

**iMaster NCE  
V100R019C10**

# **Product Description**

**Issue**                    03  
**Date**                     2020-10-15



**Copyright © Huawei Technologies Co., Ltd. 2020. 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: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

---

# About This Document

---

## Purpose

This document describes the network position, highlights, architecture, configuration, functions and features, and usage scenarios of iMaster NCE. With this document, you can obtain an overall understanding of this product.

 **NOTE**

The features related to unified network management and control depend on NCE components deployed. If only NCE management components are deployed, only management capabilities can be implemented.




## Intended Audience



This document is intended for:

- Network planning engineers
- Data configuration engineers
- System maintenance engineers

## Symbol Conventions

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

Symbol	Description
	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.

Symbol	Description
	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.
	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

## GUI Conventions

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

Convention	Description
<b>Boldface</b>	Buttons, menus, parameters, tabs, windows, and dialog titles are in <b>boldface</b> . For example, click <b>OK</b> .
>	Multi-level menus are in <b>boldface</b> and separated by the ">" signs. For example, choose <b>File &gt; Create &gt; Folder</b> .

## Command Conventions

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

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>boldface</b> .
<i>Italic</i>	Command arguments are in <i>italic</i> .
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x   y   ... }	Optional items are grouped in braces and separated by vertical bars. One is selected.
[ x   y   ... ]	Optional items are grouped in square brackets and separated by vertical bars. One or none is selected.

Convention	Description
{ x   y   ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[ x   y   ... ] *	Optional items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

## Change History

Issue	Date	Description
03	2020-10-15	Updated the document for SPC301.
02	2020-06-30	Updated the document for SPC300.
01	2020-05-31	This issue is the first official release.

---

# Contents

---

<b>About This Document.....</b>	<b>ii</b>
<b>1 Introduction.....</b>	<b>1</b>
1.1 Positioning.....	1
1.2 Highlights.....	3
<b>2 Architecture.....</b>	<b>5</b>
2.1 Solution Architecture.....	5
2.2 Software Architecture.....	8
2.3 External Interfaces.....	13
2.3.1 NBIs.....	14
2.3.1.1 XML NBI.....	18
2.3.1.2 CORBA NBI.....	22
2.3.1.3 SNMP NBI.....	25
2.3.1.4 TL1.....	26
2.3.1.5 Performance Text NBI (FTP Performance Text NBI).....	27
2.3.1.6 Customer OSS Test NBI.....	28
2.3.1.7 RESTful NBI.....	29
2.3.2 SBIs.....	33
2.4 Southbound DCN Networking.....	41
<b>3 Deployment Schemes.....</b>	<b>44</b>
3.1 Deployment on Private Clouds.....	44
3.2 EasySuite Deployment Tool.....	47
<b>4 Configuration Requirements.....</b>	<b>48</b>
4.1 Configurations for Deployment (Only Product, SUSE).....	48
4.2 Server Software Configurations.....	49
4.3 Client Configurations.....	49
4.4 Bandwidth Configurations.....	51
<b>5 Functions and Features.....</b>	<b>55</b>
5.1 System and Common Functions.....	55
5.1.1 System Management.....	55
5.1.2 Alarm Management.....	59
5.1.3 Security Management.....	72

5.1.3.1 User Management.....	73
5.1.3.2 Log Management.....	80
5.2 Network Management.....	84
5.2.1 Basic Functions.....	85
5.2.1.1 Topology Management.....	87
5.2.1.2 DCN Management.....	94
5.2.1.3 Performance Management.....	95
5.2.1.4 Inventory Management.....	105
5.2.1.5 NE Software Management.....	118
5.2.2 Transport Network Management.....	119
5.2.2.1 Transport NE Service Management.....	120
5.2.2.2 Transport Network Service Management.....	121
5.2.3 Access Network Management.....	123
5.2.4 IP Network Management.....	124
5.2.4.1 NE Management.....	125
5.2.4.2 IP Service Management.....	127
<b>6 High Availability.....</b>	<b>130</b>
6.1 Local HA.....	130
6.2 Disaster Recovery Solutions.....	132
<b>7 Security.....</b>	<b>142</b>
7.1 Security Architecture.....	142
7.2 Security Functions.....	143
<b>8 Personal Data and Privacy Protection.....</b>	<b>148</b>
8.1 Personal Data Scenarios.....	148
8.2 Principles and Key Technologies.....	149
8.3 Lifecycle Management.....	150
8.4 Privacy Protection Roles.....	151
<b>9 Specifications.....</b>	<b>152</b>
9.1 System-Wide Performance Specifications.....	152
9.2 NE Management Capabilities and Maximum Concurrent Client Connections.....	158
9.3 Service Management Capabilities.....	161
9.4 Equivalent Coefficients.....	162
9.4.1 Equivalent NEs in the Transport Domain.....	163
9.4.2 Equivalent NEs in the IP Domain.....	169
9.4.3 Equivalent NEs in the Access Domain.....	178
9.5 Equivalent Routes.....	180
<b>10 Version Requirements.....</b>	<b>182</b>
10.1 MSTP Series.....	182
10.2 WDM Series.....	198
10.3 RTN Series.....	224

10.4 PTN Series.....	240
10.5 NE/ATN/CX/Multi-service gateways Series.....	254
10.6 R/AR Series.....	275
10.7 RM9000 Series.....	294
10.8 Switch Series.....	294
10.9 Security Series.....	347
10.10 iCache Series.....	360
10.11 FTTx Series.....	360
10.12 MSAN Series.....	373
10.13 DSLAM Series.....	374
10.14 BITS/iSite/EDFA Series.....	377
<b>A Appendix.....</b>	<b>379</b>
A.1 Standards Compliance.....	379
A.2 Glossary.....	391



# 1 Introduction

---

[1.1 Positioning](#)

[1.2 Highlights](#)

## 1.1 Positioning

### Trends and Challenges

With the rapid development of the Internet industry and the advent of the cloud era, new business models are emerging one after another, and enterprises are moving towards cloudification and digitalization. The telecom industry, as a digital transformation enabler for various industries, faces both challenges and new business opportunities.

Service cloudification results in great flexibility and uncertainty in service applications. However, there is a huge gap between carriers' infrastructure networks and various applications.

- A large number of legacy networks coexist with newly-built software-defined networking/network functions virtualization (SDN) networks, making it difficult or costly to adapt to new services. Especially, deploying enterprise private line services encounters long time to market, slow customer response, and inflexible packages.
- With the migration of enterprise applications to the cloud and the development of new services such as the telecom cloud, the network traffic in carriers' pipes is more dynamic and unpredictable, making traditional network planning and optimization impracticable and posing high requirements on Service Level Agreement (SLA).
- With the continuous increase in the network scale and complexity, O&M complexity is intensified. Carriers urgently need to take automatic deployment measures to reduce the skill requirements for O&M personnel and effectively control the operating expense (OPEX) in a long term.
- Traditional tier-1 carriers are transforming from copper to optical. This requires simplified OSS integration, remote ONT deployment, and intelligent P2MP O&M capability to ensure consistent user experience.

Therefore, an intelligent adapter layer (that is, a brand-new management, control, and analysis system) needs to be established between the service applications and

the infrastructure networks. The system must be able to abstract network resources and capabilities, implement automatic and centralized scheduling, and allow application developers to conveniently invoke various network capabilities to continuously innovate services and applications at an unpredicted rate.

## Product Positioning

iMaster NCE effectively associates physical networks with business intents. In the southbound direction, it implements centralized management, control, and analytics of global networks, as well as enabling cloud-based resource management, full-lifecycle automation, and intelligent closed-loop management driven by data analytics based on business and service intents; In the northbound direction, it provides open network APIs for quick integration with IT systems.

NCE is located at the management and control layer of the cloud network:

- NCE manages and controls IP, transport, and access devices on lower-layer networks, supports unified management and control of SDN and legacy networks, and supports automation of single-domain, multi-domain, and cross-layer services.

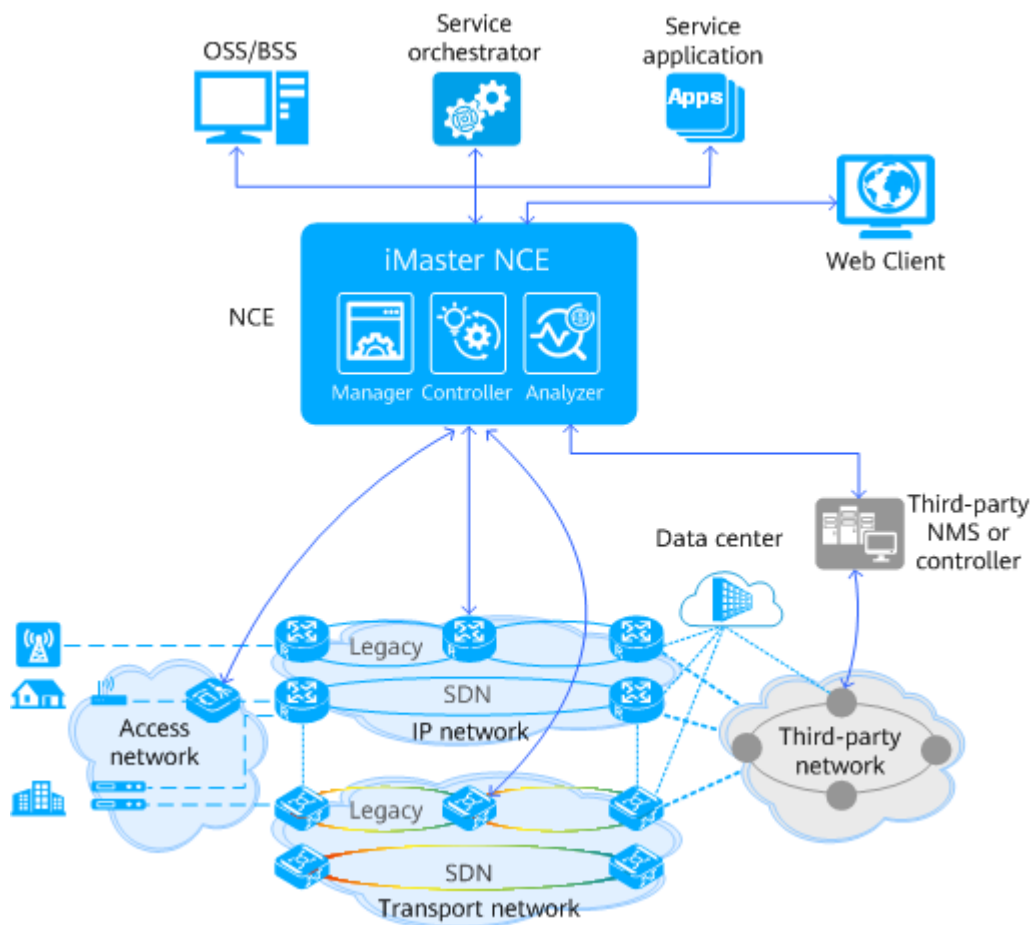
NCE can also connect to a third-party management and control system to implement cross-vendor service orchestration and automation.

- NCE also opens capabilities to support interconnection and integration with upper-layer OSSs, BSSs, and service orchestrators to support quick customization of the application layer.

The goal of NCE is to build an intent-driven network (IDN) that is first automated, then self-adaptive, and finally autonomous.

