- Application awareness and application-layer threat prevention
The NIP6000 defends against application-specific attacks and is capable of identifying, managing, and controlling network applications. Administrators can manage and control applications by configuring security and traffic policies in addition to port-, protocol-, and service-based policies.
- Context awareness
Based on asset information (including asset types, asset values, and operating systems), the NIP6000 evaluates risks of attack events, marks attack events with risk levels, and provides event results for administrators.
Administrators can configure intrusion prevention policies based on asset information and applications to defend against specific attacks.
- Unknown threat detection
The NIP6000 interworks with a sandbox to detect new network attacks, such as APT and zero-day attacks.

1.2 Highlights

Fast Signature Update for Prompt Vulnerability Detection

New types of attacks incessantly emerge and evolve, bringing about massive threats. Whenever it detects a new vulnerability, Huawei releases the corresponding signature as soon as possible to defend against attacks that exploit this vulnerability.

Huawei's dedicated security team closely traces the security bulletins of major security organizations and software vendors, analyzes and verifies the threats, and generates signature databases that protect software systems, including operating systems, application programs, and databases, in compliance with Common Vulnerabilities and Exposures (CVE) requirements. In addition, Huawei uses worldwide honeynets to capture the latest attacks, worms, and Trojan horses in real time, facilitating the generation of signatures and the identification of threat trends. With these capabilities, Huawei is able to release the signature of a virus that exploits a newly identified vulnerability and promptly update the signature databases and inspection engine.

Plug-and-Play and Flexible Deployment

All service interfaces on a delivered NIP6000 work at Layer 2, and every two interfaces form an interface pair. In an interface pair, traffic enters the NIP6000 through one interface and leaves through the other. In in-path mode, an interface pair of the NIP6000 connects to the network link in series, offering protection without changing the existing network topology.

A default intrusion prevention policy is applied to each interface on the NIP6000 to reduce configuration difficulties, achieving plug-and-play.

Each predefined interface pair on the NIP6000 can be divided into two independent interfaces to meet diversified network requirements. The independent interfaces may be used in out-of-path intrusion detection, out-of-path intrusion prevention, and route deployment scenarios.

New Hardware and Software Architecture, Providing Industry-Leading Performance

In terms of hardware, the NIP6000 uses a dedicated multi-core and multi-CPU platform, which greatly improves detection performance. In terms of the software, the NIP6000 uses a new intelligent awareness engine (IAE) for threat detection, which enables multi-level protection and concurrent processing and improves threat detection efficiency.

The NIP6000 provides 100 Mbit/s, 1000 Mbit/s, and 10000 Mbit/s performance to meet different requirements.

Interworking with the Sandbox to Detect APT Attacks

The Advanced Persistent Threat (APT) is a new attack mode that persistently attacks a specific target or system. Traditional security products defend against attacks based only on known viruses and vulnerabilities. APT attackers may exploit 0-day vulnerabilities to launch attacks, which can easily pass through the defense system.

The most effective method for APT attack defense is the sandbox technology, which creates an isolated threat inspection environment. Files are delivered to the sandbox for threat analysis. If the sandbox detects malicious files, it instructs the NIP6000 to block the files.

Dynamic Context Awareness for Intelligent Policy Tuning and Risk Evaluation

The NIP6000 provides security posture awareness to dynamically detect network environments, reducing difficulties in policy tuning and attack event evaluation for enterprises with complicated IT environments and numerous application types.

- The NIP6000 identifies attack events of high risk levels based on network environments and filters out attack events that may cause false positives, so that administrators can focus on critical attack events.

- Administrators can tune intrusion prevention policies based on the conditions of protected IT assets (including the asset type, asset value, and operating system) for better attack defense effects.

Strong Antivirus Functions That Stop Viruses Spreading

The NIP6000 rapidly and accurately scans and removes viruses in transferred files and effectively defends against multiple virus detection-escaping mechanisms, implementing virus-specific attack defense.

Huawei has a dedicated virus analysis team that constantly traces the latest viruses, ensuring the timely update of the signature databases.

Powerful Application-Layer Anti-DDoS Capability for Normal Service Operating

The NIP6000 prevents DDoS attacks at network, transport, and application layers to protect legitimate traffic and services.

Historically, SYN floods were the prevalent traffic attacks. Nowadays, UDP and ICMP floods are the most common heavy-traffic attacks, with most DDoS attacks occurring at the application layer. DDoS attacks generally target web and DNS services, especially DNS flood attacks, which cause severe damage.

The NIP6000 automatically learns traffic models and implements layer-by-layer traffic detection and cleaning techniques to prevent application-layer DDoS attacks, such as DNS flood, HTTP flood, and HTTPS flood.

Leading Quantity of Identified Applications for Refined Application Management

After an application identification signature database is loaded, the NIP6000 identifies more than 6000 web applications, covering mainstream application protocols. In addition, the NIP6000 supports popular encryption P2P protocols, Web 2.0 applications, mobile applications, and micro applications as well as user-defined applications.

Based on identified application types, the NIP6000 performs refined application access control and application bandwidth management.

2 Product Architecture

2.1 System Components

The NIP6000 works with neighboring components to form a complete intrusion prevention system. **Figure 2-1** shows system components, and **Table 2-1** lists the function description of each component.

Figure 2-1 System components

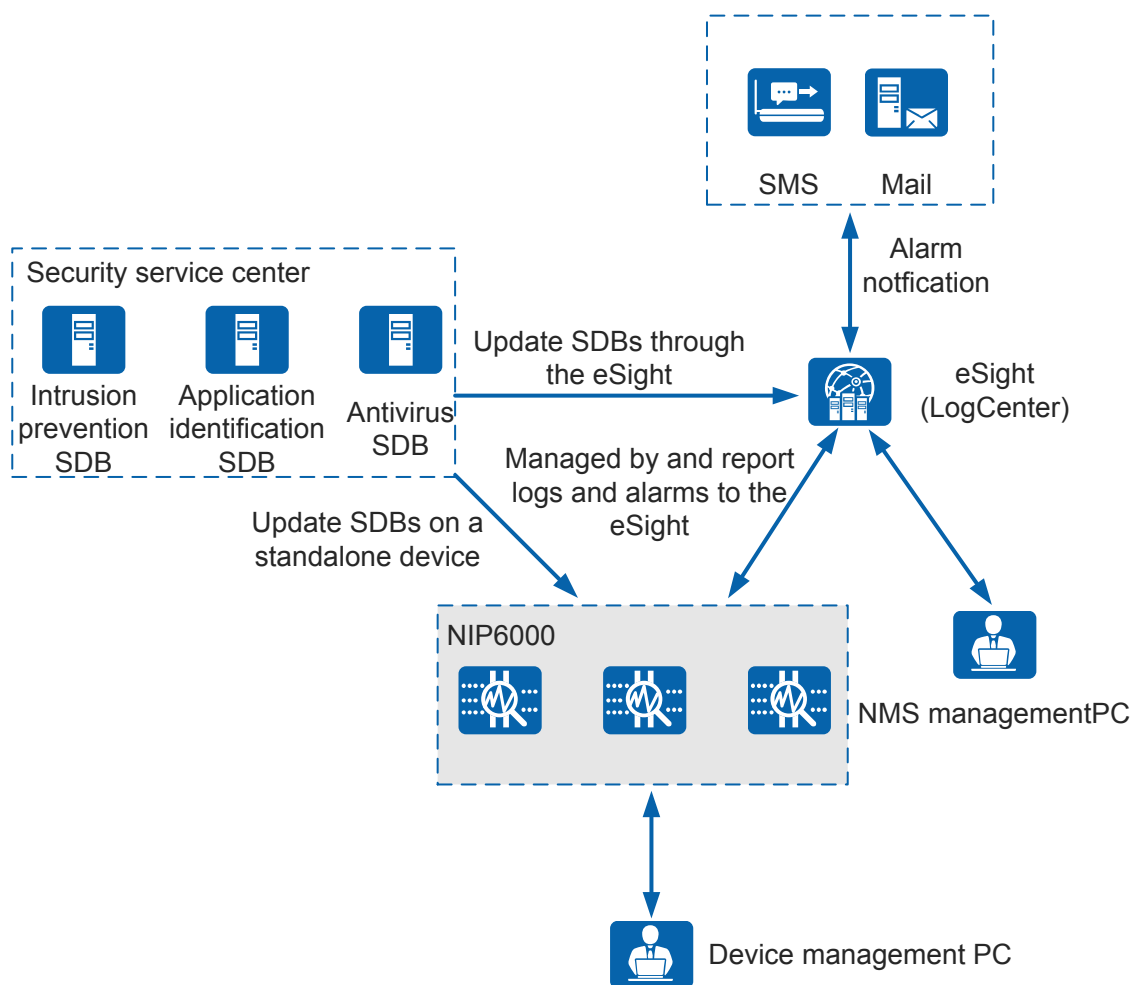


Table 2-1 Function description of system components

| Component | Description |
|----------------------------------|---|
| NIP6000 | The NIP6000 provides intrusion prevention, antivirus, application identification, and DDoS attack defense functions. |
| eSight (including the LogCenter) | The matching network management system manages multiple NIP6000s in a centralized manner. It monitors the operating status, manages alarms, and updates the signature databases of the NIP6000s. If the eSight has the LogCenter component integrated, it receives logs and generates reports. Alternatively, the LogCenter can be deployed as an independent product to receive logs. |
| Security service center | The security service center provides the latest intrusion prevention, application identification, and antivirus signature databases. It updates these signature databases, so that devices obtain the latest security protection capabilities. The signature databases on a NIP6000 can be updated locally through the built-in web system or remotely updated on the eSight. |
| Alarm notification | After detecting an attack, a NIP sends an alarm recording this attack event to the eSight. The eSight then notifies the maintenance personnel through a mail or short message. |
| Management PC | Both the NIP and eSight have web UIs. A management PC can be used to configure and manage NIPs in a standalone or centralized manner. |

2.2 Hardware Architecture

2.2.1 NIP6320

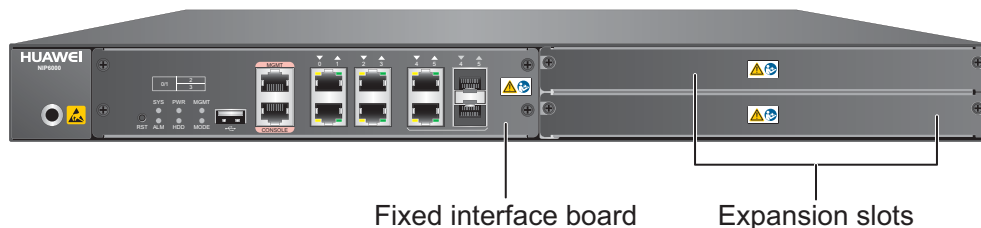
The NIP6320 uses an integrated chassis that contains the fixed interface board, power module, and fan module. You can also add some optional modules, such as hard disk, additional power module, and expansion cards, to improve system reliability and add more ports.

Appearance

Figure 2-2 illustrates the appearance of the NIP6320.

Figure 2-2 Appearance of NIP6320

Front view



Rear view

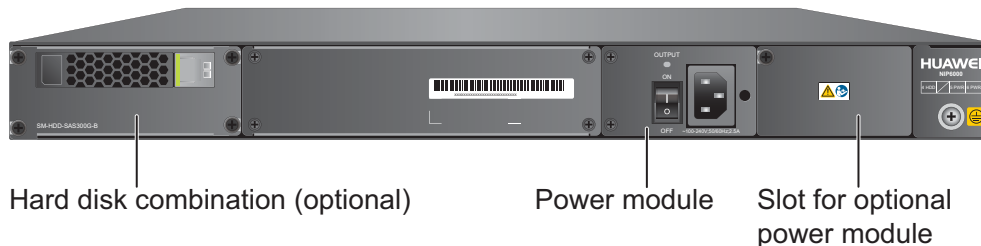


Table 2-2 describes the functions of the NIP6320 components.

Table 2-2 Functions of the NIP6610 components

| Name | Description |
|-----------------------|--|
| Fixed interface board | <p>The fixed interface board is the core component for system control and management and provides the management, forwarding, and control planes. The interface board also has an intelligent awareness engine.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |

| Name | Description |
|-----------------------|--|
| Expansion slot | Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-3 lists the supported expansion cards. |
| Power module | Build-in 150 W power module is provided by default, but you can optionally add a 170 W power module for 1+1 power redundancy. If two power modules are used and PWR6 power module fails, the other can support the entire system so that you can replace the PWR6 faulty power module without interrupting device operation. |
| Hard disk combination | Hard disks are used to store logs and reports. The device supports optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. |

Ports

The fixed interface board provides the following ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 1 USB 2.0 ports
- 2 GE Combo ports
- 4 10/100/1000M autosensing Ethernet electrical ports

[Table 2-3](#) lists the supported types of expansion cards.