- Automated: Network deployment and maintenance are automated throughout the network lifecycle.
- Self-adaptive: Service policies are automatically generated based on big data using the real-time Analyzer to implement proactive maintenance and closed-loop optimization.
- Autonomous: Artificial intelligence and machine learning are used to build an intelligent network that can automatically generate dynamic policies.

**Figure 1-1** NCE network positioning



## 1.2 Highlights

NCE is a network lifecycle automation platform that integrates management, control, and analysis. It focuses on service self-adaptation, O&M automation, and network autonomy to support carriers' transformations to network cloudification and digital operations.

### Unified Management and Control Supporting Smooth Network Evolution

NCE integrates the functions of the traditional network management system (NMS) and SDN controller to unify the management and control of SDN and non-SDN (legacy) networks. It fully utilizes the automation advantages of the SDN network, maximizes the value of existing networks, and reduces the technical difficulty and risk of network evolution.

### Network Analysis Providing Proactive Maintenance Based on Big Data

NCE uses technologies such as telemetry to collect network-wide data in real time. With the help of its big data platform and flexible optimization strategies, NCE implements panoramic display and in-depth analysis of the quality and traffic data of the entire network, to ensure that the network is running stably and accurately implementing its users' intent.

## **Cloud Platform Supporting Flexible Deployment**

NCE greatly simplifies O&M by using a unified cloud platform to provide O&M portals and user authentication, identical API proxy, unified installation, deployment, and upgrade, as well as consistent data models throughout the lifecycle.

NCE adopts a cloud service architecture, and its management, control, and analysis modules can be deployed on demand to meet different customer requirements in different scenarios.

## **Open Interfaces Implementing Agile DevOps**

NCE provides open southbound and northbound interfaces. The northbound interfaces are RESTful APIs that connect third-party platforms. With such interfaces, NCE allows flexible integration, reuse, and combination of existing microservices and third-party capabilities so that carriers and third-party partners can quickly develop and customize innovative service applications to adapt to diversified and changing business scenarios and network technologies.

# 2 Architecture

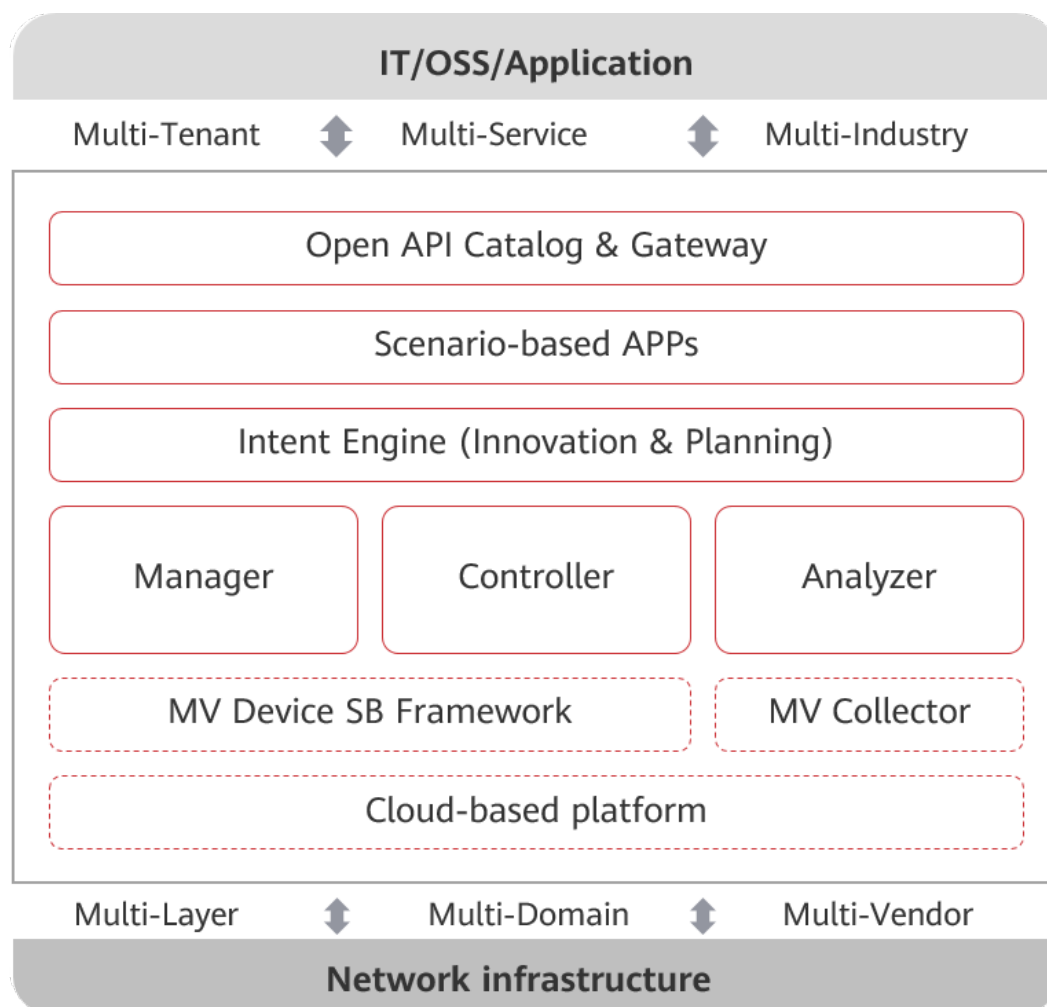
---

- [2.1 Solution Architecture](#)
- [2.2 Software Architecture](#)
- [2.3 External Interfaces](#)
- [2.4 Southbound DCN Networking](#)

## 2.1 Solution Architecture

**Figure 2-1** shows the architecture of the NCE-enabled cloud network solution.

**Figure 2-1** Architecture of the NCE-enabled cloud network solution



- IT/OSS/application layer  
The IT/OSS/application layer is a platform for carriers to implement digital operation transformation. In addition to traditional OSS and BSS, the IT/OSS/application layer also includes service orchestrator, policy generators based on big data analysis and artificial intelligence, and e-commerce portals that support self-service. The IT/OSS/application layer provides functions such as network infrastructure resource presentation, service path presentation, and service policy management to implement end-to-end operation of the entire network. Carriers provide application services to customers through this layer, including traditional services such as broadband, video, and B2B enterprise private line services and emerging services such as cloud computing and vertical industry IoT.
- NCE  
In the southbound, NCE implements centralized management, control, and analysis of network infrastructure, enables cloud-based resources, full lifecycle automation, and intelligent closed-loop driven by data analysis for business and service intension. In the northbound, NCE provides open network APIs for quick integration with IT systems, helping carriers accelerate service innovation and implement e-commerce operations.

NCE consists of the following layers from top to bottom:

- Open API catalog & gateway  
Provides secure and reliable access based on the unified API gateway.  
Provides open northbound interfaces (NBIs) to integrate with external systems such as the traditional OSS, orchestrator, and third-party applications. It supports backward compatibility of traditional interfaces such as CORBA/MTOSI and SNMP, and new interfaces such as REST/RESTCONF to adapt to future solutions and technology development.
- Scenario-based apps  
Provides application packages for business scenario automation. Users can define service requirements based on their business intentions without considering how the network implements them or what resources are utilized. NCE converts these service requirements into specific network configurations and delivers the configurations. NCE provides application packages for network operation and maintenance automation, Achieving end-to-end full-lifecycle automated management.
- Intent engine (innovation and planning)  
Provides lifecycle management and driving capabilities based on networks, services, and business intentions, supports intent planning, design, conversion, verification, activation, decision-making, and optimization, and implements flexible service innovation through model driving and open model and policy assembling.
- Manager  
Provides traditional management capabilities (FCAPS) for device configuration, alarms, performance, links, and QoS, and provides E2E automated service provisioning capabilities for traditional networks.
- Controller  
Provides single-domain and multi-domain (such as IP multi-domain, optical multi-domain, and IP+optical multi-layer) control capabilities in SDN networks, implements route optimization, and applies related control configurations through global multi-factor route computation.
- Analyzer  
Provides real-time data collection, status awareness, in-depth analysis, and intelligent prediction capabilities for network traffic and performance. Based on big data analysis, proactively identifies faults and potential risks and proactively generates warnings.
- Southbound collection framework  
The southbound collection architecture is decoupled by layer. Plugins can be injected to quickly extend capabilities such as multiple collection protocols, device types, and data output.
- Southbound collection  
Provides model-driven device data collection capabilities, shields collection protocol (such as telemetry, SNMP, and QX) and device version differences for the application layer, and filters duplicate collection tasks from multiple apps. In this way, data can be collected once and used for multiple times.
- Cloud-based platform

Based on the unified cloud platform, provides a unified user portal, unified network planning and IP address planning tool capabilities, unified engineering management capabilities such as installation, deployment, upgrade, and system monitoring, and unified public services such as alarm, security, topology, and inventory. Based on the Cloud microservice architecture, can be deployed independently based on user scenarios, meeting flexible requirements of different scenarios. Based on virtualization technologies, supports cloud-based deployment, which reduces CAPEX.

- Network infrastructure

The infrastructure layer (physical layer) is the network infrastructure of carriers, including the devices on the transport, IP, and access networks. It implements the most basic communication connection services. The infrastructure layer of a cloud network is a constantly evolving and ubiquitously connected network that consists of existing traditional networks and new SDN networks, and provides communication services with high broadband and low delay. It adapts to different access devices and abstracts the devices into network resource pools to support the ultimate implementation of business intents.

## 2.2 Software Architecture

NCE is a cloud-based system that uses a service-oriented software architecture. It is deployed on the virtualization platform and can be scaled flexibly. Based on the cloud platform, NCE implements three logical modules (network management, network control, and network analysis) and various application scenarios as services and components to achieve flexible modular deployment based on customer requirements.

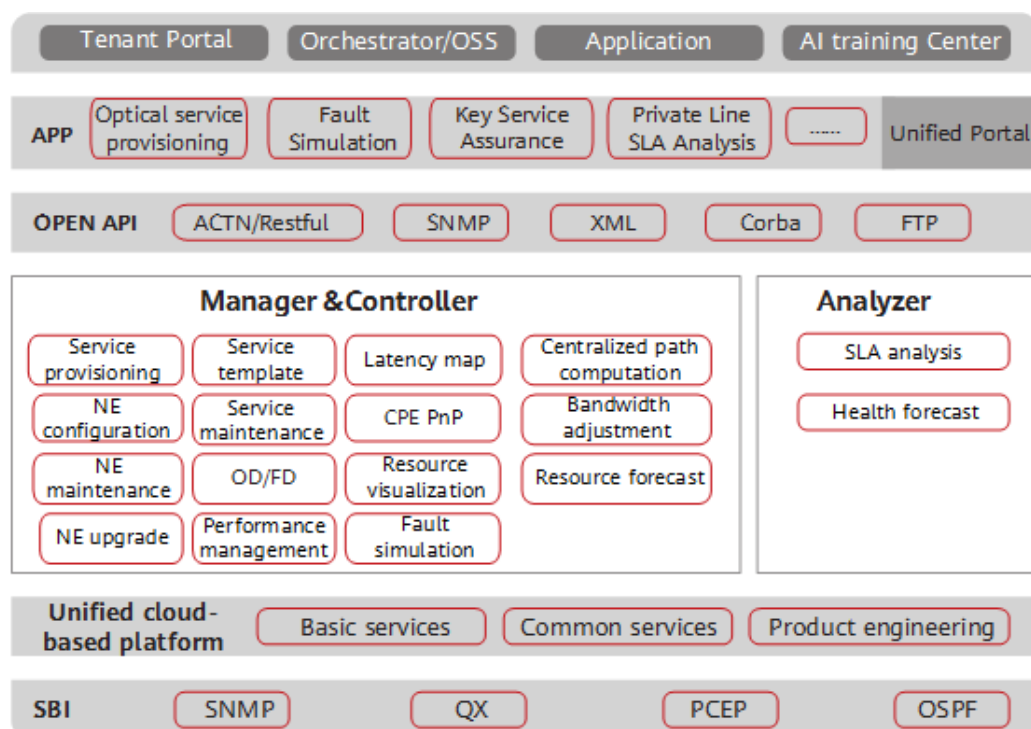
### Software Logical Architecture

Based on the cloud platform, NCE implements three logical modules (network management, network control, and network analysis) and various scenario-oriented applications as services and components. This allows customers to deploy NCE in a flexible and modular manner to meet their specific requirements.