Table 2-3 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

NOTE

WSIC: Wide Service Interface Card

2.2.2 NIP6330

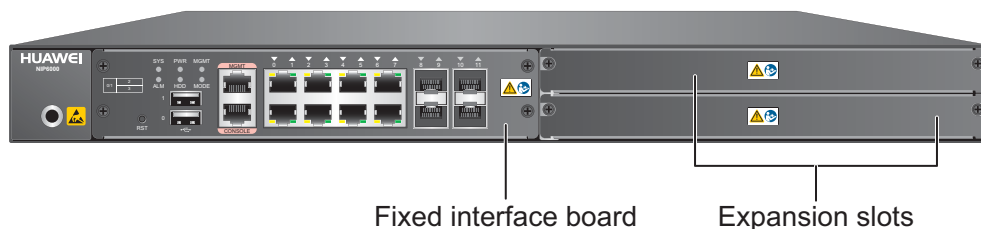
The NIP6330 uses an integrated chassis that contains the fixed interface board, power module, and fan module. You can also add some optional modules, such as hard disk, additional power module, and expansion cards, to improve system reliability and add more ports.

Appearance

Figure 2-3 illustrates the appearance of the NIP6330.

Figure 2-3 NIP6330 appearance

Front view



Rear view

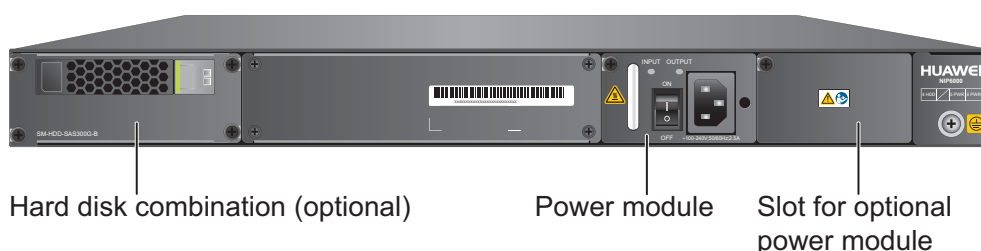


Table 2-4 describes the functions of the NIP6330 components.

Table 2-4 Functions of NIP6330 components

| Name | Description |
|-----------------------|--|
| Fixed interface board | <p>The fixed interface board is the core component for system control and management and provides the management, forwarding, and control planes. The interface board also has an intelligent awareness engine.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |

| Name | Description |
|-----------------------|--|
| Expansion slot | Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-5 lists the supported expansion cards. |
| Power module | By default, an AC power module is provided. Two power modules are supported to provide 1+1 power redundancy. If one power module fails, the other can support the entire system so that you can replace the faulty power module without interrupting device operation. |
| Hard disk combination | Hard disks are used to store logs and reports. The device supports optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. |

Ports

The fixed interface board provides the following ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 2 USB 2.0 ports
- 4 GE optical ports
- 8 10/100/1000M autosensing Ethernet electrical ports

[Table 2-5](#) lists the supported types of expansion cards.

Table 2-5 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

NOTE

WSIC: Wide Service Interface Card.

2.2.3 NIP6610

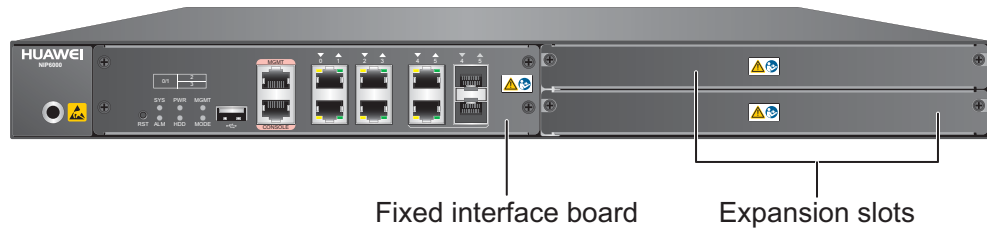
The NIP6610 uses an integrated chassis that contains the fixed interface board, power module, and fan module. You can also add some optional modules, such as hard disk, additional power module, and expansion cards, to improve system reliability and add more ports.

Appearance

Figure 2-4 illustrates the appearance of the NIP6610.

Figure 2-4 Appearance of NIP6610

Front view



Rear view

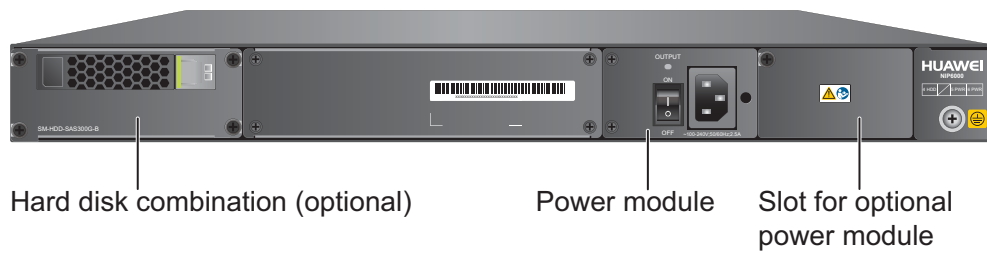


Table 2-6 describes the functions of the NIP6610 components.

Table 2-6 Functions of the NIP6610 components

| Name | Description |
|-----------------------|--|
| Fixed interface board | <p>The fixed interface board is the core component for system control and management and provides the management, forwarding, and control planes. The interface board also has an intelligent awareness engine.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |
| Expansion slot | Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-7 lists the supported expansion cards. |
| Power module | Build-in 150 W power module is provided by default, but you can optionally add a 170 W power module for 1+1 power redundancy. If two power modules are used and PWR6 power module fails, the other can support the entire system so that you can replace the PWR6 faulty power module without interrupting device operation. |
| Hard disk combination | Hard disks are used to store logs and reports. The device supports optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. |

Ports

The fixed interface board provides the following ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 1 USB 2.0 ports
- 2 GE Combo ports
- 4 10/100/1000M autosensing Ethernet electrical ports

[Table 2-7](#) lists the supported types of expansion cards.

Table 2-7 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

 **NOTE**

WSIC: Wide Service Interface Card

2.2.4 NIP6620

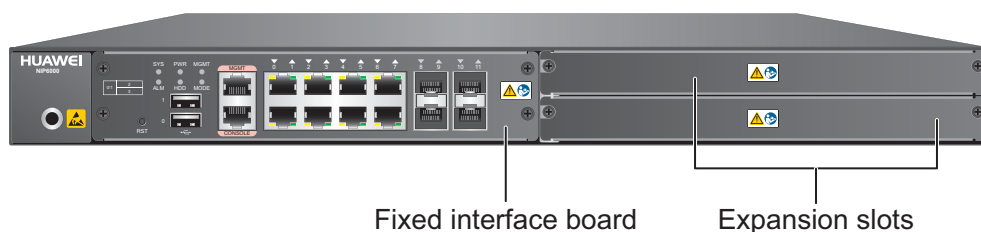
The NIP6620 uses an integrated chassis that contains the fixed interface board, power module, and fan module. You can also add some optional modules, such as hard disk, additional power module, and expansion cards, to improve system reliability and add more ports.

Appearance

Figure 2-5 illustrates the appearance of the NIP6620.

Figure 2-5 Appearance of NIP6620

Front view



Rear view

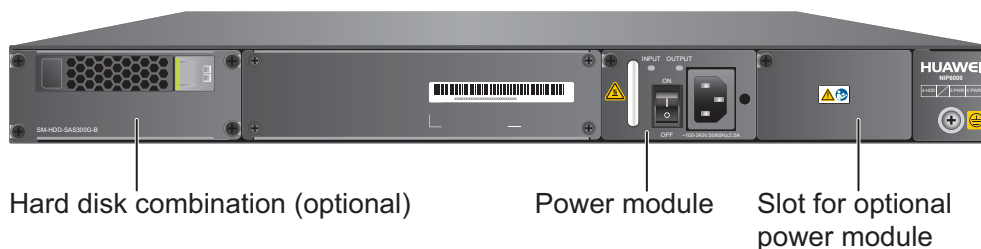


Table 2-8 describes the functions of the NIP6620 components.

Table 2-8 Functions of the NIP6620 components

| Name | Description |
|-----------------------|--|
| Fixed interface board | <p>The fixed interface board is the core component for system control and management and provides the management, forwarding, and control planes. The interface board also has an intelligent awareness engine.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |
| Expansion slot | Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-9 lists the supported expansion cards. |
| Power module | By default, power module is provided. Two power modules are supported to provide 1+1 power redundancy. If one power module fails, the other can support the entire system so that you can replace the faulty power module without interrupting device operation. |
| Hard disk combination | Hard disks are used to store logs and reports. The device supports optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. |

Ports

The fixed interface board provides the following ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 2 USB 2.0 ports
- 4 GE optical ports
- 8 10/100/1000M autosensing Ethernet electrical ports

[Table 2-9](#) lists the supported types of expansion cards.

Table 2-9 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

NOTE

WSIC: Wide Service Interface Card

2.2.5 NIP6650

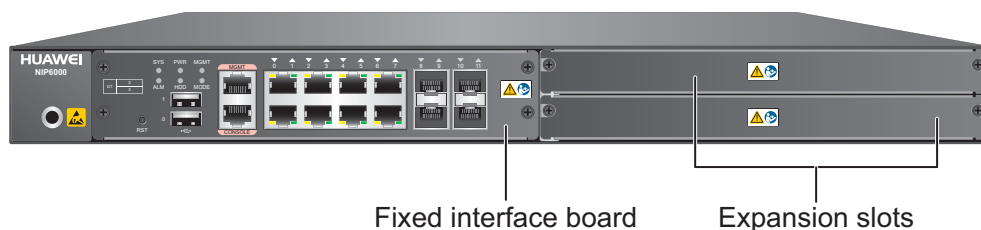
The NIP6650 uses an integrated chassis that contains the fixed interface board, power module, and fan module. You can also add some optional modules, such as hard disk, and expansion cards, to improve system reliability and add more ports.

Appearance

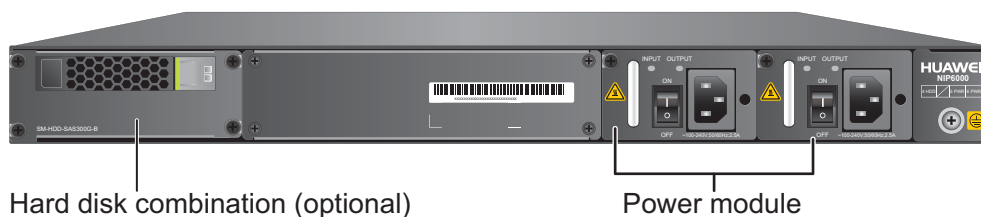
Figure 2-6 illustrates the appearance of the NIP6650.

Figure 2-6 Appearance of NIP6650

Front view



Rear view of the AC model



Rear view of the DC model

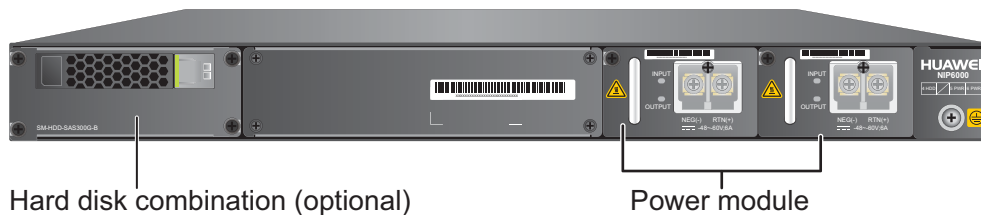


Table 2-10 describes the functions of the NIP6650 components.

Table 2-10 Functions of the NIP6650 components

| Name | Description |
|-----------------------|--|
| Fixed interface board | <p>The fixed interface board is the core component for system control and management and provides the management, forwarding, and control planes. The interface board also has an intelligent awareness engine.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |
| Expansion slot | Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-11 lists the supported expansion cards. |
| Power module | Two DC or AC power modules are mandatory to provide 1+1 power redundancy. If one power module fails, the other can support the entire system so that you can replace the faulty power module without interrupting device operation. |
| Hard disk combination | Hard disks are used to store logs and reports. The device supports optional hard disk combination SM-HDD-SAS300G-B, SM-HDD-SAS600G-B or SM-HDD-SAS1200G-B. |

Ports

The fixed interface board provides the following ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 2 USB 2.0 ports
- 4 GE optical ports

- 8 10/100/1000M autosensing Ethernet electrical ports

Table 2-11 lists the supported types of expansion cards.

Table 2-11 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

 **NOTE**

WSIC: Wide Service Interface Card

2.2.6 NIP6680

The NIP6680 uses an integrated chassis that contains the SPUA (main processing unit), SPUB (service engine), interface card, power module, and fan module. You can also add some optional modules, such as hard disk and expansion cards, to improve system reliability and add more ports.

Appearance

Figure 2-7 illustrates the appearance of the NIP6680.

Figure 2-7 Appearance of NIP6680

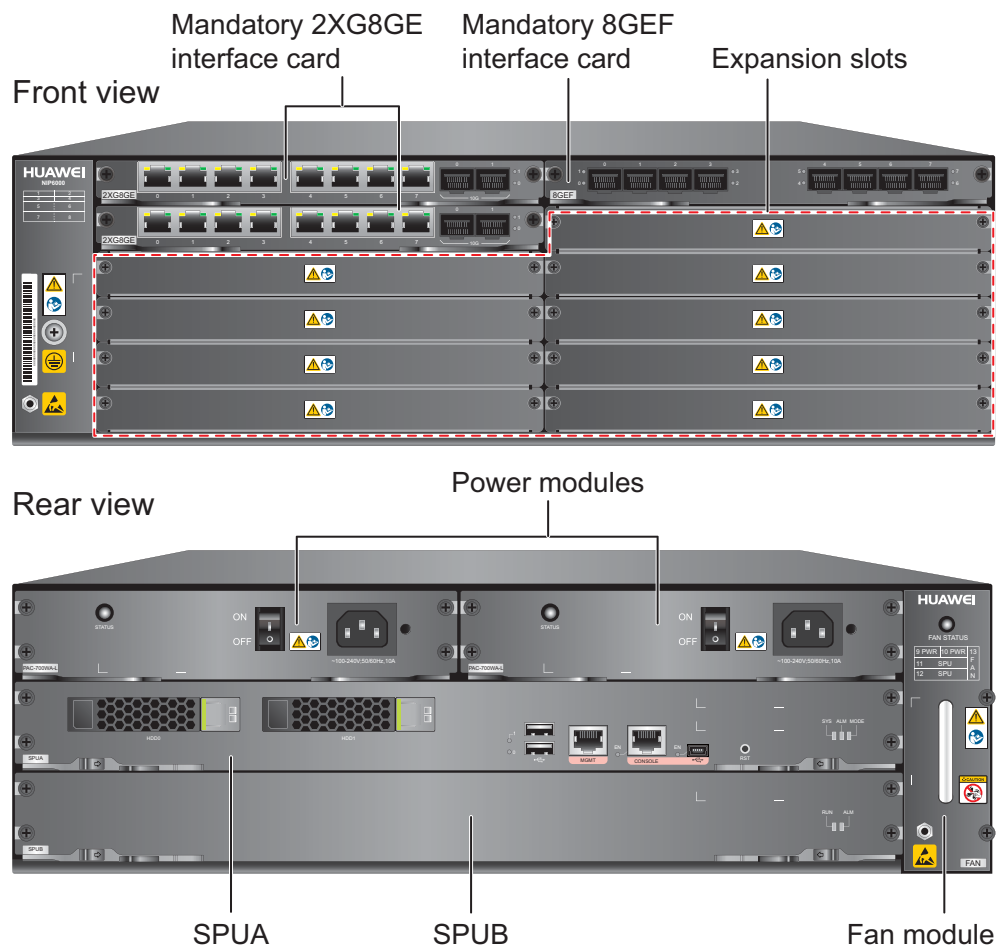


Table 2-12 describes the functions of the NIP6680 components.

Table 2-12 Functions of the NIP6680 components

| Name | Description |
|---------------------------------|---|
| SPUA (the main processing unit) | <p>SPUA is the core component for system control and management and provides the management, forwarding, and control planes. Meanwhile, both SPUA and SPUB have an intelligent awareness engine (IAE) and provide intelligent awareness service.</p> <ul style="list-style-type: none"> ● Management plane: provides ports for configuration, test, and maintenance and implements such functions as running status monitoring, environment monitoring, log and alarm processing, system loading, and system upgrades. It can use the hard disk SM-HDD-SAS300G-A, SM-HDD-SAS600G-A or SM-HDD-SAS1200G-A to record logs and reports in real time. ● Forwarding plane: parses and processes packets and associates with other planes to forward, discard, or translate packets. ● Control plane: obtains user authentication information and sends authentication results to the forwarding plane, so that the forwarding plane can process packets based on user information. ● Intelligent awareness engine: is aware of the service of each packet, parses the content to identify the application of the packet as well as the file, virus, URL, intrusion, and attack information in the packet or flow, and provides the forwarding plane with the detection result for further processing. |
| SPUB (the service engine) | <p>SPUB has an IAE to provide content security. The CPU resources of SPUB on the NIP6680 are dedicated for the IAE. Therefore, NIP6680 has a higher performance than other NIP products.</p> |
| Interface card (mandatory) | <p>The interface card provides gigabit and 10-gigabit electrical and optical ports. The interface card is installed before shipment and can be moved to another slot. The interface card is not hot-swappable.</p> |
| Expansion slot | <p>Expansion slots are reserved for expansion cards to provide more ports or functions. Table 2-13 lists the supported expansion cards.</p> |
| Power module | <p>Two DC or AC power modules are mandatory to provide 1+1 power redundancy. If one power module fails, the other can support the entire system so that you can replace the faulty power module without interrupting device operation.</p> |

| Name | Description |
|------------|--|
| Fan module | The fan module provides air flow for heat dissipation. The fan module supports hot-swapping and can be replaced without interrupting device operation. However, to prevent overheating, do not operate the device without a functioning fan module for more than one minute. |

Ports

The SPUA provides the following fixed ports:

- 1 out-of-band management port (RJ45)
- 1 console port (RJ45)
- 1 console port (mini USB)
- 2 USB 2.0 ports

The NIP6680 by default has two 2XG8GE interface cards and one 8GEF interface card to provide the following service ports:

- 8 GE optical ports
- 16 10/100/1000M autosensing Ethernet electrical ports
- 4 10GE optical ports

The five expansion slots on the NIP6680 support the expansion cards listed in [Table 2-13](#).

NOTE

The slots are divided into two types: one for Wide Service Interface Cards (WSIC) and the other for Extended Service Interface Cards (XSIC). An XSIC is twice as high as a WSIC. An XSIC slot can also hold a WSIC card, but only in the lower part, and in this case, no other card can be installed in the upper part.

When you install a WSIC card on the NIP6680, you can install it only in the lower part of slot 5/6/7/8, as shown in the red box in [Figure 2-8](#).

Figure 2-8 WSIC installation slots



Table 2-13 Supported expansion cards

| Expansion Card | Description |
|----------------------------|--|
| 8GE WSIC Interface Card | Provides eight gigabit RJ45 Ethernet ports. |
| 2XG8GE WSIC Interface Card | Provides eight gigabit RJ45 ports and two 10-gigabit SFP+ ports. |
| 8GEF WSIC Interface Card | Provides eight gigabit SFP ports. |
| 4GE-BYPASS WSIC Card | Provides two electrical bypass links. |

2.2.7 NIP6830

This section describes the appearance and hardware system features of the NIP6830.

Appearance

The NIP6830 has an integrated chassis and adopts a centralized routing engine and a distributed forwarding architecture.

The NIP6830 chassis have both AC and DC models. [Figure 2-9](#) shows the DC chassis, and the [Figure 2-10](#) shows the AC chassis.

Figure 2-9 DC chassis



Figure 2-10 AC chassis



System Features

The NIP6830 provides the following system features:

- Distributed hardware-based forwarding
- Separation of control and service channels for ensuring non-blocking of control channels
- Carrier-class reliability and manageability
- Modular-level shielding for meeting Electro Magnetic Compatibility (EMC) requirements
- Hot-swappable boards, power modules, and fans
- MPUs in 1:1 backup mode
- Backup for key components such as power modules, fan modules, clocks, and management buses
- Protection against misinsertion of boards
- Queries about alarm prompts, alarm indications, running status, and alarm status of the power supply
- Queries about alarm prompts, alarm indications, running status, and alarm status of the voltage and ambient temperature

2.2.8 NIP6860

This section describes the appearance and hardware system features of the NIP6860.

Appearance

The NIP6860 has an integrated chassis and adopts a centralized routing engine and a distributed forwarding architecture.

Figure 2-11 shows the chassis of the NIP6860.

Figure 2-11 NIP6860 chassis



System Features

The NIP6860 provides the following system features:

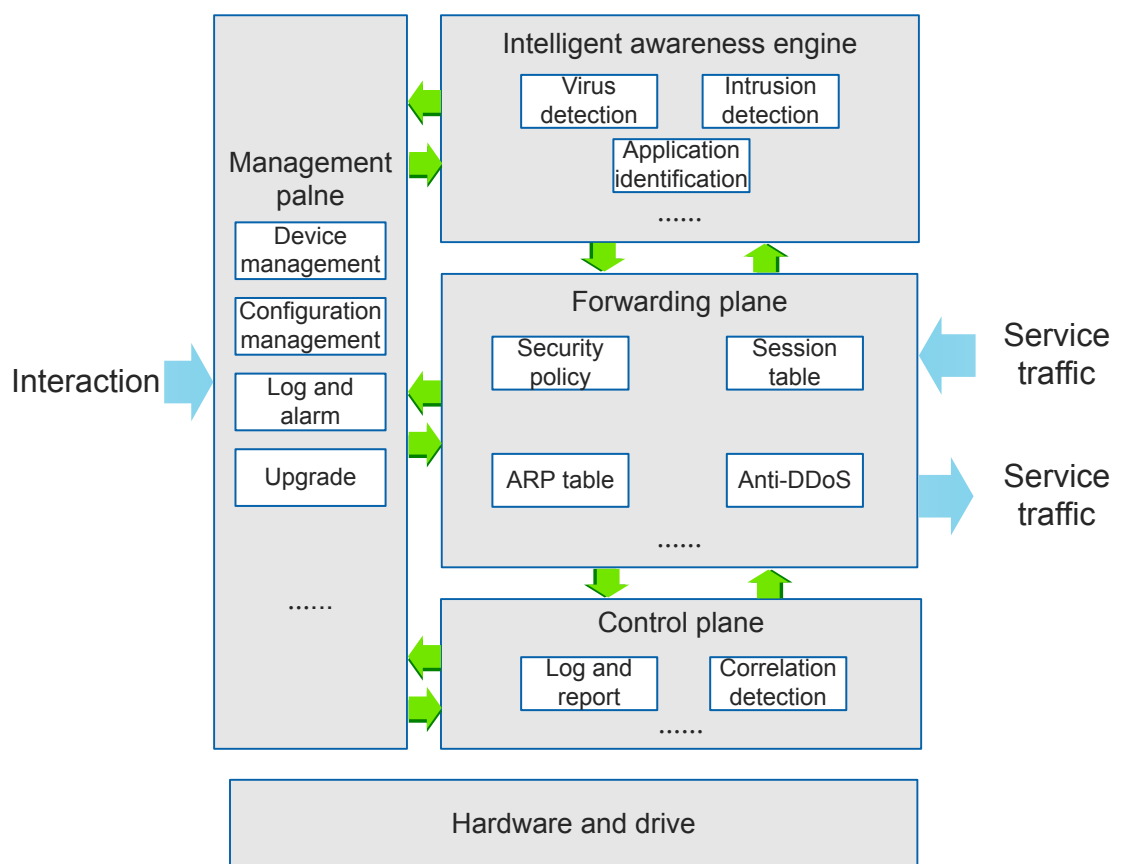
- Upgradable and congestion-free switching fabric, with switching capacity in the Tbit/s range
- Distributed hardware-based forwarding and rapid service deployment
- Compact structure for increasing interface density
- Normalized system component design
- Separation of control, service, and monitoring channels for ensuring non-blocking of control and monitoring channels
- Carrier-class reliability and manageability
- Modular-level shielding for meeting Electro Magnetic Compatibility (EMC) requirements
- Hot-swappable boards, power modules, and fans
- U-shaped air channels for improving system heat dissipation
- Distributed power supply for enhancing power supply capabilities of a single chassis
- 200-mm fans
- SRUAs in 1:1 backup mode

- SFUs in load balancing mode
- Backup for key components such as power modules, fan modules, clocks, and management buses
- Protection against misinsertion of boards
- Queries about alarm prompts, alarm indications, running status, and alarm status of the voltage and ambient temperature

2.3 Software Architecture

As shown in **Figure 2-12**, the NIP6000 uses the new multi-plane software architecture to ensure high-speed packet processing and system stability.

Figure 2-12 Software architecture



- **Hardware and drive**
Provide hardware and drive supports to packet forwarding.
- **Management plane**
A plane on which an administrator configures, manages, and maintains the NIP6000.
- **Forwarding plane**
A plane through which packets are forwarded to corresponding service modules for service processing.
For the packets that match security policies, this plane forwards these packets to the IAE for content security detection and processes them based on detection results and policies.

The separation of the forwarding plane and IAE guarantees high-speed packet forwarding and low delays. If the NIP is overloaded, packets are preferentially forwarded.

- IAE

An engine that performs content security detection on the packets from the forwarding plane. It performs deep application identification and protocol decoding as well as fine-grained intrusion and virus detection on decoded fields.

- Control plane

A plane for non-forwarding service processing. For services such as log report generation and content security detection, the service processing requirement is higher than the packet forwarding requirement.

3 Product Functions

3.1 Product Function List

Table 3-1 lists the functions supported by the NIP6000.