## Logical Architecture of NCE (Transport Domain)

Figure 2-2 NCE



The following table lists the scenario-based apps supported by NCE (Transport Domain).

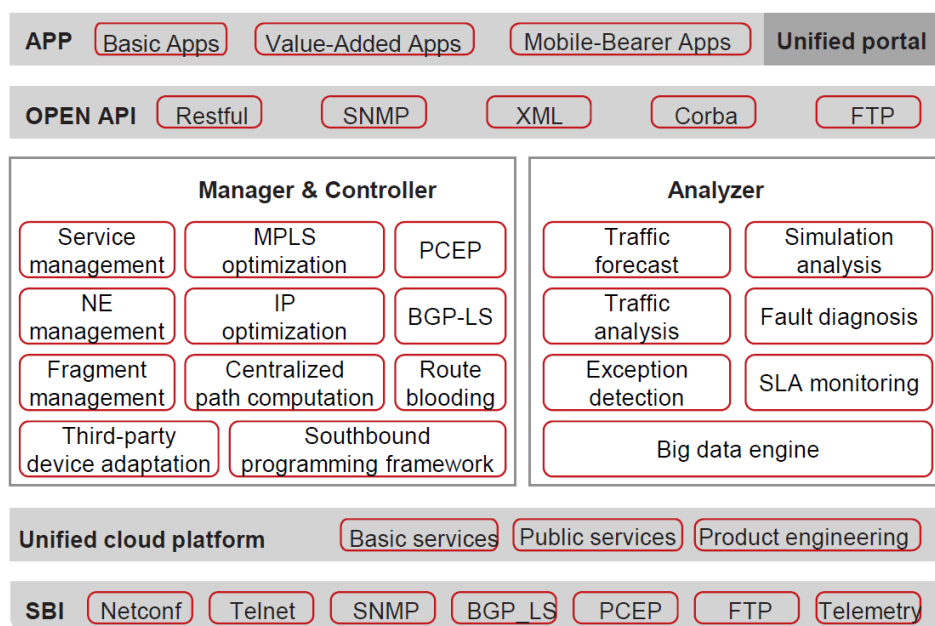
Table 2-1 Scenario-based apps

App Name	Description
System Settings	System Settings provides functions such as license management, broadcast message, remote notification, and southbound system interconnection.
Security Management	Security Management involves functions such as user management and security policies. Security Management prevents unauthorized users from accessing the system and ensures system data security.
Alarm Monitor	Alarm Monitor enables users to monitor and manage alarms or events reported by the system or MOs. Alarm Monitor also provides various monitoring and handling rules to meet different monitoring and handling requirements. In this way, network faults can be efficiently monitored, quickly located, and handled.
Network Management	Network Management enables users to perform basic management, such as security, topology, alarm, performance, and inventory management on networks and NEs.

App Name	Description
Data Collector	Data Collector provides data collection monitoring and management capabilities, including collection indicators, collection instances, and collection tasks, helping users monitor the running status of the collector.
Optical Network Health Assurance	Oriented to transport devices, analyzes the performance indicators of span fibers and optical channel with full functionality (OCh) on optical transport networks (OTNs) in real time. In addition, by combining with service path correlation analysis, the app evaluates the quality of span fibers and OChs on the entire network, identifies optical performance deterioration information in advance, and provides functions such as optical performance subhealth risk warning and automatic fiber fault locating, improving proactive network maintenance and processing and intelligent prediction and analysis capabilities.
Private Line SLA Analysis	The <b>Private Line SLA Analysis</b> app monitors the running status of private lines by collecting traffic of tenants, service quality, and availability indicators of private lines and tenants, and displays statistics directly from the perspective of tenants and private lines to visualize private line data and improve private line O&M experience.
Private Line Analysis and Assurance	Private Line Analysis and Assurance uses Big Data analysis to help you monitor the end-to-end (E2E) SLAs of private line services in real time and analyze deteriorated SLAs. You can take actions, such as evaluation, troubleshooting, prevention, and prediction in this proactive assurance system for private line SLAs.

## Logical Architecture of NCE (IP Domain)

Figure 2-3 NCE



The following table lists the scenario-based apps supported by NCE (IP Domain).

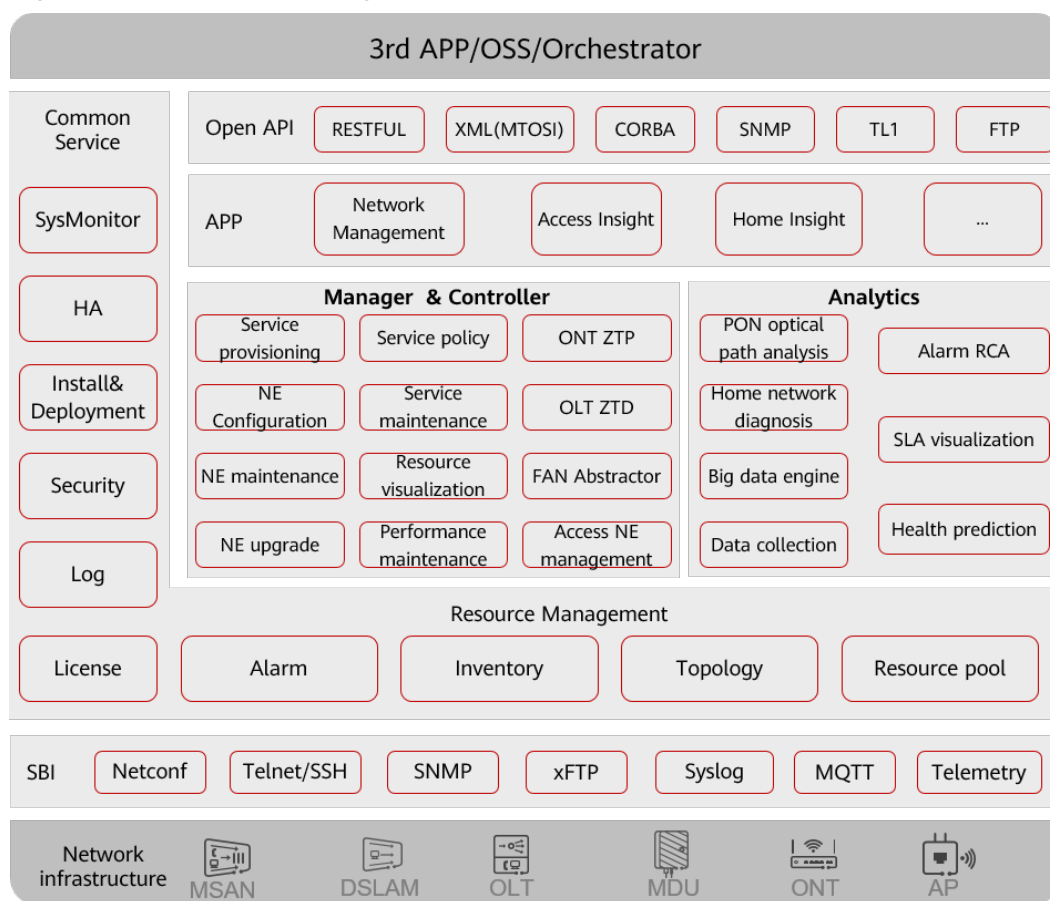
Table 2-2 Scenario-based apps

App Name	Description
System Settings	System Settings provides functions such as license management, broadcast message, remote notification, and southbound system interconnection.
Security Management	Security Management involves functions such as user management and security policies. Security Management prevents unauthorized users from accessing the system and ensures system data security.
Alarm Monitor	Alarm Monitor enables users to monitor and manage alarms or events reported by the system or managed objects (MOs). Alarm Monitor also provides various monitoring and handling rules to meet different monitoring and handling requirements. In this way, network faults can be efficiently monitored, quickly located, and handled.
Network Management	Network Management enables users to perform basic management, such as security, topology, alarm, performance, and inventory management on networks and NEs.

App Name	Description
Data Collector	Data Collector provides data collection monitoring and management capabilities, including collection indicators, collection instances, and collection tasks, helping users monitor the running status of the collector.
Smart Clock	Regarding the clock synchronization function between NEs on the bearer network in the PTN network scenario, this app enables you to plan and apply the SyncE and PTP clock configuration to online NEs.

## Logical Architecture of NCE (Access Domain)

Figure 2-4 NCE software logical architecture



The following table lists the scenario-based apps supported by NCE (Access Domain).

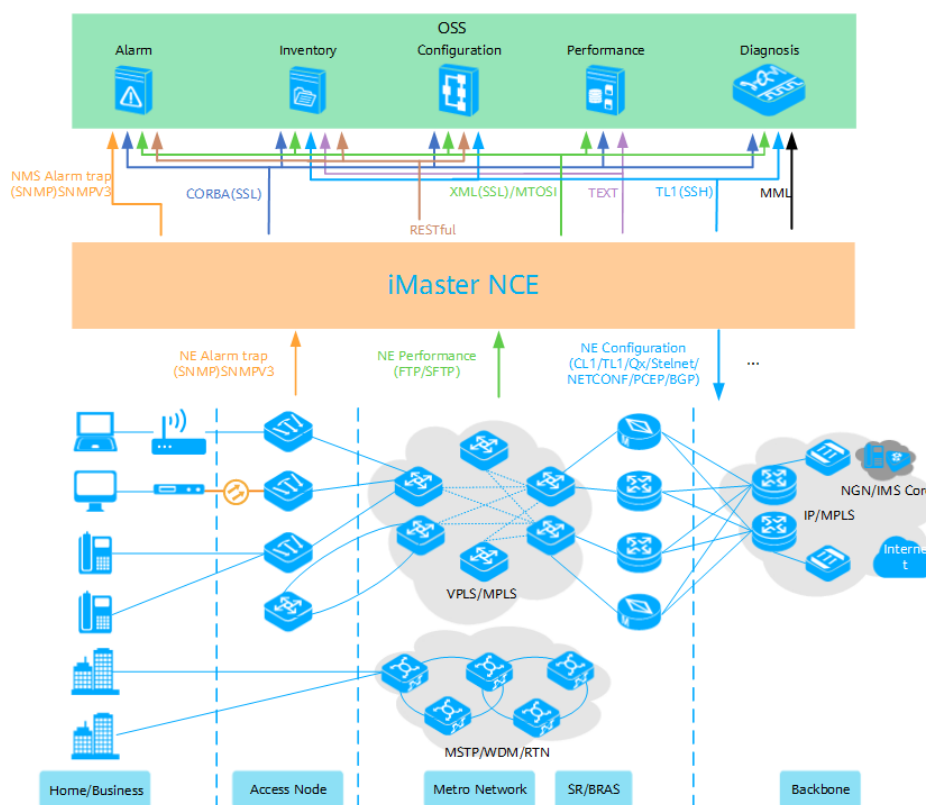
**Table 2-3** Scenario-based apps

App Name	Description
System Settings	System Settings provides functions such as license management, broadcast message, remote notification, and southbound system interconnection.
Security Management	Security Management involves functions such as user management and security policies. Security Management prevents unauthorized users from accessing the system and ensures system data security.
Alarm Monitor	Alarm Monitor enables users to monitor and manage alarms or events reported by the system or managed objects (MOs). Alarm Monitor also provides various monitoring and handling rules to meet different monitoring and handling requirements. In this way, network faults can be efficiently monitored, quickly located, and handled.
Network Management	Network Management enables users to perform basic management, such as security, topology, alarm, performance, and inventory management on networks and NEs.
Data Collector	Data Collector provides data collection monitoring and management capabilities, including collection indicators, collection instances, and collection tasks, helping users monitor the running status of the collector.