Table 3-1 List of the functions supported by the NIP6000

| Function | Subfunction | Description |
|----------------|--|---|
| Threat defense | Intrusion prevention | Defends against common attacks, such as worms, Trojan horses, botnets, cross-site scripting, and SQL injection, based on the signature database, and provides user-defined signatures to defend against new attacks. |
| | Antivirus | Scans for viruses in files transmitted through HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB and prevents virus-infected files from being transmitted. |
| | URL filtering | Configuring malicious URL detection and blacklist prevents users from access malicious URLs and blacklist URLs. |
| | Application identification and control | Identifies more than 6000 applications, including P2P, IM, online gaming, social networking, video, and audio applications, based on the application identification signature database. Takes actions (block, traffic limit, and application usage display) for the identified applications. |
| | APT Defense | Interworks with Huawei FireHunter to defend against APT attacks. |
| | IPv6 traffic detection | Detects threats in IPv6 traffic. |
| | SSL traffic detection | Decrypts HTTPS traffic and detects threats. |

| Function | Subfunction | Description |
|----------------------------|---------------------------------------|---|
| | Tunnel traffic detection | Detects attacks on IPv4 over IPv6, IPv6 over IPv4, MPLS (Layer 1/Layer 2 encapsulation), QinQ, and GRE tunnel traffic. |
| | Interworking with firewalls | Sends detection results to a connected firewall, so that the firewall adds the source or destination IP addresses of attack packets to the blacklist and blocks subsequent attack packets. |
| Abnormal traffic defense | Anti-DDoS | <ul style="list-style-type: none"> ● Supports the auto-learning of traffic models. ● Defends against multiple types of DDoS attacks, including: <ul style="list-style-type: none"> - Network-layer DDoS attacks, such as SYN flood, UDP flood, ICMP flood, and ARP flood - Application-layer DDoS attacks, such as HTTP flood, HTTPS flood, DNS flood, and SIP flood |
| | Single-packet attack defense | <p>Defends against multiple types of single-packet attacks, including:</p> <ul style="list-style-type: none"> ● Scanning attacks, such as IP sweep and port scanning ● Malformed packet attacks, such as IP spoofing, LAND, Smurf, Fraggle, WinNuke, Ping of Death, Teardrop, IP fragment, ARP spoofing, and attacks using invalid TCP flags ● Special control packet attacks, including attacks using oversized ICMP packets, ICMP unreachable packets, ICMP redirect packets, Tracert packets, and packets with options such as IP source routing, IP record route, and IP timestamp |
| | IP reputation | Discards traffic initiated from the IP addresses recorded in the loaded IP reputation database. |
| | IP-MAC binding | Supports IP-MAC address binding to prevent IP spoofing. |
| Security posture awareness | IT context awareness | Detects the types, operating systems, and enabled services of protected IT assets and dynamically generates suitable intrusion prevention policies for the IT environment. |
| | Threat map | Displays an overview of the global threat distribution and allows you to query the distribution of attacking and attacked regions and detailed attack information. |
| Bandwidth management | IP address-based bandwidth management | Restricts the maximum bandwidth on a per IP address basis or for all IP addresses. |

| Function | Subfunction | Description |
|---------------------------------------|--|---|
| | IP address-based connection management | Limits the maximum number of connections on a per IP address basis or for all IP addresses. |
| Route switching and packet forwarding | Interface pair | Supports interface pairs. In an interface pair, traffic enters one interface and is then forwarded through another, without routing table or MAC address table lookup. |
| | Out-of-path detection | Receives mirroring traffic and performs threat detection on the traffic. |
| | Layer 2 switching | Supports common link layer protocols and techniques, such as ARP and VLAN. |
| | Layer 3 routing | Supports static routes and dynamic routing protocols, such as OSPF, RIP, BGP, and IS-IS. |
| | Network protocol | Supports network protocols, such as DNS, DHCP, and ICMP. |
| Availability | Hot standby | Supports hot backup protocols, such as VRRP, VGMP, and HRP, and provides a hot standby mechanism to ensure automatic and smooth service switching to the standby device if the active device fails. |
| | Hardware bypass | Provides a bypass card to ensure service continuity if the system does not work properly due to software faults, hardware failures, or power-off. |
| Logs and reports | Logs | Provides multiple types of logs, such as traffic logs, threat logs, URL logs, operation logs, system logs, and policy matching logs, for administrators to learn network events. |
| | Reports | Provides multiple types of reports, such as traffic reports, threat reports, and policy matching reports for administrators to view network traffic and threat situations. The NIP6000 can also interwork with the eSight to provide more comprehensive and diversified reports. |
| | Network security report | NIP6000 provides a function for exporting the original report data. An administrator can upload the original data file to Huawei security center (sec.huawei.com). Then a network security report is generated for the administrator. |
| | IP address isolation | Blacklists the source or destination IP addresses of attacks to block the follow-up packets from or to the blacklisted IP addresses. Administrators can view the list of isolated IP addresses. |

| Function | Subfunction | Description |
|---------------------------|---------------------------|--|
| Operation and maintenance | Configuration management | Allows administrators to manage the device through the web UI, CLI (console, Telnet, and STelnet), and network management system (SNMP). |
| | Signature database update | Supports online and offline updates of the intrusion prevention, SA, and antivirus signature databases to ensure the defense capabilities of the device remain up-to-date. |
| | Fault diagnosis | Provides visualized fault diagnosis for administrators to diagnose fault causes, and automatically displays the diagnosis results and troubleshooting suggestions. |

3.2 Virtual Patch

The signatures of the NIP6000 are advanced and are based on vulnerabilities instead of attacks. All attacks that target at the same vulnerability are prevented. Therefore, the signatures function as virtual patches to the system.

Just as that a key of a specific pattern can open a lock of the same pattern, only the worms of specific signatures can attack exploits of the specific patterns. The NIP6000 protects unpatched operating systems and applications as follows:

1. Identify the signature of a vulnerability.
2. Scan the network traffic against the signature to block all packets of the same signature. Therefore, all worms that target at the vulnerability can be blocked, regardless of the features of the worms.

Huawei tracks and studies the evolution of every exploit (one exploit can evolve into many variants) to provide protection against the latest attack with a single signature. The signatures are created in a generic way because the more generic the signatures, the more likely the NIP6000 can prevent future exploits or variants targeting at known vulnerabilities.

3.3 Web Application Protection

The web platform forms the basis for about 90% of Internet applications, including online banking, online shopping, online gaming, web portals, and enterprise ERP/CRM. For enterprises, both internal applications and external network services involve web technology. However, the web technology used to carry important web applications poses huge security risks. Currently, more than 50% of web attacks exploit web application vulnerabilities, especially SQL injection and XSS attacks. In addition, scanning, guessing, and snooping attacks, as well as DoS and DDoS attacks that greatly compromise server availability, severely threaten web application security.

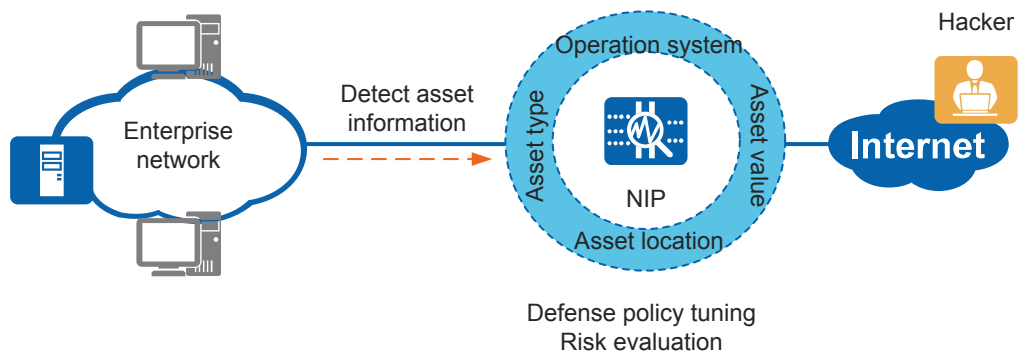
Web application protection has become crucial for enterprise networks. The NIP6000 provides abundant signatures against SQL injection and XSS attacks as well as anti-DoS/DDoS capabilities to effectively protect web servers.

3.4 Security Posture Awareness

Traditional intrusion prevention devices check packets based only on attack packet characteristics, ignoring the actual conditions of protected assets on networks. This implementation may decrease the accuracy of vulnerability risk evaluation and impair defense policy making. The NIP6000 uses security posture awareness to resolve this problem. Details are as follows:

1. The NIP6000 detects information about the protected assets on a network. Administrators can evaluate risks and tune policies based on the asset information.
In the current version, administrators must enter asset information, including the asset type, asset value, and operating system, on the NIP6000. In future versions, asset information will be detected by a vulnerability scanning system and from traffic.
2. Based on the asset information, the NIP6000 evaluates attack event risks and generates defense policies.
 - Risk evaluation: Traditional intrusion prevention devices check packets based only on attack packet characteristics, ignoring the actual conditions of protected assets on networks and causing false positives. For example, an attacker tries to exploit a Windows vulnerability by launching an attack against an intranet server that is assumed to run a Windows operating system. However, because the intranet server runs a Linux operating system, the intrusion prevention device regards the attack as a low-level risk after detecting the attack packets. This problem cannot be resolved on traditional intrusion prevention devices, resulting in false positives.
When detecting an attack, the NIP6000 extracts such information as the operating system and service from the signature. Then the NIP6000 compares the extracted information with the actual asset information stored on the device and determines the risk level of the attack event based on the asset value. The NIP6000 can filter out false positives based on the risk levels of attack events, helping administrators focus on high-risk attack events.
 - Policy tuning: Selecting appropriate signatures from a signature database can be a difficult task for an administrator. If too few signatures are selected, some attacks cannot be detected; if too many signatures are selected, the detection performance deteriorates.
Administrators can generate intrusion prevention policies specific to operating systems or applications based on asset information for more accurate attack defense.

Figure 3-1 Schematic diagram for security posture awareness

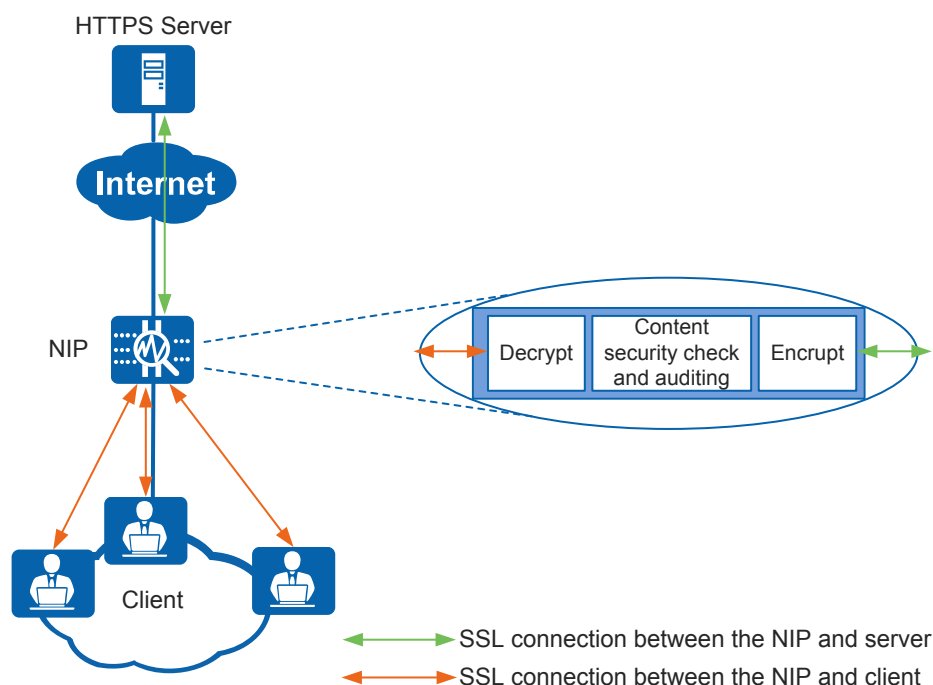


3.5 SSL Traffic Detection

For data transmission security, more and more websites and enterprises use SSL to encrypt transmitted data. As SSL traffic is encrypted, the NIP6000 must decrypt the traffic before performing threat detection on it.

The NIP6000 provides decryption policies to decrypt SSL traffic. Currently, only HTTPS traffic can be decrypted. On the network shown in [Figure 3-2](#), when an HTTPS request matches the decryption policy, the NIP6000 that serves as the SSL proxy decrypts the HTTPS packet from the client (or server), performs threat detection on the packet, encrypts the packet, and sends it to the server (or client).

Figure 3-2 Schematic diagram for SSL traffic detection



3.6 Antivirus

A virus is a set of self-replicable instructions or program codes compiled independently or embedded in certain computer programs to adversely affect the computer use by damaging certain functions or data of the computer. Commonly, viruses are embedded in files and are spread through emails, web pages, and file transfer protocols. If hosts on the intranet are infected with viruses, the entire system may crash, relevant services may be interrupted, and important data may be leaked, bringing tremendous loss to enterprises.

The antivirus function of the NIP6000 detects and scans the file transfer and file sharing protocols that are commonly used to transfer viruses. The NIP6000 blocks multiple detection-evasive mechanisms used by viruses, enhancing the antivirus capability of the network. The antivirus capabilities of the NIP6000 are as follows:

- Support of abundant protocols and applications at the application layer

The NIP6000 supports virus scanning for files transmitted through HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB.

- Virus scanning for compressed files

The NIP6000 supports the decompression of ZIP, TAR, or GZIP files with a maximum of 3 decompressable layers before it performs virus scanning.

- Signature database with massive signatures

The signature database with massive signatures ensures the advanced virus detection capability of the NIP6000. The professional virus analysis team of the Huawei traces and analyzes the latest type of viruses and updates the virus signature database for network administrators. This ensures that the NIP6000 obtains the latest signature database and has the capability to identify the maximum number of viruses.

- Different defense measures for traffic flows of various kinds and antivirus policies based on application and virus exceptions

Through security policy configuration, you can create and apply granular defense policies for different traffic flows to provide pointed network protection.