## 2.3 External Interfaces

NCE provides multiple NBIs to quickly interconnect with the OSS. It is also compatible with multiple southbound interfaces (SBIs) to implement unified management and control over transport, IP, and access devices.

Figure 2-5 Functions and features of external interfaces



### 2.3.1 NBIs

NCE offers network monitoring information, such as the alarm, performance, and inventory information, for OSSs through NBIs. The NBIs support network management, control, and analysis functions, such as service configuration and diagnostic tests. Through the NBIs, NCE can integrate with different OSSs flexibly.

The devices of each product domain support different NBI functions. For details, see the following tables.

Supported	√
Not supported	×

Table 2-4 NBI functions supported by the transport domain

Interface	Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM)	TDM RTN	Packet RTN	PTN
XML (MTO SI)	Alarm	√	√	√	√	√	√	√	√

Interface	Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM)	TDM RTN	Packet RTN	PTN
	Performance	√	√	√	√	√	√	√	√
	Inventory	√	√	√	√	√	√	√	√
	Configuration	√	√	√	√	√	√	√	√
CORBA	Alarm	√	√	√	√	√	√	√	√
	Performance	√	√	√	√	√	√	√	√
	Inventory	√	√	√	√	√	√	√	√
	Configuration	√	√	√	√	√	√	√	√
SNMP	Alarm	√	√	√	√	√	√	√	√
Performance text NBI (FTP)	Performance (Historical Performance)	√	√	√	√	√	√	√	√
RESTful	Inventory	x	x	x	√ NOTE Only USP-based NEs are supported.	x	x	x	x
	Configuration (IETF ACTN)	x	x	√	√	x	x	x	x
	Alarm	√/√	√	√	√	√	√	√	√

Interface	Feature	MSTP	Hybrid MSTP	WDM	OTN	Hybrid RTN (TDM)	TDM RTN	Packet RTN	PTN
	Performance	×	×	×	×	×	×	×	×

**Table 2-5** NBI functions supported by the access domain

Interface	Feature	MSAN/DSLAM (Narrowband Port)	MSAN/DSLAM (Broadband Port)	FTTH	FTTB/C
XML (MTOSI)	Alarm	√	√	√	√
	Performance	×	×	×	×
	Inventory	√	√	√	√
	Configuration	√	√	√	√
CORBA	Alarm	√	√	√	√
SNMP	Alarm	√	√	√	√
Performance text NBI (FTP)	Performance (Historical Performance)	√	√	√	√
TL1	Diagnosis	√	√	√	√
	Inventory	√	√	√	√
	Configuration	√	√	√	√
Customer OSS test	Diagnosis	√	√	×	×
RESTful	Inventory	×	×	×	×
	Alarm	√	√	√	√
	Performance	×	×	×	×



Interface	Feature	MSAN/DSLAM (Narrowband Port)	MSAN/DSLAM (Broadband Port)	FTTH	FTTB/C
	Configuration	x	x	x	x

**Table 2-6** NBI functions supported by the IP domain

Interface	Feature	NE Series	CX Series	Switch	BRAS	ATN	Security Series	PTN
XML (MTO SI)	Alarm	√	√	√	√	√	x	√
	Performance	√	√	x	x	√	x	√
	Inventory	√	√	√	√	√	x	√
	Configuration	√	√	√	√	√	x	√
CORBA	Alarm	√	√	√	√	√	x	√
SNMP	Alarm	√	√	√	√	√	√	√
Performance text NBI (FTP)	Performance (Historical Performance)	√	√	√	√	√	x	√
RESTful	Alarm	√	√	√	√	√	√	x
	Performance	x	x	x	x	x	x	x
	Inventory	x	x	x	x	x	x	√ <b>NOTE</b> Only VRPv8-based PTN NEs are supported.
	Configuration	√	√	x	x	√	√	x

### 2.3.1.1 XML NBI

The XML NBI is developed for NCE by referring to the MTOSI series. Using the XML NBI, NMSs of different levels can communicate with each other. The application of the XML NBI meets the development trends of integrated and cross-domain network management. The XML NBI supports alarm, configuration, performance, and inventory management functions, and enables NCE to integrate with the OSS flexibly.

## Performance Indicators

**Table 2-7** Performance indicators of the XML NBI

Indicator	Description
Number of concurrent interface requests	20. <ul style="list-style-type: none"> <li>The number of concurrent interfaces on the following interfaces is 1: getInventory, executeCLI</li> <li>The number of concurrent interfaces on the following interfaces is 4: getAllManagedElements, getAllManagedElementNames, getAllTopologicalLinks, getAllSubnetworkConnections, getAllSubnetworkConnectionNames, getAllProtectionSubnetworks, getAllFlowDomainFragments, getAllFlowDomainFragmentNames, getActiveAlarms, getHistoryAlarms, getHistoryPerformanceMonitoringData, getAllCurrentPerformanceMonitoringData, getAllTopoViewNodesInfo</li> </ul>
Delay of response to XML requests	When querying a large quantity of alarms, the XML interface handles at least 100 alarms per second, depending on the network and NE status.
Number of notification connections	10
Alarm notification processing capability	More than 60 records per second when three OSSs are connected
Alarm notification transmission delay	Shorter than 10s when three OSSs are connected
Size of an SOAP request packet	500,000 characters

## Transport Functions

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables NCE to provide alarm, performance, inventory, and configuration management on transport devices for OSSs.

The XML NBI supports the following functions:

- **Alarm management**
  - Alarm reporting
  - Synchronization of active alarms
  - Alarm acknowledgment
  - Alarm unacknowledgment
  - Alarm clearance
  - Collection of alarm statistics
- **Performance management**
  - Query of historical performance data
  - Query of current performance data
  - Reporting of performance threshold-crossing events
  - Query of performance threshold-crossing events
  - PTN performance instance management (creation, deletion, suspension, enabling, and query)
- **Inventory management**
  - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
  - Query of logical inventory, such as logical ports, fibers or cables, cross-connections, and trails
  - Export of inventory data
  - Report of changes in inventory
- **Configuration management**
  - E2E WDM trail management, including creating, deleting, activating, deactivating, and modifying trails
  - E2E OTN trail management, including creating, deleting, activating, deactivating, and modifying trails
  - MS-OTN E2E EPL/EPLAN/TrunkLink/SDH trail management, including creating, deleting, activating, and deactivating trails
  - MS-OTN E2E PWE3/VPLS trail management, including creating, deleting, activating, deactivating, and modifying trails
  - MSTP+ E2E PWE3/VPLS trail management, including creating, deleting, activating, deactivating, and modifying trails
  - Hybrid MSTP E2E trail management, including creating, deleting, activating, deactivating, and modifying trails
  - E2E EoO/EoW trail management, including creating, deleting, activating, and deactivating trails
  - Link (fiber and Layer 2 link) management, including creating and deleting links

- Per-NE-based service management for L2VPN/L3VPN/NativeEth of PTN/RTN devices, including creating, deleting, activating, deactivating, and modifying services
- **Protection group management**
  - SNCP protection (querying the protection group information and performing switching)
  - NE tunnel APS (creating, deleting, and querying protection groups and performing switching)
  - SDH MSP (querying the protection group information and switching status)
  - WDM OCP or OLP (querying the protection group information and switching status)
  - NE protection (querying the protection group information and switching status)
  - E2E tunnel APS (TNP) management (querying, creating, and deleting APS) of Hybrid MSTP NEs

## Access Functions

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables NCE to provide alarm, performance, inventory, configuration, and diagnosis management on access devices for OSSs.

The XML NBI supports the following functions:

- **Alarm management**
  - Alarm reporting
  - Synchronization of active alarms
  - Alarm acknowledgment
  - Alarm unacknowledgment
  - Alarm clearance
  - Collection of alarm statistics
  - TCA synchronization
- **Inventory management**
  - Query of IP DSLAM inventory (ADSL ports, SHDSL ports, VDSL2 ports, and templates)
  - Query of GPON physical inventory such as NEs, slots, boards, and physical ports
  - Query of GPON logical inventory such as VLANs and services
  - Query of service ports
  - Query of RU information
  - Query of ANCP information (including ADSL and VDSL2)
- **Configuration management**
  - FTTH (GPON) service creation, modification, deletion, activation, and deactivation
  - FTTB/FTTC (GPON) service creation, modification, deletion, activation, and deactivation

- xDSL configuration (including ADSL and VDSL2)
- Service port management (creation, deletion, activation, and deactivation)
- RU management (creation, deletion, and modification)
- ANCP information configuration (including ADSL and VDSL2)
- **Access diagnosis management**
  - xDSL port test (including ADSL and VDSL2)
  - Port loopback
  - OAM detection
  - ONT management

In addition, NCE supports the XML NBI that complies with the SOAP protocol in the access domain to provide functions such as VDSL2, GPON, service port, and multicast configuration and inventory queries for the OSS in a customized manner. For details, see [2.3.1.4 TL1](#). If an office requires the XML interface for interconnection with the OSS, contact Huawei engineers to customize the wsdl files and documents based on the customer's service requirements.

## IP Functions

Complying with the TMF MTOSI 2.0 series standards, the XML NBI enables NCE to provide alarm, performance, inventory, configuration, diagnostic test, and protection group management on IP devices for OSSs.

The XML NBI supports the following functions:

- **Alarm management**
  - Alarm reporting
  - Synchronization of active alarms
  - Alarm acknowledgment
  - Alarm unacknowledgment
  - Alarm clearance
  - Collection of alarm statistics
  - Synchronization of correlative alarms
- **Performance management**
  - Query of historical performance data
  - Query of performance threshold-crossing events
  - Performance instance management, including creating, deleting, enabling, suspending, and querying performance instances
- **Inventory management**
  - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
  - Query of logical inventory such as logical ports, fibers or cables, tunnels, and services
  - Export of inventory data and reporting of changes in inventory
  - QoS management (query, creation, deletion, applying, and unapplying)

- **Configuration management**
  - Provisioning of tunnel resources (TE tunnels, static CR tunnels, and static tunnels)
  - Provisioning of service resources (ATM PWE3, CES PWE3, Ethernet PWE3, VPLS, L3VPN, and PWSwitch)
- **Diagnostic test management**
  - Management of MDs, MAs, MEPS, MIPs, and RMEPS based on 802.1ag, 802.3ah, and Y.1731 standards
  - CC, LB, and LT tests
  - Management of test suites and test cases
  - BFD session management, including creating, deleting, binding, and unbinding BFD sessions
  - OAM statistics management (query, creation, and execution)
- **Protection group management**
  - E-trunk management, including creating, deleting, and querying E-trunks
  - E-APS management, including creating, deleting, and querying E-APS protection groups

### 2.3.1.2 CORBA NBI

This section describes the NCE CORBA NBI functions.