In addition, the administrator can adjust the antivirus policy to ensure the transmission of service packets by configuring extra actions for certain HTTP-based applications or adding certain false-positive viruses to the virus exception list.

3.7 Application Identification and Control

The era in which applications are defined based on ports has gone. Currently, web applications using non-well-known ports or multiple types of applications using one well-known port is common. The NIP6000 identifies more than 6000 applications, including P2P, IM, online gaming, social networking, video, and audio applications, based on detailed analysis on application signatures. In addition, Huawei's dedicated application analysis team traces the latest types of applications in real time, analyzes the applications, and rapidly updates the application identification signature database to improve the application identification capabilities of the NIP6000.

For identified applications, the NIP6000 provides the following application management and control measures:

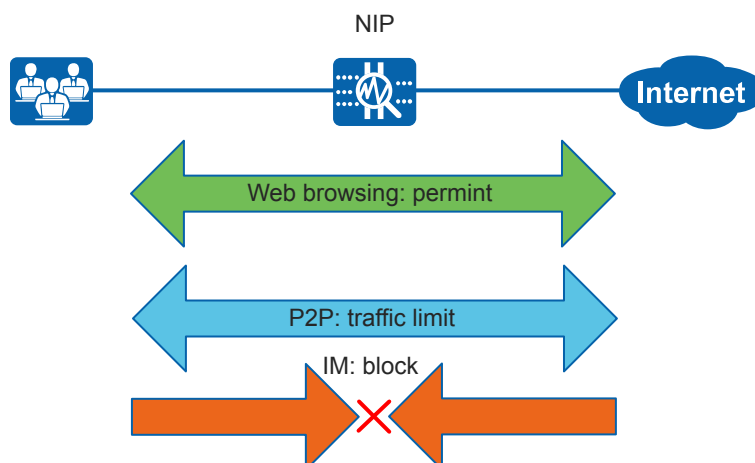
- Application access control

The NIP6000 allows the traffic of office applications to pass and blocks the traffic of applications that impact productivity, such as IM and video applications, by using application-based security policies.

- Application traffic control

To prevent P2P traffic and other traffic unrelated to work from occupying the bandwidth resources of enterprises, the NIP6000 provides application-based bandwidth management, which restricts the maximum bandwidth for P2P traffic.

Figure 3-3 Schematic diagram for application control



3.8 URL Filtering

The NIP6000 denies access to websites in the URL blacklist for the following purposes:

- To prohibit access to illegal websites or websites unrelated to work, regulating online behavior and improving working efficiency.
- To prevent worms, Trojan horses, and viruses incurred by access to malicious websites.

3.9 Abnormal Traffic Prevention

DDoS Attack Defense

An attacker launches DDoS attacks by controlling many zombie hosts to send a large number of attack packets to the attack target. As a result, links are congested, and system resources are exhausted on the attacked network. In this case, the attack target fails to provide services for legitimate users.

Servers (such as mail and web servers) are deployed in most large and medium-sized enterprises and data centers, and are vulnerable to attack. Currently, most targeted attacks are DDoS attacks, such as SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood. These DDoS attacks cause network congestion and severely threaten servers, which may prevent the servers from providing services or even force them off-line.

The NIP6000 defends against multiple types of DDoS attacks, including:

- Network-layer DDoS attacks, such as SYN flood, UDP flood, ICMP flood, and ARP flood
- Application-layer DDoS attacks, such as HTTP flood, HTTPS flood, DNS flood, and SIP flood

Setting a proper defense threshold is crucial for DDoS attack defense. If the traffic volume exceeds the threshold, the NIP6000 considers the traffic abnormal and takes a predefined defense action. The NIP6000 can automatically learn the traffic baseline to generate a defense threshold, greatly improving detection and defense accuracy and simplifying deployment and use.

Single-Packet Attack Defense

The NIP6000 defends against multiple types of single-packet attacks, including:

- Scanning attacks
Scanning attacks do not directly interrupt network devices. Such attacks gather network information for attacks. The NIP6000 can flexibly and efficiently detect such scanning and snooping packets through comparative analysis to prevent subsequent attacks. The NIP6000 can detect IP sweep and port scanning attacks.
- Malformed packet attacks
Systems targeted by malformed packets may crash if they cannot process such packets. Through packet validity checks, the NIP6000 can detect malformed packet attacks, such as IP spoofing, LAND, Smurf, Fraggle, WinNuke, Ping of Death, Teardrop, IP fragment, ARP spoofing, and attacks using invalid TCP flags.
- Attacks using control packets
Control packets can be used for attack reconnaissance, such as to probe network structures. The NIP6000 can detect multiple types of attacks using control packets, such as oversized ICMP packets, ICMP unreachable packets, ICMP redirect packets, Tracert packets, and packets with options such as IP source routing, IP record route, and IP timestamp.

IP Reputation

Huawei's IP reputation database is based on various botnet mining techniques and the blacklist generated for attack defense. The NIP6000 discards traffic initiated from the IP addresses recorded in the loaded IP reputation database. Using the IP reputation database improves defense efficiency and minimizes the false positive ratio.

3.10 Logs and Reports

For intrusion prevention products, logs and reports are important evidence for attack source tracing and network situation evaluation. The NIP6000 provides the following types of logs and reports:

- Logs
Provides multiple types of logs, such as traffic logs, threat logs, operation logs, system logs, and policy matching logs, for administrators to learn network events.
Supports the sending of logs to log servers for analysis and storage.
- Reports
Provides multiple types of reports, such as traffic reports, threat reports, and policy matching reports for administrators to view network traffic and threat situations.
The NIP6000 can also interwork with the eSight to provide more comprehensive and diversified reports.
- Maps
Provides a traffic map and threat map to display global traffic and threat distribution, based on which administrators can take further control measures.
- Network security report
Besides providing logs and reports, the NIP6000 also allows administrators to upload the raw report data to Huawei security center (sec.huawei.com). Then network security

reports are generated for the administrators. The reports provide not only the network diagnosis results and improvement suggestions but also diversified reports (in pie charts, bar charts, and curve charts). These reports display traffic, threat, web page browsing, and data leak analysis results, from which the administrator can gain visibility into network security.

Figure 3-4 and **Figure 3-5** display the threat report and threat map, respectively. Reports and maps allow administrators to get a complete picture of potential threats.

Figure 3-4 Threat report

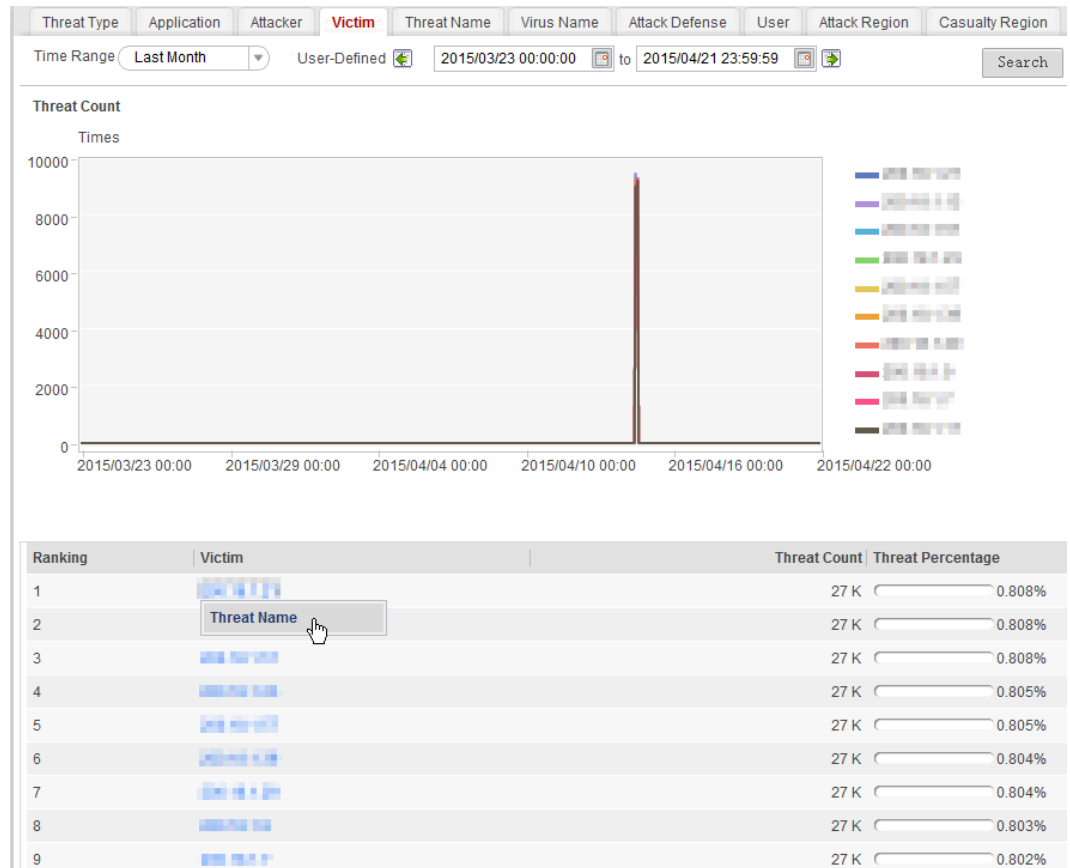
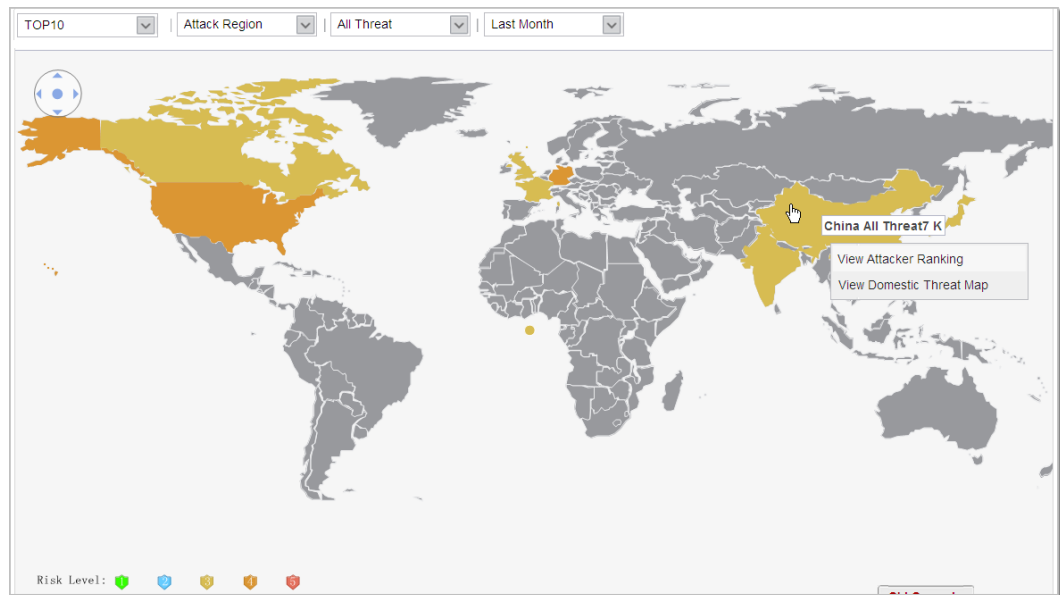


Figure 3-5 Threat map



3.11 Availability

Based on years of carrier-class product design and manufacture experience, Huawei provides the NIP6000 with carrier-class availability mechanisms at multiple levels for stable operating.

Hardware Availability

The following hardware design ensures the operating stability of the NIP6000 and prevents abnormalities in hardware environments from affecting how the device operates:

- 1+1 power module backup
The NIP6000 supports 1+1 power module backup. If one power module fails, the other ensures non-stop device operating. When both power modules are working, one power module can be hot swapped.
- Hardware bypass
The NIP6000 supports a bypass interface card. If the NIP6000 fails or is powered off, a pair of bypass interfaces on the bypass interface card interconnect the upstream and downstream devices of the NIP6000 for non-stop services. After the fault on the NIP6000 is rectified, the NIP6000 is restored to process and then forward traffic for service security.
- Heat dissipation system
The heat dissipation system ensures good heat dissipation. Fan modules are hot swappable and easy-to-maintain.

Networking Reliability

With the following networking reliability techniques, the NIP6000 software can detect device or link faults and make adjustments in a timely manner for non-stop services.

- Hot standby

The NIP6000 supports hot standby networking. If one NIP6000 fails, services can be seamlessly switched to another. The NIP6000s back up configurations and status information using HRP for smooth active/standby switchovers.

- Link-group

Link-group is a logical group into which physical interfaces are bundled. If any interface in the group is faulty, the system changes the other interfaces to Down. After all interfaces in the group recover, the system changes all interfaces to Up. This mechanism ensures unified switching for multiple links, so that service traffic can be promptly switched to healthy links.

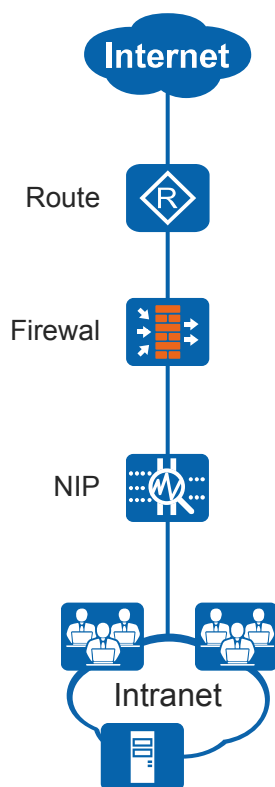
4 Application Scenarios

4.1 Internet Border

As shown in **Figure 4-1**, the NIP6000 is deployed on the border of an enterprise network and the Internet for the security of the enterprise network.

In such a scenario, the NIP6000 is often deployed in the downstream of an egress firewall or a router and transparently connects to the network. To protect multiple links, use multiple interface pairs on the NIP6000 for access.

Figure 4-1 NIP6000 deployment on the Internet border



In this scenario, the NIP6000 mainly provides the following functions:

- Application control: The NIP6000 controls P2P, video, and IM application traffic to guarantee that major services of the enterprise operate smoothly.
- Intrusion prevention: Defend against worm activities from the Internet and attacks specific to browsers and plug-ins to ensure that the enterprise network remains healthy. Block Trojan horse or spyware activities based on vulnerability attacks to protect key data information such as privacy and identity information in office computers.
- Antivirus: Perform virus scans on files downloaded from the Internet to prevent PCs on the enterprise network from being infected by viruses.
- URL filtering: Control the access of enterprise users to websites to prevent the adverse impact on working efficiency and network threats.

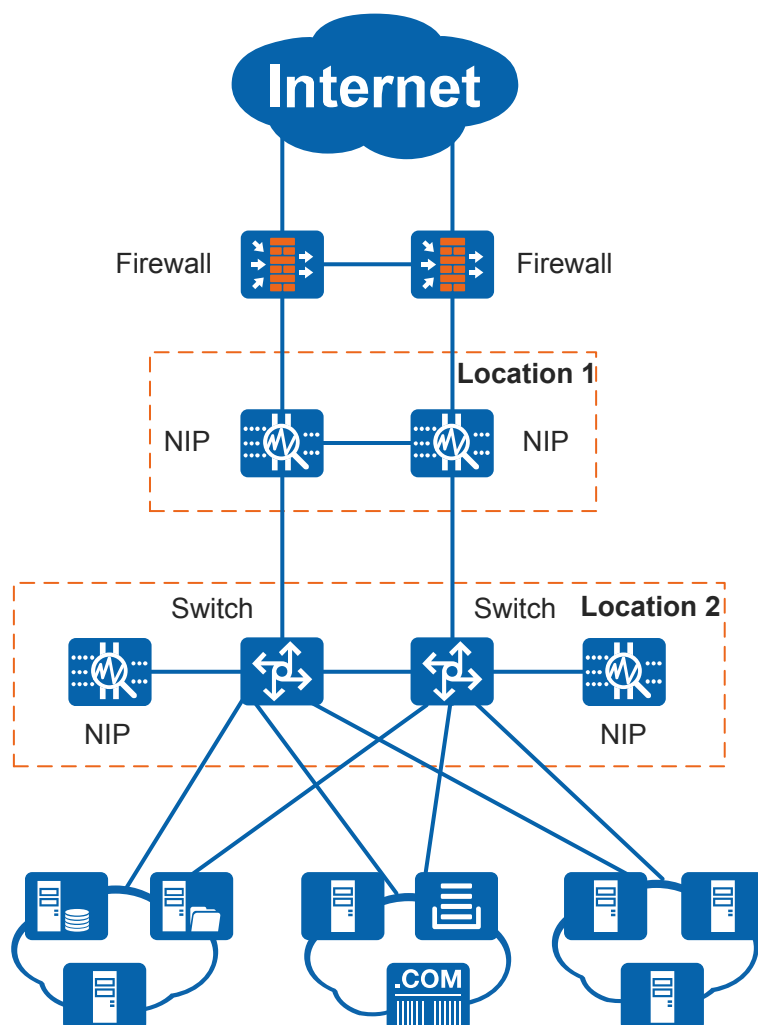
4.2 IDC/Server Upstream

As shown in [Figure 4-2](#), NIP6000s are deployed in the upstream of IDC and enterprise servers to protect data security on the servers.

In such a scenario, dual NIP6000s are often deployed against single points of failures (SPOFs). NIP6000s can be deployed in the following locations:

- Location 1: in-path deployment in the upstream of servers. In this case, the NIP6000s transparently access the network.
- Location 2: out-of-path deployment (NIP6000s are attached to switches or routers). Traffic exchanged between the Internet and servers is diverted to the NIP6000s for processing and then injected back to the main links.

Figure 4-2 NIP6000 deployment in the upstream of an IDC or servers



In this scenario, the NIP6000s mainly provide the following functions:

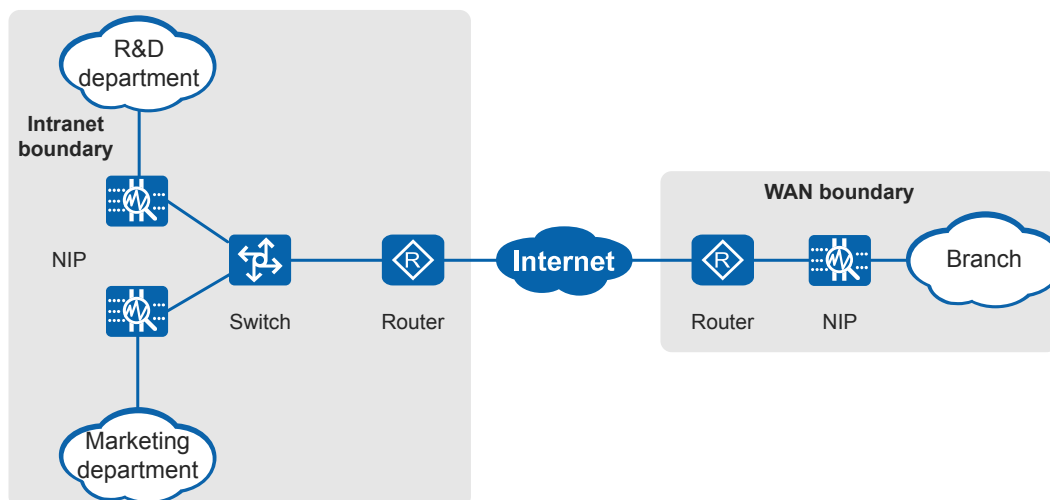
- Intrusion prevention: Defend against worm activities specific to web, mail, and DNS servers, as well as vulnerability attacks specific to services and platforms, to prevent malicious software from damaging, tampering with, or stealing data on the servers. Defend against SQL injection, scanning, guessing, and snooping attacks specific to web applications.
- Antivirus: Perform virus scans on files uploaded to the servers to prevent the servers from being infected by viruses.
- DDoS attack defense: Defend against DoS and DDoS attacks specific to the servers.

4.3 Network Border

For a large or medium-sized enterprise, its network is often divided into zones with different security levels. Isolation or security control is applied to communication between zones.

On the enterprise network shown in [Figure 4-3](#), two NIP6000s are deployed on the border between the R&D and marketing departments, and another NIP6000 is deployed between the headquarters and a branch for network isolation.

Figure 4-3 NIP6000 deployment on the network border



In this scenario, the NIP6000 mainly provides the following functions:

- **Intrusion prevention:** The NIP6000 defends against worm activities and exploits of browser and plug-in vulnerabilities to ensure the healthy operating of the enterprise network. In addition, the NIP6000 blocks Trojan horses and spyware that exploit vulnerabilities to protect key data information, such as privacy and identity information in office computers.
- **Antivirus:** The NIP6000 scans the uploaded and downloaded files to protect the PCs on the intranet.

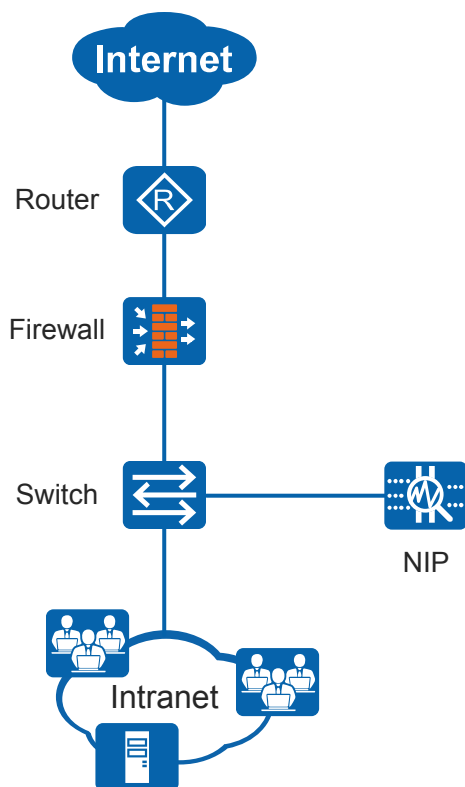
4.4 Out-of-Path Detection

Intrusion prevention devices can be deployed in out-of-path mode on networks to monitor the network security situation. In such a scenario, an intrusion prevention device records attack events and web application traffic situations, providing evidence for network security event audit and user behavior analysis, but does not take defense actions in most cases.

On the network shown in [Figure 4-4](#), a NIP6000 is attached to a switch, and the switch mirrors the traffic to be checked to the NIP6000 for detection and analysis.

The core of out-of-path deployment is that the NIP6000 checks mirrored service traffic but does not participate in traffic forwarding. The NIP6000 can be connected to the listening port on the switch or use a listening device (such as an optical splitter) to copy traffic to the NIP6000 in mirroring or optical splitting mode.

Figure 4-4 Out-of-path detection using a NIP6000



In this scenario, the NIP6000 mainly provides the following functions:

- Application identification: Identify and count P2P, video, and IM application traffic and display application usage to the enterprise administrators through reports.
- Intrusion detection: Detect the attacks initiated from the Internet and enterprise network and display the attack events through logs and reports for the enterprise administrators to evaluate network security. In addition, provide attack event risk evaluation to simplify evaluation.
- Firewall interworking: Notify a connected firewall of attack events, so that the firewall blocks attacking traffic.

5 Operation and Maintenance

5.1 Configuration and Management

NIP6000s support the following configuration and management modes:

- Web UI: You are advised to configure NIP6000s on the web UI, which simplifies configuration.
- CLI: Instead of using the web UI, you can also configure the NIP6000 using CLI commands, which can be used to configure advanced functions that cannot be configured on the web UI.
- SNMP: You can manage and maintain NIP6000s in a centralized manner on the eSight through SNMP. The eSight provides abundant reports to display network security situations.

5.2 System Maintenance

The NIP6000 provides easy-to-use maintenance functions to facilitate system maintenance.

- System software upgrade
The NIP6000 provides a hassle-free mechanism for upgrading the device and for saving configuration data, exporting data, loading software, and restarting the device.
- Fault diagnosis
The web UI provides visualized fault diagnosis to list possible causes and offer troubleshooting suggestions. Fault diagnosis includes one-click diagnosis information collector, tracert, ping, quintuple packet capture, and quintuple packet discarding statistics.
- Update of intrusion prevention/antivirus/application identification signature databases
Scheduled online update, immediate online update, local update, and rollback of the signature databases are supported. The update of signature databases empowers the NIP6000 with the latest security protection capabilities.
- Dashboard monitoring
On the Dashboard of the web UI, you can view the device operating status and query the current system information, connection status, operating load, traffic statistics, and latest logs and threat events. The shortcut links also allow you to configure functions or modify the configurations.

5.3 Security

Data System Security

The system takes the following measures to ensure data security:

- Backup recovery policy
The system data (including system software, configuration files, log files, and data in databases) can be saved to another storage medium at a specific time. If the system fails, the backup data can be imported to the system for restoration.
- Disaster recovery configuration
A configuration file is preset for disaster recovery and specified as the startup configuration file. If the current configuration file is unavailable, the disaster recovery configuration file takes effect for normal service operating.

Operation and Maintenance Security

The NIP6000 provides multi-dimensional security mechanisms, such as device management, application, and log, to ensure the security of operation and maintenance.

- Administrator permission control
The NIP6000 supports hierarchical permission control. Administrators can be granted different permissions. The login of an administrator requires a user name and password pair. Upon a successful login, an administrator can operate the NIP6000 under the granted permission.
- Access channel control
The NIP6000 supports the in-band management plane isolation mechanism and provides an independent management interface to isolate the service and management channels. By default, HTTP, HTTPS, ping, STelnet, SNMP, and Telnet services are disabled on service interfaces. Administrators are not allowed to log in to the NIP6000 through service interfaces.
Communications between the NIP6000 and NMS can be implemented using secure protocols. Services using secure protocols, such as HTTPS and STelnet, can be enabled. Services using insecure protocols, such as HTTP and Telnet, can be disabled.
- Security logging function
The security logging function is provided for important operations, such as login, logout, and management operations. The logs can be used for system security audit.
- Protection mechanism for sensitive user information
The NIP6000 supports password and identity authentication and uses an advanced encryption algorithm to encrypt sensitive user information before storage. The system allocates a password to each user for verification, securing user information. Upon the first login or password expiration, the system requests password changes to strengthen security management.
- Anti-brute-force mechanism
Unauthorized users may attempt to hack into the system by guessing an administrator's user name and password. The NIP6000 counts failed login attempts. If the number of

failed login attempts reaches the upper limit, the system adds the IP address of the user to the blacklist and blocks the access from the user for a certain period of time.