## Performance Indicators

**Table 2-8** Performance indicators of the CORBA NBI

Indicator	Description
Number of concurrent interface requests	4. <ul style="list-style-type: none"><li>● The maximum invocation concurrency of the CORBA NBI is 4. If the number of invocations exceeds 4, the invocations are queued.</li><li>● For interfaces that involve a large amount of data, such as getAllEquipment and getHistoryPMDData, it takes a long time for the NCE server to process the interface invocations. The number of concurrent interface invocations is small. Therefore, single-thread serial invocation is recommended. Otherwise, an error indicating a fully loaded task may be reported.</li></ul>
Alarm notification processing capability	A maximum of 100/s
Alarm sending delay	Shorter than 10s when three OSSs are connected.

#### NOTICE

- The alarm handling capability of the CORBA NBI depends on many factors, such as the alarm quantity on the network, and CPU performance and memory size of the server. At the same time, the CORBA NBI sends alarms synchronously, that is, another alarm will not be sent until the OSS receives the previous alarm and responds to the CORBA NBI. Therefore, the network stability between NCE and the OSS and the handling capability of the OSS will affect the alarm handling capability of NCE.
- If an alarm storm occurs, the CORBA NBI will possibly reach its handling limit. The CORBA NBI can report a maximum of 1,000,000 alarms within one hour. To ensure the stability of the system, the CORBA NBI will discard some alarms if the alarm quantity exceeds 1,000,000. You are recommended to handle network faults instantly if an alarm storm occurs. In addition, the OSS is suggested to synchronize alarms actively at proper time, for example, when the system is idle.

## Transport Functions

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables NCE to provide unified alarm and inventory management for transport devices. The CORBA NBI also enables NCE to provide service configuration, performance, diagnostic test, and protection group management for transport devices.

The CORBA NBI supports the following functions:

- **Alarm management**
  - Alarm reporting
  - Synchronization of active alarms
  - Alarm acknowledgment
  - Alarm unacknowledgment
  - Alarm clearance
- **Performance management**
  - Query of historical performance data
  - Query of current performance data
  - Reporting of performance threshold-crossing events
  - Query of performance threshold-crossing events
- **Inventory management**
  - Inventory change notification reporting
  - Query of physical inventory, such as NEs, subracks, slots, boards, and physical ports
  - Query of logical inventory, such as logical ports, fibers or cables, cross-connections, and trails
- **Configuration management**
  - Configuration of E2E services (SDH, WDM, OTN, MSTP, ASON, and RTN) in the transport domain
  - Configuration of per-NE-based services (SDH, WDM, OTN, MSTP, and PTN) in the transport domain

- Configuration of per-NE-based services for tunnels (MPLS tunnels and IP tunnels)
- Configuration of per-NE-based services (ATM PWE3, CES PWE3, Ethernet PWE3, VPLS, and PWSwitch)
- Configuration of E2E services for tunnels (only for PTN devices) (static-CR tunnel)
- Configuration of E2E services (only for PTN devices) (CES PWE3 and Ethernet PWE3)
- **Diagnostic test management (RTN and PTN)**
  - Port loopback and alarm insertion
  - Ethernet CC, LB, and LT tests
  - OAM management for MPLS LSP, PW, PWE3, and VPLS services
- **Protection group management (SDH, WDM, OTN, PTN, RTN, and Hybrid MSTP)**
  - Board protection, including querying protection groups and performing switching
  - Port protection, including querying protection groups and performing switching
  - Subnetwork connection protection (SNCP) protection, including querying protection groups and performing switching
  - Tunnel APS protection, including creating, deleting, and querying tunnel APS protection groups
  - E2E tunnel APS (TNP) management, including creating, deleting, and querying E2E tunnel APS (TNP)

## Access Functions

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables NCE to provide unified alarm for access devices.

The CORBA NBI supports the following functions:

- **Alarm management**
  - Alarm reporting
  - Synchronization of active alarms
  - Alarm acknowledgment
  - Alarm unacknowledgment
  - Alarm clearance

## IP Functions

Complying with the TMF MTNM V3.5 series standards, the CORBA NBI enables NCE to provide unified alarm and inventory management for IP devices.

The CORBA NBI supports the following functions:

- **Alarm management**
  - Alarm reporting



- Synchronization of active alarms
- Alarm acknowledgment
- Alarm unacknowledgment
- Alarm clearance
- **Inventory management**
  - Query of physical inventory, including NEs and boards.
- **Configuration management**
  - Configuration of E2E services for tunnels (only for PTN devices) (static-CR tunnel)
  - Configuration of E2E services (only for PTN devices) (CES PWE3 and Ethernet PWE3)

### 2.3.1.3 SNMP NBI

Complying with the SNMP v1/v2c/v3 standard, the SNMP NBI enables NCE to provide unified alarm management for OSSs.

## Performance Indicators

**Table 2-9** Performance indicators of the SNMP NBI

Indicator	Description
Maximum number of concurrent OSS connections	10
Alarm reporting efficiency	More than 60 alarms per second when three OSSs are connected
Alarm reporting delay	Shorter than 10 seconds when three OSSs are connected

## Functions

The SNMP NBI supports the following functions:

- Alarm reporting
- Synchronization of active alarms
- Alarm acknowledgment
- Alarm unacknowledgment
- Alarm clearance
- Heartbeat alarm reporting
- Setting of alarm filter criteria
- Alarm maintenance status reporting

### 2.3.1.4 TL1

Complying with the GR 831 standard, the TL1 NBI enables NCE to provide service provisioning (xDSL, xPON, broadband, and narrowband services), inventory query, and diagnostic test (line test and ETH OAM) in the access domain for OSSs.

The TL1 NBI supports service provisioning, inventory query, and diagnosis test functions, and uses the default port 9819.

## Performance Indicators

**Table 2-10** Performance indicators of the TL1 NBI

Item	Specification
Maximum number of OSS connections that can be received at one time	<ul style="list-style-type: none"><li>• Small- and medium-sized networks: 20<ul style="list-style-type: none"><li>- Service provisioning: 15</li><li>- Inventory query: 2</li><li>- Diagnosis test: 3</li></ul></li><li>• Large- and ultra large-sized networks: 30<ul style="list-style-type: none"><li>- Service provisioning: 20</li><li>- Inventory query: 2</li><li>- Diagnosis test: 8</li></ul></li></ul>
Processing capability for requesting commands of TL1	10 per second (only for configuration commands)
Response time for requesting commands of TL1	Within two minutes (excluding test commands)

## Functions

The TL1 NBI supports the following functions:

- **Service provisioning**
  - Provisioning of xDSL (ADSL, G.SHDSL, and VDSL2) services
  - Provisioning of G.fast services
  - Provisioning of multicast services
  - Provisioning of xPON (GPON and EPON) services
  - Provisioning of CNU services
  - Management of VLANs
  - Management of Ethernet ports
  - Management of service ports
  - Management of PVCs
  - Provisioning of voice (VoIP, PSTN, ISDN, and SPC) services

- Management of ACL & QoS and HQoS
- **Inventory query**
  - Query of various resources, such as devices, xDSL (ADSL, G.SHDSL, and VDSL2), G.fast, video, xPON (GPON and EPON), CNU, VLAN, Ethernet, service port, PVC, voice (VoIP, PSTN, ISDN, and SPC), ACL & QoS, and HQoS resources
  - Notification of resource changes
- **Diagnostic test**
  - Line test
  - ETH OAM

### 2.3.1.5 Performance Text NBI (FTP Performance Text NBI)

The performance text NBI enables NCE to export performance statistics for OSSs. NCE exports performance statistics to a specified FTP server for analysis.

## Performance Indicators

**Table 2-11** Performance indicators of the performance text NBI

Item	Indicator
Maximum number of connected OSSs	As the FTP client, NCE transmits files to one OSS only.

## Functions

The performance text NBI supports the following functions:

- Generates the performance text file in a unified format (\*.csv).
- Exports the performance text file based on the collection period (the period can be 5, 10, 15, 30, 60, 360, or 1440 minutes).
- Exports the performance text file at the scheduled time (5, 10, 15, 30, 60, 360, or 1440 minutes; the time must be longer than the collection period).
- Specifies the start time to export the performance text file.
- Checks data integrity of the performance text file. If the performance text file fails to be generated, the data will be saved to the performance text file that will be generated in the next period. (SDH, WDM and OTN performance data does not support this function.)
- Transmits the performance text file to the specified FTP or SFTP server.
- Exports the performance text file by indicator.
- Specifies the start time to delete the performance text file.
- Clears earlier performance text files periodically.
- Specifies the number of data records in a single file.

### 2.3.1.6 Customer OSS Test NBI

The customer OSS test NBI includes two types of NBI: narrowband line test NBI and ADSL line test NBI. The narrowband line test NBI provides tests on narrowband access devices (lines and terminals). The ADSL line test NBI provides query on ADSL ports and line capture and line release on ADSL lines.

#### Performance Indicators

Item	Specification
Maximum number of connections	64 clients
Connection duration	After a connection is set up, if the client does not send a command in one hour, the connection is automatically disconnected.

#### Functions

The customer OSS test NBI supports the following functions:

- **Narrowband line test NBI**
  - Dial tone test for POTS users
  - Feed voltage test for POTS users
  - Loop current test for POTS users
  - Line test for POTS users
  - Ringing test for POTS users
  - DTMF or pulse test for POTS users
  - Howler tone test for POTS users
  - Circuit test for ISDN users
  - Line test for ISDN users
  - NT1 terminal test for ISDN users
  - Narrowband line capture test
  - Narrowband line release test
  - Ringing current voltage test
  - Test stopping
- **ADSL line test NBI**
  - Query of the information about an ADSL user port
  - Control of the DSLAM test bus
  - Loopback diagnostic tests performed at the central office end on the user port
  - OAM test

### 2.3.1.7 RESTful NBI

Complying with the IETF standard, the NCE RESTful interface provides the OSS with APIs for service management, resource management, and network O&M.

RESTful is a software architecture style rather than a standard. It provides a set of software design guidelines and constraints for designing software for interaction between clients and servers. RESTful software is simpler and more hierarchical, and facilitates the implementation of the cache mechanism.

## Performance Indicators

**Table 2-12** Performance indicators of the RESTful NBI

Indicator	Description
Number of concurrent requests for a single interface	A maximum of 10. <ul style="list-style-type: none"><li>The number of concurrent interfaces on the following interfaces is 3: /restconf/v1/data/ietf-alarms:alarms/summary</li><li>The number of concurrent interfaces on the following interfaces is 5: /restconf/v1/data/ietf-alarms:alarms/alarm-inventory</li></ul>
Request response timeout interval	5 minutes
Request packet size limit	2M
Response packet size limit	10M
Notification reporting capability	A maximum of 100/s
Notification and alarm reporting delay	Less than 10 seconds
Number of notification connections (WebSocket&SSE)	A maximum of 100
Alarm reporting capability	A maximum of 100/s alarms can be reported continuously. Peak value: 400 /s (not discarded for 15s) Alarm persistency capability: When the persistent data size reaches 5 GB or the persistency duration reaches 24 hours, persistent data is triggered.

## Transport Functions

- **Resource inventory**
  - Query NEs, boards, ports, and fiber links.
  - Report resource changes of NEs, ports, and fiber links.
- **Topology**
  - Query of nodes
- **Service inventory**
  - Query of OCh and ODU tunnels and client, packet (Ethernet), and SDH services
- **Service provisioning and configuration**
  - Provisioning of OCh and ODU tunnels and client, packet (Ethernet) and SDH services
  - Service path computation
- **Fault management**
  - Alarm subscription
  - Alarm reporting
  - Alarm synchronization
  - Alarm acknowledgment/unacknowledgment
  - Query of static alarm information

Restrictions and limitations: RESTful interface IDs are not unified. Interfaces with different IDs cannot be used together.

**Table 2-13** Information about interfaces for the transport domain

Protocol Type	Function Description	Model and Standard	ID
RESTful	Inventory and OTN/ packet service provisioning	Custom model	Private ID
RESTful	Query of inventory (NEs, boards, and ports) and text export	Custom model defined by referring to the IETF standard (recommended)	UUID
Web socket/SSE	Resource change notification	Custom model defined by referring to the IETF standard (recommended)	UUID

Protocol Type	Function Description	Model and Standard	ID
RESTful	Alarm subscription, alarm reporting, alarm synchronization, alarm acknowledgment/unacknowledgement, and query of static alarm information	IETF alarm model	UUID

## IP Functions

- **Resource management**
  - Query NEs, boards, ports, fiber links, and IGP links.
  - Report resource changes of NEs, ports, fiber links, and IGP links.
- **Service management**
  - SR TE, RSVP TE, and L3VPN provisioning
  - Query of L3VPN, and tunnel services
  - Service path computation
  - Service deletion
- **Network optimization**
  - IP traffic optimization
  - MPLS traffic optimization
- **Fault management**
  - Alarm subscription
  - Alarm reporting
  - Alarm synchronization
  - Alarm acknowledgment/unacknowledgement
  - Query of static alarm information

Restrictions and limitations:

The RESTful interface IDs have been unified. The new RESTful interface models are unified, including L3VPN service provisioning interfaces, NE, board, and port inventory query interfaces, and L3VPN, and tunnel service query interfaces. Other capabilities are planned based on market requirements.

**Table 2-14** Information about interfaces for the IP domain

Protocol Type	Function Description	Model and Standard	ID
RESTful	SPTN service provisioning NBI	Enterprise standard model	UUID

Protocol Type	Function Description	Model and Standard	ID
RESTful	IP RAN service provisioning NBI	Enterprise standard model	UUID
RESTful	XML-to-RESTful, IP service provisioning, and inventory	TMF MTOSI model	MTOSI RDN
RESTful	Optimization	Custom model	UUID
RESTful	Query of inventory (NEs, boards, and ports) and text export	Custom model defined by referring to the IETF standard (recommended)	UUID
RESTful	L3VPN service provisioning	Custom model defined by referring to the IETF standard (recommended)	UUID
Web socket/SSE	Resource change notification	Custom model defined by referring to the IETF standard (recommended)	UUID
RESTful	Alarm subscription, alarm reporting, alarm synchronization, alarm acknowledgment/unacknowledgement, and query of static alarm information	IETF alarm model	UUID

## Access Functions

The RESTful NBI supports the following functions:

- **Fault management**
  - Alarm subscription
  - Alarm reporting
  - Alarm synchronization
  - Alarm acknowledgment/unacknowledgement
  - Query of static alarm information



## 2.3.2 SBIs

Using SBIs, NCE can interconnect with physical-layer network devices and other management and control systems to implement management and control functions.

The transport devices that NCE can manage include the MSTP, WDM, and RTN series.

**Table 2-15** SBI functions supported by transport devices

SBI Type	Description	Supported Transport Devices
Qx	<p>A Qx interface is a private communication interface simplified based on ITU-T Q3 interface regulations and works in compliance with the standard TCP/IP management protocol. It can transmit data through inband DCC/ECC or outband communication medium and features fewer overheads, standard structure, and high efficiency. NCE automatically adapts to different protocol types.</p>	All transport devices
TFTP/FTP/SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"> <li>• TFTP is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text.</li> <li>• FTP is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text.</li> <li>• SFTP uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission.</li> </ul> <p>Transport NEs use NE Software Management to implement functions such as NE upgrades, backup, and patch installation.</p>	All transport devices
Syslog	<p>The Syslog SBI serves as an interface for NCE to receive system logs from NEs. With the Syslog SBI, NCE can manage NE logs.</p> <p>Transport NEs support NE security logs.</p>	All transport devices

SBI Type	Description	Supported Transport Devices
NETCONF	<ul style="list-style-type: none"> <li>• NETCONF is used to manage network data device configurations. This protocol is designed to supplement the SNMP and Telnet protocols for network configuration.</li> <li>• NETCONF defines a simple mechanism for installing, manipulating, and deleting the configurations of network devices. NETCONF uses XML-based data encoding for the configuration data and protocol messages. In an automatic network configuration system, NETCONF plays a crucial role.</li> </ul>	<p>The OTN series based on the VRP V8 platform.</p> <p>The RTN NEs that support the SDN technology are supported.</p>
OSPF/ OSPF-TE	<ul style="list-style-type: none"> <li>• OSPF is used to obtain the topology information of TSDN NEs.</li> <li>• OSPF-TE is used to obtain TE link information.</li> </ul>	<p>Only WDM NEs that support the TSDN technology are supported</p>
PCEP	<p>PCEP implements centralized control of TSDN NEs. NCE functions as the path computation element (PCE), and each TSDN NE functions as a path computation client (PCC). They communicate with each other using PCEP to allow NCE to obtain device resource information, provide the centralized path computation service, and maintain the link status.</p>	<p>Only WDM NEs that support the TSDN technology are supported</p>

SBI Type	Description	Supported Transport Devices
<p><b>NOTE</b></p> <p>The following WDM products versions support the TSDN technology and feature application with the NCE (Transport Domain):</p> <ul style="list-style-type: none"> <li>• OSN 9800 V100R005C00 and later versions</li> <li>• OSN 9600 V100R005C00 and later versions</li> <li>• OSN 8800 V100R011C10 and later versions</li> <li>• OSN 1800 V V100R007C00 and later versions (with TNZ5UXCMS as the system control board)</li> <li>• OSN 1800 II E V100R008C10 and later versions (with TNZ2UXCL as the system control board)</li> <li>• OSN 1800 I E V100R009C00 and later versions (with TMA1UXCL as the system control board)</li> <li>• OSN 902 V100R002C10</li> </ul> <p>The following RTN products versions support the SDN technology and feature application with the NCE (Transport Domain):</p> <ul style="list-style-type: none"> <li>• OptiX RTN 310 V100R019C10SPC120 version</li> <li>• OptiX RTN 320 V100R019C10SPC120 version</li> <li>• OptiX RTN 380 V100R019C10SPC120 version</li> <li>• OptiX RTN 380A V100R019C10SPC120 version</li> <li>• OptiX RTN 380AX V100R019C10SPC120 version</li> <li>• OptiX RTN 380H V100R019C10SPC120 version</li> <li>• OptiX RTN 905 V100R019C10SPC120 version</li> <li>• OptiX RTN 950 V100R019C10SPC120 version</li> <li>• OptiX RTN 950A V100R019C10SPC120 version</li> <li>• OptiX RTN 980 V100R019C10SPC120 version</li> </ul>		

The IP devices that NCE can manage include NE series routers, CX series routers, Ethernet switches, BRASs, ATN devices, and security devices.

**Table 2-16** SBI functions supported by IP devices

SBI Type	Description	Supported IP Devices
SNMP	<p>SNMP is a TCP/IP-based network management protocol at the application layer. SNMP uses the UDP protocol at the transmission layer. Through the SNMP SBI, NCE can manage network devices that support agent processes.</p> <p>NCE supports the SNMP SBI that complies with SNMPv1, SNMPv2c, and SNMPv3. Through the SNMP SBI, NCE can connect to devices. The SNMP SBI supports basic management functions such as auto-discovery of network devices, service configuration data synchronization, fault management, and performance management.</p>	All IP devices
Telnet/ STelnet	<p>The Telnet and STelnet SBIs are a basic type of interface used for remote login to and management of NEs. The Telnet and STelnet SBIs address the disadvantages of the SNMP SBI and allow NCE to provide more management functions.</p> <ul style="list-style-type: none"><li>• Telnet is a TCP/IP-based network management protocol at the application layer. Through the Telnet SBI, users can log in to an NE in the CLI and run commands directly in the CLI to maintain and configure the NE. Using the TCP protocol at the transmission layer, the Telnet protocol provides services for network communication. The Telnet protocol transmits communication data in plain text, which is not secure.</li><li>• STelnet provides secure Telnet services based on SSH connections. Providing encryption and authentication, SSH protects NEs against attacks of IP address spoofing.</li></ul>	All IP devices

SBI Type	Description	Supported IP Devices
TFTP/FTP/SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"><li>• TFTP is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text.</li><li>• FTP is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text.</li><li>• SFTP uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission.</li></ul> <p>Routers and switches whose VRP version is 5.7 or later use the TFTP, FTP, or SFTP SBI to synchronize data with NCE. IP NEs use NE Software Management to implement functions such as NE upgrades, backup, and patch installation.</p>	All IP devices
Syslog	<p>The Syslog SBI serves as an interface for NCE to receive system logs from NEs. With the Syslog SBI, NCE can manage NE logs. IP NEs support Syslog running logs.</p>	All IP devices
ICMP	<p>ICMP is a network-layer protocol. It provides error reports and IP packet processing messages that will be sent back to the source. ICMP is usually used as an IP-layer or higher-layer protocol and ICMP packets are usually encapsulated in IP packets for transmission. Some ICMP packets carry error packets that will be sent back to NEs.</p>	All IP devices

SBI Type	Description	Supported IP Devices
NETCONF	<ul style="list-style-type: none"> <li>NETCONF is used to manage network data device configurations. This protocol is designed to supplement the SNMP and Telnet protocols for network configuration.</li> <li>NETCONF defines a simple mechanism for installing, manipulating, and deleting the configurations of network devices. NETCONF uses XML-based data encoding for the configuration data and protocol messages. In an automatic network configuration system, NETCONF plays a crucial role.</li> </ul>	Only the routers (NE series and CX series) based on the VRP V8 platform
NetStream	NetStream is a network traffic collection protocol based on UDP transmission, which reports network traffic collection results to Analyzer. By using this protocol, Analyzer can be aware of the volume, source, and destination of network traffic.	Only ATN series, CX series, ETN series, ME series, NE series and PTN series devices
Telemetry	Telemetry is an efficient performance data collection technology. It uses efficient data formats and transmission modes such as Google Protocol Buffer (GPB) and gRPC Remote Procedure Calls (gRPC), collects data by means of subscription and push, and supports seconds-level data sampling.	Only ATN series, CX series, ETN series, MA series, ME series, NE series, PTN series and VNE series devices
PCEP	PCEP is used by the controller to control tunnel paths on forwarders in MPLS network optimization scenarios.	Only NE series, CX series, ATN series and PTN series devices
BGP-LS	BGP-LS is used by the SDN controller to collect network topology information from forwarders. The router collects information such as network topology, bandwidth, and packet loss using IGP (such as OSPF and IS-IS), and then sends the information to the SDN controller using BGP-LS. Then the SDN controller computes service paths based on the information.	
BGP FlowSpec	BGP FlowSpec routes are new BGP routes and carry traffic matching rules and actions. The SDN controller delivers BGP FlowSpec routes to forwarders to implement traffic optimization.	