6 Technical Specifications

6.1 Hardware Specifications

6.1.1 NIP6320

This section describes the dimensions, weight, and power and environment specifications of the NIP6320.

Table 6-1 lists the technical specifications of the NIP6320.

Table 6-1 NIP6320 Technical Specifications

| Item | Description |
|--|--|
| System specifications | |
| CPU | Multi-core 1.0 GHz processor |
| Memory | DDR3 4 GB |
| Flash | 16 MB |
| CF card | 2 GB |
| Hard disk | Optional hot-swappable 300GB, 600GB or 1200GB 2.5-inch SAS hard disk. The hard disk unit is hot-swappable, but the hard disk combination is not hot-swappable. |
| SPUB (the service engine) | Not supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 44.4 mm x 442 mm x 421 mm |
| Weight | Standard: 6 kg Fully configured: 8 kg |
| Power consumption and heat consumption | |

| Item | Description |
|---|---|
| Typical power consumption | 43.4 W |
| Maximum power consumption | 44.6 W |
| Typical heat consumption | 148.0 BTU/hour |
| Maximum heat consumption | 152.3 BTU/hour |
| Power specifications | |
| AC power | Supported; 150 W built-in power module (default) and 170 W hotswappable power module (optional) |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz |
| Maximum input current (AC) | 2.5 A |
| DC power | Not supported. |
| Maximum output power | 150 W (default) or 170 W (optional) |
| Heat dissipation | |
| Fan module | Built-in fan module, cannot be removed. |
| Number of fans | 3 |
| Air flow (hot air flow, viewed facing the rear panel) | Intake on the front and left sides, exhaust on the right side |
| Port density | |
| Out-of-band management port | 1 (RJ45) |
| Console port | 1 (RJ45) |
| USB 2.0 port | 1 |
| Mandatory service ports | <ul style="list-style-type: none"> ● 2 GE Combo ports ● 4 10/100/1000M autosensing Ethernet electrical ports |
| Expansion slot | 2×WSIC |
| Types of expansion cards | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card |
| Environment specifications^c | |

| Item | | Description |
|---|-------------------------|--|
| System reliability | MTBF (year) | 11.58 |
| | MTTR (hour) | 1 |
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^e : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^e : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |
| <p>NOTE</p> <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. | | |

6.1.2 NIP6330

This section describes the dimensions, weight, and power and environment specifications of the NIP6330.

Table 6-2 lists the technical specifications of the NIP6330.

Table 6-2 NIP6330 technical specifications

| Item | Description |
|--|---|
| System specifications | |
| CPU | Multi-core 1.1 GHz processor |
| Memory | DDR3 4 GB |
| Flash | 16 MB |
| CF card | 2 GB |
| Hard disk | Optional hot-swappable 300GB, 600GB or 1200GB 2.5-inch SAS hard disk. The hard disk unit is hot-swappable, but the hard disk combination is not hot-swappable. |
| SPUB (the service engine) | Not supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 44.4 mm x 442 mm x 421 mm |
| Weight | Standard: 6 kg Fully configured: 8.6 kg |
| Power consumption and heat consumption | |
| Typical power consumption | 73.2 W |
| Maximum power consumption | 74.1 W |
| Typical heat consumption | 249.8 BTU/hour |
| Maximum heat consumption | 252.8 BTU/hour |
| Power specifications | |
| AC power | Supported. By default, one power module is provided, but two power modules are supported. If two power modules are used and one module fails, you can hot-swap the faulty power module. |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz |
| Maximum input current (AC) | 2.5 A |
| DC power | Not supported |
| Maximum output power | 170 W |
| Heat dissipation | |
| Fan module | Built-in fan module, cannot be removed. |

| Item | | Description |
|---|-------------------------|---|
| Number of fans | | 5 |
| Air flow (hot air flow, viewed facing the rear panel) | | Intake on the front and left sides, exhaust on the right side |
| Port density | | |
| Out-of-band management port | | 1 (RJ45) |
| Console port | | 1 (RJ45) |
| USB 2.0 port | | 2 |
| Mandatory service ports | | <ul style="list-style-type: none"> ● 4 GE optical ports ● 8 10/100/1000M autosensing Ethernet electrical ports |
| Expansion slot | | 2×WSIC |
| Types of expansion cards | | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card |
| Environment specifications^c | | |
| System reliability | MTBF (year) | 11.96 |
| | MTTR (hour) | 1 |
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^e : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^e : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |

| Item | Description |
|---|-------------|
| <p>NOTE</p> <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. | |

6.1.3 NIP6610

This section describes the dimensions, weight, and power and environment specifications of the NIP6610.

Table 6-3 lists the technical specifications of the NIP6610.

Table 6-3 NIP6610 Technical Specifications

| Item | Description |
|--|--|
| System specifications | |
| CPU | Multi-core 1.0 GHz processor |
| Memory | DDR3 4 GB |
| Flash | 16 MB |
| CF card | 2 GB |
| Hard disk | Optional hot-swappable 300GB, 600GB or 1200GB 2.5-inch SAS hard disk. The hard disk unit is hot-swappable, but the hard disk combination is not hot-swappable. |
| SPUB (the service engine) | Not supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 44.4 mm x 442 mm x 421 mm |
| Weight | Standard: 6 kg Fully configured: 8 kg |
| Power consumption and heat consumption | |
| Typical power consumption | 43.4 W |

| Item | Description | |
|---|---|-------|
| Maximum power consumption | 44.6 W | |
| Typical heat consumption | 148.0 BTU/hour | |
| Maximum heat consumption | 152.3 BTU/hour | |
| Power specifications | | |
| AC power | Supported; 150 W built-in power module (default) and 170 W hotswappable power module (optional) | |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz | |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz | |
| Maximum input current (AC) | 2.5 A | |
| DC power | Not supported. | |
| Maximum output power | 150 W (default) or 170 W (optional) | |
| Heat dissipation | | |
| Fan module | Built-in fan module, cannot be removed. | |
| Number of fans | 3 | |
| Air flow (hot air flow, viewed facing the rear panel) | Intake on the front and left sides, exhaust on the right side | |
| Port density | | |
| Out-of-band management port | 1 (RJ45) | |
| Console port | 1 (RJ45) | |
| USB 2.0 port | 1 | |
| Mandatory service ports | <ul style="list-style-type: none"> ● 2 GE Combo ports ● 4 10/100/1000M autosensing Ethernet electrical ports | |
| Expansion slot | 2×WSIC | |
| Types of expansion cards | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card | |
| Environment specifications^c | | |
| System reliability | MTBF (year) | 11.58 |

| Item | | Description |
|---|-------------------------|--|
| | MTTR (hour) | 1 |
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^e : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^e : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |
| <p>NOTE</p> <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. | | |

6.1.4 NIP6620

This section describes the dimensions, weight, and power and environment specifications of the NIP6620.

Table 6-4 lists the technical specifications of the NIP6620.

Table 6-4 NIP6620 Technical Specifications

| Item | Description |
|------------------------------|-------------|
| System specifications | |

| Item | Description |
|--|---|
| CPU | Multi-core 1.1 GHz processor |
| Memory | DDR3 4 GB |
| Flash | 16 MB |
| CF card | 2 GB |
| Hard disk | Optional hot-swappable 300GB, 600GB or 1200GB 2.5-inch SAS hard disk. The hard disk unit is hot-swappable, but the hard disk combination is not hot-swappable. |
| SPUB (the service engine) | Not supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 44.4 mm x 442 mm x 421 mm |
| Weight | Standard: 6 kg Fully configured: 8.6 kg |
| Power consumption and heat consumption | |
| Typical power consumption | 73.2 W |
| Maximum power consumption | 74.1 W |
| Typical heat consumption | 249.8 BTU/hour |
| Maximum heat consumption | 252.8 BTU/hour |
| Power specifications | |
| AC power | Supported. By default, one power module is provided, but two power modules are supported. If two power modules are used and one module fails, you can hot-swap the faulty power module. |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz |
| Maximum input current (AC) | 2.5 A |
| DC power | Not supported. |
| Maximum output power | 170 W |
| Heat dissipation | |
| Fan module | Built-in fan module, cannot be removed. |
| Number of fans | 5 |

| Item | | Description |
|---|-------------------------|---|
| Air flow (hot air flow, viewed facing the rear panel) | | Intake on the front and left sides, exhaust on the right side |
| Port density | | |
| Out-of-band management port | | 1 (RJ45) |
| Console port | | 1 (RJ45) |
| USB 2.0 port | | 2 |
| Mandatory service ports | | <ul style="list-style-type: none"> ● 4 GE optical ports ● 8 10/100/1000M autosensing Ethernet electrical ports |
| Expansion slot | | 2×WSIC |
| Types of expansion cards | | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card |
| Environment specifications^c | | |
| System reliability | MTBF (year) | 11.96 |
| | MTTR (hour) | 1 |
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^e : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^e : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |

| Item | Description |
|--|-------------|
| NOTE | |
| <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. | |

6.1.5 NIP6650

This section describes the dimensions, weight, and power and environment specifications of the NIP6650.

[Table 6-5](#) lists the technical specifications of the NIP6650.

Table 6-5 NIP6650 Technical Specifications

| Item | Description |
|--|--|
| System specifications | |
| CPU | Multi-core 1.0 GHz processor |
| Memory | DDR3 8 GB |
| Flash | 16 MB |
| CF card | 2 GB |
| Hard disk | Optional hot-swappable 300GB, 600GB or 1200GB 2.5-inch SAS hard disk. The hard disk unit is hot-swappable, but the hard disk combination is not hot-swappable. |
| SPUB (the service engine) | Not supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 44.4 mm x 442 mm x 421 mm |
| Weight | Standard: 6 kg Fully configured: 8.7 kg |
| Power consumption and heat consumption | |
| Typical power consumption | 107.7 W |

| Item | Description |
|---|--|
| Maximum power consumption | 110 W |
| Typical heat consumption | 367.6 BTU/hour |
| Maximum heat consumption | 375.3 BTU/hour |
| Power specifications | |
| AC power | Supported. By default, two power modules are provided. If two power modules are used and one module fails, you can hot-swap the faulty power module. |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz |
| Maximum input current (AC) | 2.5 A |
| DC power | Supported. By default, two power modules are provided. If two power modules are used and one module fails, you can hot-swap the faulty power module. |
| Rated input voltage (DC) | -48 V to -60V |
| Maximum input voltage (DC) | -40 V to -72 V |
| Maximum input current (DC) | 6 A |
| Maximum output power | 170 W |
| Heat dissipation | |
| Fan module | Built-in fan module, cannot be removed. |
| Number of fans | 5 |
| Air flow (hot air flow, viewed facing the rear panel) | Intake on the front and left sides, exhaust on the right side |
| Port density | |
| Out-of-band management port | 1 (RJ45) |
| Console port | 1 (RJ45) |
| USB 2.0 port | 2 |
| Mandatory service ports | <ul style="list-style-type: none"> ● 4 GE optical ports ● 8 10/100/1000M autosensing Ethernet electrical ports |
| Expansion slot | 2×WSIC |

| Item | | Description |
|--|-------------------------|---|
| Types of expansion cards | | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card |
| Environment specifications^c | | |
| System reliability | MTBF (year) | 10.08 |
| | MTTR (hour) | 1 |
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^e : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^e : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |
| NOTE <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. | | |

6.1.6 NIP6680

This section describes the dimensions, weight, and power and environment specifications of the NIP6680.

Table 6-6 lists the technical specifications of the NIP6680.