SBI Type	Description	Supported IP Devices
BGP RPD	BGP-Route Policy Distribute (RPD) is used by the SDN controller to send traffic optimization policy routes to forwarders in inbound traffic optimization scenarios.	

The access devices that NCE can manage include DSLAM, MSAN, OLT, MDU, ONT devices.

**Table 2-17** SBI functions supported by access devices

SBI Type	Description	Supported Access Devices
SNMP	<p>SNMP is a TCP/IP-based network management protocol at the application layer. SNMP uses the UDP protocol at the transmission layer. Through the SNMP SBI, NCE can manage network devices that support agent processes.</p> <p>NCE supports the SNMP SBI that complies with SNMPv1, SNMPv2c, and SNMPv3. Through the SNMP SBI, NCE can connect to devices. The SNMP SBI supports basic management functions such as auto-discovery of network devices, service configuration data synchronization, fault management, and performance management.</p>	FTTx series (except ONT), DSLAM, MSAN series NEs
Telnet/STelnet	<p>The Telnet and STelnet SBIs are a basic type of interface used for remote login to and management of NEs. The Telnet and STelnet SBIs address the disadvantages of the SNMP SBI and allow NCE to provide more management functions.</p> <ul style="list-style-type: none"> <li>Telnet is a TCP/IP-based network management protocol at the application layer. Through the Telnet SBI, users can log in to an NE in the CLI and run commands directly in the CLI to maintain and configure the NE. Using the TCP protocol at the transmission layer, the Telnet protocol provides services for network communication. The Telnet protocol transmits communication data in plain text, which is not secure.</li> <li>STelnet provides secure Telnet services based on SSH connections. Providing encryption and authentication, SSH protects NEs against attacks of IP address spoofing.</li> </ul>	FTTx series (except ONT), DSLAM, MSAN series NEs

SBI Type	Description	Supported Access Devices
TFTP/FTP/SFTP	<p>TFTP, FTP, and SFTP are TCP/IP-based network management protocols at the application layer and are dependent on the UDP protocol.</p> <ul style="list-style-type: none"> <li>• TFTP is a simple and low-overhead protocol (as compared with FTP and SFTP) used to upload and download files. The TFTP protocol does not support password configuration and transfers file contents in plain text.</li> <li>• FTP is a set of standard protocols used for transferring files on networks. The FTP protocol transfers passwords and file contents in plain text.</li> <li>• SFTP uses the SSH protocol to provide secure file transfer and processing. For data backup using the SFTP protocol, passwords and data are encrypted during transmission.</li> </ul> <p>Access NEs use the TFTP, FTP, or SFTP SBI to synchronize data with NCE, and use NE Software Management to implement functions such as NE upgrades, backup, and patch installation.</p>	All access devices
Syslog	The Syslog SBI serves as an interface for NCE to receive system logs from NEs. With the Syslog SBI, NCE can manage NE logs. Access NEs support Syslog operation logs.	FTTx series (except ONT), DSLAM, MSANseries NEs
ICMP	ICMP is a network-layer protocol. It provides error reports and IP packet processing messages that will be sent back to the source. ICMP is usually used as an IP-layer or higher-layer protocol and ICMP packets are usually encapsulated in IP packets for transmission. Some ICMP packets carry error packets that will be sent back to NEs.	FTTx series (except ONT), DSLAM, MSANseries NEs
NETCONF	<ul style="list-style-type: none"> <li>• NETCONF is used to manage network data device configurations. This protocol is designed to supplement the SNMP and Telnet protocols for network configuration.</li> <li>• NETCONF defines a simple mechanism for installing, manipulating, and deleting the configurations of network devices. NETCONF uses XML-based data encoding for the configuration data and protocol messages. In an automatic network configuration system, NETCONF plays a crucial role.</li> </ul>	Access devices that requires controller



SBI Type	Description	Supported Access Devices
MQTT	MQTT is a TCP/IP-based network management protocol at the application layer. MQTT uses the TCP protocol at the transmission layer. It can manage network devices that support agent processes. NCE manages the home gateway through the Message Queuing Telemetry Transport (MQTT) protocol.	ONT series NEs
Telemetry	Telemetry is used to remotely collect data from physical devices or virtual devices at a high speed, and collects online and offline information about home broadband subscribers on the BRAS in real time.	Only Huawei BRASs

## 2.4 Southbound DCN Networking

NCE and each managed device communicate with each other through the internal data communication network (DCN) or external DCN. The two modes can also be used together for DCN networking.

### NOTE

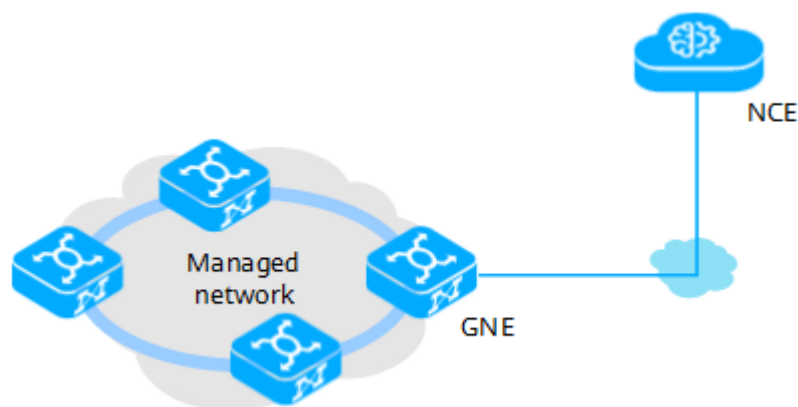
For details about the bandwidth requirements of the southbound DCN, see [4.4 Bandwidth Configurations](#).

### Internal DCN Networking

In internal DCN networking, NCE uses the communication channels provided by managed devices to transmit management and control information and implement network management and control.

In this mode, the managed network is generally divided into multiple DCN subnets. NCE directly communicates with one NE in each subnet called the gateway NE (GNE). The communication between NCE and the other NEs in the subnet is forwarded by the GNE. If NCE and the GNE are in the same equipment room, they can be connected through LAN; otherwise, they need to be connected through private lines.

**Figure 2-6** Internal DCN networking



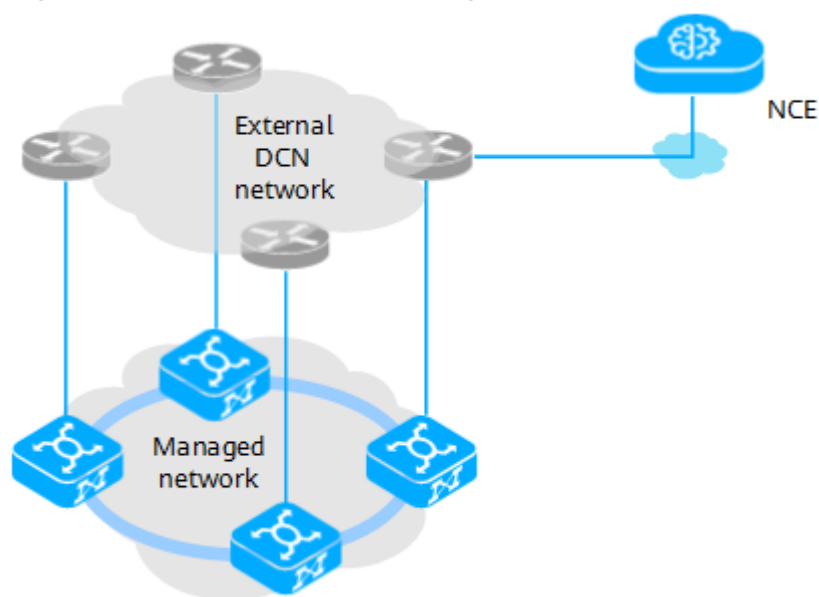
Internal DCN networking has the following characteristics:

- Advantages: Internal DCN networking is flexible, device-independent, and cost-effective.
- Disadvantages: When a network fault occurs and the communication channel between NCE and the managed network is interrupted, NCE cannot maintain the related devices.

## External DCN Networking

In external DCN networking, NCE uses the communication channels provided by intermediate devices on an external DCN network to transmit management and control information to managed devices and implement network management and control. Generally, the managed devices connect to the external DCN through the management ports on their system control boards.

**Figure 2-7** External DCN networking



External DCN networking has the following characteristics:

- Advantages: External DCN networking allows NCE to connect to the managed network through other devices. When a managed device is faulty, the device will not be unreachable from NCE due to the fault of the managed device.
- Disadvantages: External DCN networking requires the construction of an independent maintenance network that provides no service channels, which makes network deployment expensive.

# 3 Deployment Schemes

---

Based on whether Huawei provides E2E support for software and hardware, NCE supports two deployment modes: on-premises and private cloud.

## 3.1 Deployment on Private Clouds

Deployment on private clouds means that customers prepare the bottom-layer deployment environment according to the NCE configuration requirements and Huawei install OS and NCE in this environment.

## 3.2 EasySuite Deployment Tool

In the on-premises and private cloud scenarios where factory installation is not performed, EasySuite is used to install and deploy NCE.

## 3.1 Deployment on Private Clouds

Deployment on private clouds means that customers prepare the bottom-layer deployment environment according to the NCE configuration requirements and Huawei install OS and NCE in this environment.

### Single Site and DR System

Based on different system protection expectations, deployment on private clouds can be divided to two modes: single site and DR.

- Single site: A complete set of NCE is deployed in a place with internal protection enabled.
- DR system: Two sets of NCE with the same installation solution are deployed in two places to form a DR system. In addition to the internal protection of a single site, the two sets of NCE protect each other.