Table 6-6 NIP6680 Technical Specifications

| Item | Description |
|---|---|
| System specifications | |
| CPU | Multi-core 1.2 GHz processor |
| Memory | DDR3 16 GB |
| Flash | 64 MB |
| CF card | 2 GB |
| Hard disk | Optional. Purchase one or two 2.5-inch SAS hard disks (300GB/600GB/1200GB available) from Huawei as required. Two hard disks with the same capacity can form RAID1 back up and are hot swappable. NOTE The NIP6680-AC supports three types of hard disks: 300 GB, 600 GB and 1200 GB. The NIP6680-DC supports only the 300 GB hard disk. |
| SPUB (the service engine) | Supported |
| Dimensions and weight | |
| Dimensions (H ^b x W ^a x D) | 130.5 mm x 442 mm x 470 mm |
| Weight | Standard: 20 kg Fully configured: 26 kg |
| Power consumption and heat consumption^g | |
| Typical power consumption | 181.1 W |
| Maximum power consumption | 286 W |
| Typical heat consumption | 617.9 BTU/hour |
| Maximum heat consumption | 975.9 BTU/hour |
| Power specifications | |
| AC power | Supported, 1+1 power redundancy, hot-swappable |
| Rated input voltage (AC) | 100 V to 240 V, 50 Hz/60 Hz |
| Maximum input voltage (AC) | 90 V to 264 V, 47 Hz to 63 Hz |

| Item | | Description |
|---|-------------|---|
| Maximum input current (AC) | | 10 A |
| Maximum output power (AC) | | 700 W |
| DC power module | | Supported, 1+1 power redundancy, hot-swappable |
| Rated input voltage (DC) | | -48 V to -60 V |
| Maximum input voltage (DC) | | -40 V to -72 V |
| Maximum input current (DC) | | 9.6 A |
| Maximum output power (DC) | | 350 W |
| Heat dissipation | | |
| Fan module | | Supported, hot-swappable |
| Number of fans | | 3 |
| Air flow (hot air flow, viewed facing the rear panel) | | Intake on the front and left sides, exhaust on the right side |
| Port density | | |
| Out-of-band management port | | 1 (RJ45) |
| Console port | | 1 RJ45 and 1 Mini USB (only either of them can be used at a time) |
| USB 2.0 port | | 2 |
| Mandatory service ports | | <ul style="list-style-type: none"> ● 8 GE optical ports ● 16 10/100/1000M autosensing Ethernet electrical ports ● 4 10GE optical ports |
| Expansion slot | | NIP6680-AC: 5 WSIC slots NIP6680-DC: 2 WSIC slots with 2XG8GE or 3 WSIC slots without 2XG8GE ^e |
| Types of expansion cards | | <ul style="list-style-type: none"> ● 8GE-WSIC-8×1GE RJ45 interface card ● 2XG8GE-WSIC-8×1GE RJ45+2×10GE SFP+ interface card ● 8GEF-WSIC-8×1GE SFP interface card ● 4GE-BYPASS-WSIC-2×electrical links Bypass card |
| Environment specifications^c | | |
| System reliability | MTBF (year) | 19.18 |
| | MTTR (hour) | 1 |

| Item | | Description |
|--|-------------------------|--|
| Ambient temperature | Short-term ^d | Without hard disk: -5°C to 55°C With hard disk(s) ^f : 5°C to 40°C |
| | Long-term | Without hard disk: 0°C to 45°C With hard disk(s) ^f : 5°C to 40°C |
| Storage temperature | | -40°C to 70°C |
| Operating relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Storage relative humidity | | Without hard disk: 5% RH to 95% RH, non-condensing With hard disk(s): 5% RH to 90% RH, non-condensing |
| Altitude | | Without hard disk: 5,000 m With hard disk(s): 3,000 m |
| <p>NOTE</p> <ul style="list-style-type: none"> ● a. The width does not include the size of mounting ears. ● b. The height is 3 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards. ● c. Temperature and humidity are measured 1.5 m above the floor and 0.4 m in front of the rack when no protection plate exists before or after the rack. ● d. The short term operating conditions mean that the continuous operating period does not exceed 48 hours and the accumulative total period within a year does not exceed 15 days. If the continuous operating period exceeds 48 hours or the total period within a year exceeds 15 days, it is regarded as long term. ● e. As the maximum output power of a NIP6680-DC is 350 W, to prevent insufficient power supply, you can insert up to three WSICs without 2XG8GE or two WSICs with 2XG8GE in the five expansion slots. ● f. The ambient temperature change rate of a device with hard disk(s) is less than or equal to 20°C per hour. ● g. The power consumption and heat consumption of the device refer to the power consumption and heat consumption of the device equipped with one SPUB, one 8GEF WSIC interface card and two 2XG8GE WSIC interface cards. | | |

6.1.7 NIP6830

This section describes the dimensions, weight, power, and environment specifications of the NIP6830.

Table 6-7 lists the technical specifications of the NIP6830.

Table 6-7 NIP6830 Technical Specifications

| Item | | Specifications |
|--|------------------------------|--|
| System specifications | | |
| Processing unit of the MPU | | Main frequency: 1 GHz |
| BootROM capacity of the MPU | | 1 MB |
| SDRAM capacity of the MPU | | 2 GB |
| NVRAM capacity of the MPU | | 512 MB |
| Flash capacity of the MPU | | 32 MB |
| CF card | | 1 x 2 GB |
| Number of slots | MPU | 2 (slots 4, 5) |
| | SFU | - |
| | LPU/SPU | 3 (slots 1, 2, 3) |
| Dimensions and weight | | |
| Dimensions (width ^a x depth x height ^b) | | DC chassis: 442 mm x 650 mm x 175 mm (4 U) AC chassis: 442 mm x 650 mm x 220 mm (5 U) The depth is 750 mm, including the dust filter and cable rack. |
| Installation position | | N68E cabinet or a standard 19-inch cabinet |
| Weight | Empty chassis | DC chassis: 15kg AC chassis: 25kg |
| | Full configuration (maximum) | DC chassis: 30.7 kg AC chassis: 40.7 kg |
| Power specifications | | |
| Power supply mode | DC | Double hot-swappable power modules |
| | AC | Double hot-swappable power modules |
| Rated input voltage range | DC | -48 V DC to -60 V DC |
| | AC | <ul style="list-style-type: none"> ● 220 V rated voltage: 200 V AC to 240 V AC, 50/60 Hz ● 110 V rated voltage: 100 V AC to 120 V AC, 50/60 Hz |
| Maximum input voltage range | DC | -72 V DC to -38 V DC |

| Item | | Specifications |
|---|------------------------|---|
| | AC | <ul style="list-style-type: none"> ● 220 V rated voltage: 175 V AC to 264 V AC, 47 Hz to 63 Hz ● 110 V rated voltage: 90 V AC to 175 V AC, 47 Hz to 63 Hz (The output power reduces to half of the maximum output when the input voltage is in the range of 90 V AC to 175 V AC.) |
| Typical power (One LPUF-120 and two SPUs are configured.) | DC | 1270 W |
| | AC | 1406 W |
| Maximum Power (One LPUF-120 and two SPUs are configured.) | DC | 1500 W |
| | AC | 1646 W |
| Heat dissipation | | |
| Fan module | | 1 hot-swappable fan module that has two fans |
| Air flow | | Left-to-back airflow |
| Air filter | | 1 air filter in the air intake vent of the air channel |
| Environment specifications | | |
| System reliability | MTBF (year) | 25 |
| | MTTR (hour) | 0.5 |
| Ambient temperature ^c | Long-term ^d | 0°C to 45°C |
| | Short-term | -5°C to 50°C |
| | Remarks | Temperature change rate limit: 30°C/hour |
| Storage temperature | | -40°C to 70°C |
| Ambient relative humidity | Long-term | 5% RH to 85% RH, no coagulation |
| | Short-term | 5% RH to 95% RH, no coagulation |
| Storage relative humidity | | 0% RH to 95% RH |
| Long-term altitude | | Lower than 3000 m |
| Storage altitude | | Lower than 5000 m |

| Item | Specifications |
|--|----------------|
| <p>NOTE</p> <p>a. The width does not include the size of attached mounting ear.</p> <p>b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards.</p> <p>c. The measurement point of the temperature and humidity is 1.5 m above the floor and 0.4 m in front of the cabinet without the front and the back doors.</p> <p>d. The heat dissipation system allows the device to operate at the ambient temperature for a short time as long as, at the time of failure, the system has not been operating continuously for more than 96 hours and the accumulated operation time of the system per year does not exceed 15 days.</p> | |

6.1.8 NIP6860

This section describes the dimensions, weight, power, and environment specifications of the NIP6860.

Table 6-8 lists the technical specifications of the NIP6860.

Table 6-8 NIP6860 technical specifications

| Item | | Description |
|--|---------------|---|
| System specifications | | |
| Processing unit of the SRU | | Main frequency: 1.5 GHz |
| BootROM capacity of the SRU | | 8 MB |
| SDRAM capacity of the SRU | | 4 GB |
| NVRAM capacity of the SRU | | 4 MB |
| Flash capacity of the SRU | | 32 MB |
| CF card | | 2 x 2 GB |
| Number of slots | SRU | 2 (slots 9 and 10) |
| | SFU | 1 (slot 11) |
| | LPU/SPU | 8 (slots 1 to 8) |
| Dimensions and weight | | |
| Dimensions (width ^a x depth x height ^b) | | 442 mm x 650 mm x 620 mm (14 U). The depth is 770 mm covering the dust filter and cable rack. |
| Installation position | | N68E cabinet or a standard 19-inch cabinet |
| Weight | Empty chassis | 43.2 kg |

| Item | | Description |
|---|------------------------------|---|
| | Full configuration (maximum) | 112.9 kg |
| Power specifications | | |
| Power supply mode | DC | 4 hot-swappable PEMs |
| | AC | 4 PEMs+1 external AC power chassis |
| Rated input voltage range | DC | -48 V DC to -60 V DC |
| | AC | <ul style="list-style-type: none"> ● 220 V rated voltage: 200 V AC to 240 V AC, 50/60 Hz ● 110 V rated voltage: 100 V AC to 120 V AC, 50/60 Hz |
| Maximum input voltage range | DC | -72 V DC to -38 V DC |
| | AC | <ul style="list-style-type: none"> ● 220 V rated voltage: 175 V AC to 264 V AC, 47 Hz to 63 Hz ● 110 V rated voltage: 90 V AC to 175 V AC, 47 Hz to 63 Hz (The output power reduces to half of the maximum output when the input voltage is in the range of 90 V AC to 175 V AC.) |
| Typical power (Four LPUF-240s and four SPUs are configured.) | DC | 3760 W |
| | AC | 4000 W |
| Maximum power (Four LPUF-240s, and four SPUs are configured.) | DC | 4560 W |
| | AC | 4850 W |
| Heat dissipation | | |
| Fan module | | 2 hot-swappable fan modules, each with one fan |
| Air flow | | Front-to-back airflow |
| Air filter | | 1 air filter in the air intake vent of the air channel |
| Environment specifications | | |
| System reliability | MTBF (year) | 25 |
| | MTTR (hour) | 0.5 |

| | | |
|--|------------------------|--|
| Ambient temperature ^c | Long-term ^d | 0°C to 45°C |
| | Short-term | -5°C to 50°C |
| | Remarks | Temperature change rate limit: 30°C/hour |
| Storage temperature | | -40°C to 70°C |
| Ambient relative humidity | Long-term | 5% RH to 85% RH, no coagulation |
| | Short-term | 5% RH to 95% RH, no coagulation |
| Storage relative humidity | | 0% RH to 95% RH |
| Long-term altitude | | Lower than 3000 m |
| Storage altitude | | Lower than 5000 m |
| <p>NOTE</p> <p>a. The width does not include the size of the attached mounting ear.</p> <p>b. The height is 1 U (1 U = 1.75 inches, or about 44.45 mm), which is a height unit defined in International Electrotechnical Commission (IEC) 60297 standards.</p> <p>c. The measurement point of the temperature and humidity is 1.5 m above the floor and 0.4 m in front of the cabinet without the front and the back doors.</p> <p>d. The heat dissipation system allows the device to operate at the ambient temperature for a short time as long as, at the time of failure, the system has not been operating continuously for more than 96 hours and the accumulated operation time of the system per year does not exceed 15 days.</p> | | |

6.2 Standards and Protocols

This section describes the protocols and standards in which the NIP6000 is in compliance.

Table 6-9 ETS standards

| Standard or Protocol | Description |
|-----------------------------|--|
| ETS 300 019-2-2 | Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment. Part2-2: specification of environmental tests transportation |
| ETS 300 119-3 | European telecommunication standard for equipment practice Part 3: Engineering requirements for miscellaneous racks and cabinets |
| EN 300 386 Version 1.2.1 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements |

Table 6-10 IEC standards

| Standard or Protocol | Description |
|-----------------------------|--|
| IEC 61000 | Electromagnetic compatibility (EMC) |
| IEC 61000-4-2 | Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 2: Electrostatic discharge immunity test - Basic EMC publication |
| IEC 61000-4-3 | Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity test |
| IEC 61000-4-4 | Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 4: Electrical fast transient/burst immunity test - Basic EMC publication |
| IEC 61000-4-5 | Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test |
| IEC 61000-4-6 | Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 6: Immunity to conducted disturbances, induced by radio-frequency fields |
| IEC 61000-3-2 | Electromagnetic compatibility (EMC) - Part 3-2: Limits; Limits for harmonic current emissions (equipment input current $\leq 16\text{ A}$ per phase) |
| IEC 61000-3-3 | Electromagnetic compatibility (EMC) - Part 3: Limits; section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current $\leq 16\text{ A}$ |
| IEC 62151 | Safety of equipment electrically connected to a telecommunication network |

Table 6-11 ISO standards

| Standard or Protocol | Description |
|-----------------------------|--|
| ISO/IEC 11801 | Information technology - Generic cabling for customer premises |
| ISO/IEC 15802-2 | Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management |

Table 6-12 CISPR standards

| Standard or Protocol | Description |
|----------------------|--|
| CISPR 22 | Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement |

Table 6-13 ITU-T standards

| Standard or Protocol | Description |
|----------------------|--|
| I.430 | [I.430] Recommendation I.430 (11/95) - Basic user-network interface - Layer 1 specification |
| I.431 | [I.431] Recommendation I.431 (03/93) - Primary rate user-network interface - Layer 1 specification |

Table 6-14 IEEE standards

| Standard or Protocol | Description |
|----------------------|---|
| IEEE802.3 | Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification |
| IEEE802.3u | Media Access Control (MAC) parameters, physical Layer, medium attachment units, and repeater for 100 Mb/s operation, type 100Base-T |
| IEEE802.1D | Media Access Control (MAC) Bridges |
| IEEE802.3af | DTE Power via MDI |