**Figure 3-1** NCE system networking (private cloud, single site)

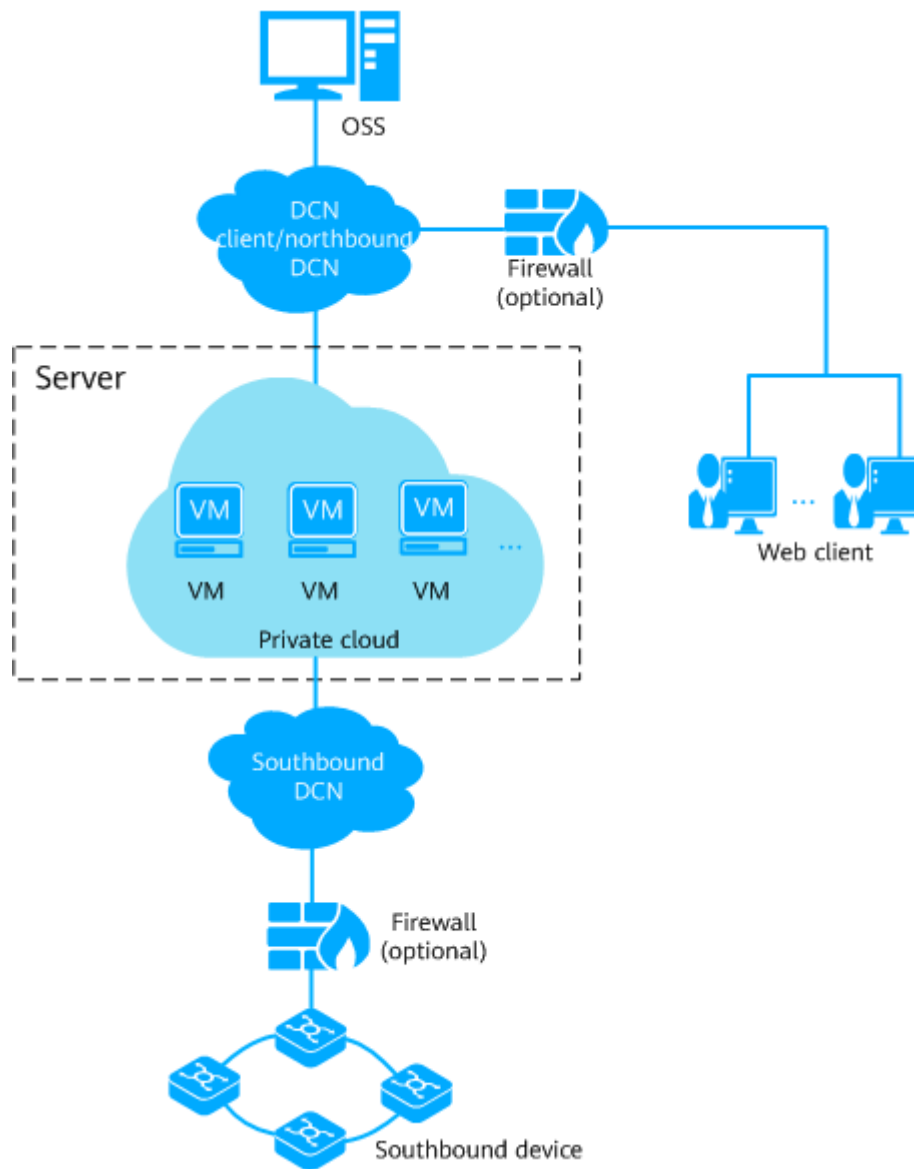
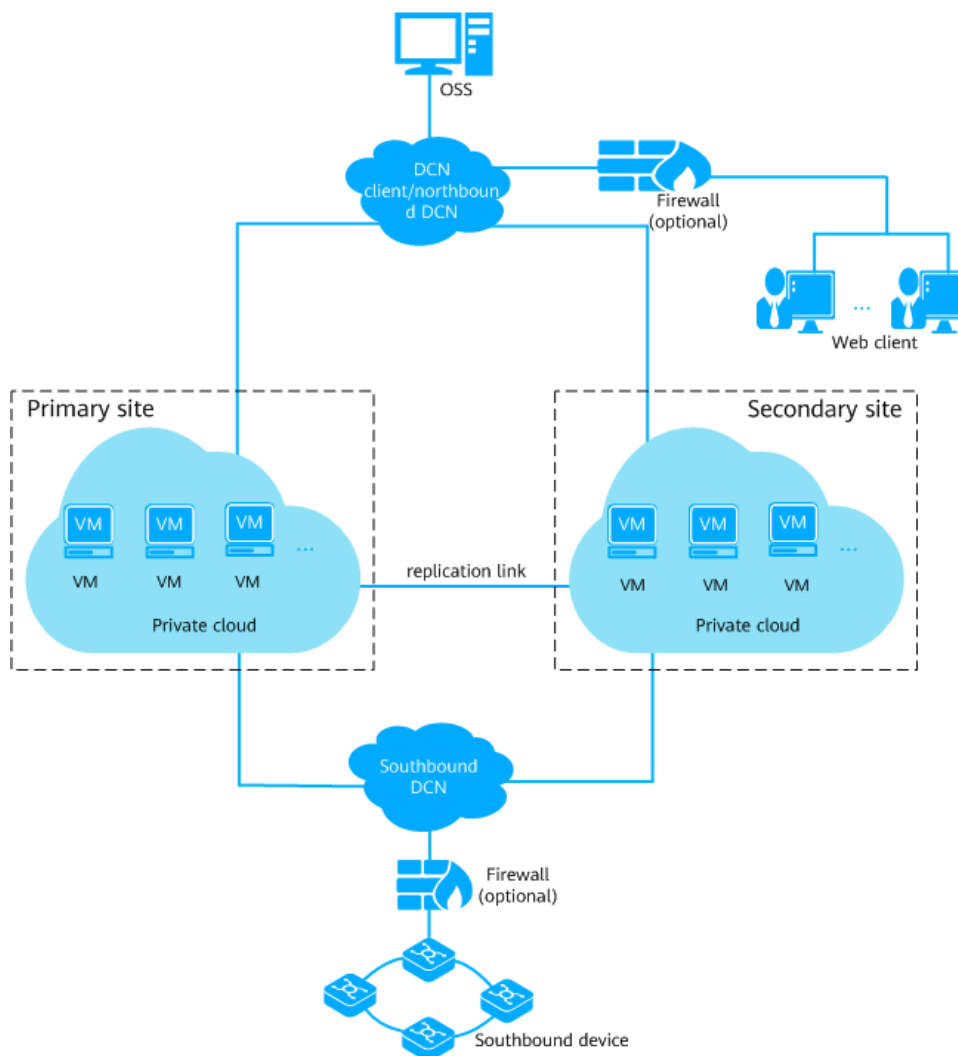


Figure 3-2 NCE system networking (private cloud, DR)



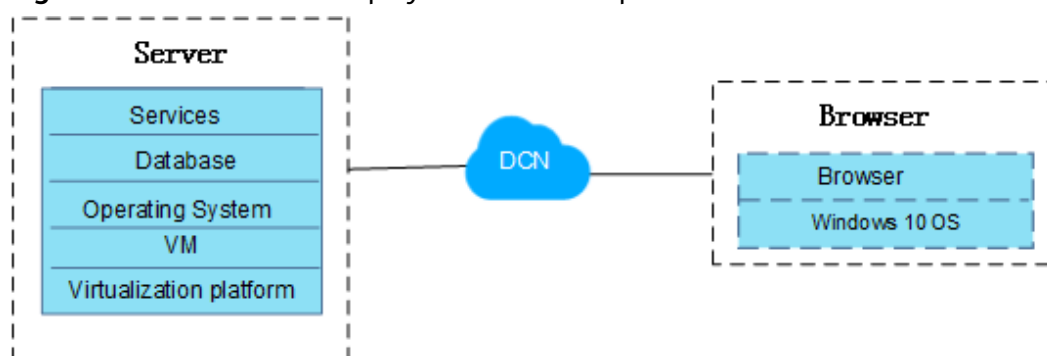
**NOTE**

The DR system requires high bandwidth. A replication link must be configured between the primary and secondary sites.

## Software Deployment Mode

NCE uses the B/S architecture for software deployment during deployment on private clouds. You can easily access NCE through a browser without installing traditional clients.

**Figure 3-3** NCE software deployment mode on private clouds



## 3.2 EasySuite Deployment Tool

In the on-premises and private cloud scenarios where factory installation is not performed, EasySuite is used to install and deploy NCE.

### Basic Concept

EasySuite is a green web-based engineering tool provided by Huawei. It covers complex engineering scenarios such as planning, installation, and migration. Using EasySuite to create an NCE installation project simplifies installation and deployment operations and improves efficiency.

### Operations in Each Installation Scenario

**Table 3-1** Deployment operations on EasySuite

Deployment Solution	EasySuite One-Click Installation
On-premises deployment on physical machines	<ol style="list-style-type: none"> <li>1. Configure hardware, including configuring RAID and hardware alarm reporting parameters.</li> <li>2. Install and configure the OS.</li> <li>3. Install NCE, including installing the database.</li> </ol>
Deployment on private clouds	<ol style="list-style-type: none"> <li>1. (Optional) Install VMs, including installing and configuring the OS.</li> <li>2. Install NCE, including installing the database.</li> </ol>

# 4 Configuration Requirements

NCE has specific requirements on the hardware, software, client, and bandwidth to ensure the stable running of the system.

## [4.1 Configurations for Deployment \(Only Product, SUSE\)](#)

### [4.2 Server Software Configurations](#)

### [4.3 Client Configurations](#)

### [4.4 Bandwidth Configurations](#)

## 4.1 Configurations for Deployment (Only Product, SUSE)

**Table 4-1** Hardware resources required for physical machine deployment of NCE Manager

Service Scenario	Network Scale	CPU	RAM (GB)	Storage (GB)	NIC
NCE Manager (single domain)	< 2000 equivalent NEs	2.0 GHz, 16 cores	64	500	1 x 4 GE
	< 6000 equivalent NEs (only for NCE (Transport Domain))	2.0 GHz, 40 cores	128	700	1 x 4 GE
	< 6000 equivalent NEs (only for NCE (Access Domain))	2.0 GHz, 12 cores	128	600	1*4 GE



**Table 4-2** VM resources required for private cloud deployment of NCE Manager

Service Scenario	Network Scale	VMs	vCPUs	Memory (GB)	Storage (GB)	IOPS
Manager (single domain)	2000–6,000 equivalent NEs	2	2.0 GHz, 40 Core	128	700	2000
	6,000–15,000 equivalent NEs	2	2.0 GHz, 48 Core	192	750	2500
	15,000–30,000 equivalent NEs	2	2.0 GHz, 72 Core	288	800	3500

## 4.2 Server Software Configurations

**Table 4-3** Server software configuration requirements (Manager, X86, SUSE)

Item	Type	Version	Remarks
Compatible software configurations	OS	<ul style="list-style-type: none"> <li>SUSE Linux Enterprise Server 12 SP5</li> <li>SUSE Linux Enterprise Server 12 SP4</li> </ul>	Used in the suse compatible deployment scenario.
	Data base	GaussDB T V3	

## 4.3 Client Configurations

**Table 4-4** Client configuration requirements

Type	Requirements
PC	Minimum Configuration: <ul style="list-style-type: none"> <li>CPU: 2 Core, 2.6GHz</li> <li>Memory: 4GB</li> <li>Hard disk: 8GB</li> </ul> Recommended Configuration: <ul style="list-style-type: none"> <li>CPU: 4 Core, 3.1GHz</li> <li>Memory: 8GB</li> <li>Hard disk: 8GB</li> </ul>

Type	Requirements
Cloud Desktop	Minimum Configuration: <ul style="list-style-type: none"> <li>● CPU: 4 Core, 2.6GHz</li> <li>● Memory: 4GB</li> <li>● Hard disk: 8GB</li> </ul> Recommended Configuration: <ul style="list-style-type: none"> <li>● CPU: 6 Core, 3.1GHz</li> <li>● Memory: 8GB</li> <li>● Hard disk: 8GB</li> </ul>
OS	Windows 10 (32-bit or 64-bit)
Language	<ul style="list-style-type: none"> <li>● Simplified Chinese</li> <li>● English</li> </ul>
Web browser	<ul style="list-style-type: none"> <li>● Recommended:                             <ul style="list-style-type: none"> <li>- Google Chrome 70 or later (32-bit or 64-bit)</li> <li>- Firefox ESR 61.0.1 or later (32-bit or 64-bit)</li> </ul> </li> <li>● Compatible:                             <ul style="list-style-type: none"> <li>- Google Chrome 57 or later (32-bit or 64-bit)</li> <li>- Firefox ESR 52 or later (32-bit or 64-bit)</li> </ul> </li> </ul> <p><b>NOTE</b></p>
Resolution	1366 x 768 px or higher; recommended resolution: 1920 x 1080 px <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● Zoom ratio of the browser: 100% is recommended and 80% to 200% is compatible.</li> <li>● If the resolution is within the compatibility scope of the browser, functions are available but the layout may not be user-friendly. If the resolution is not within the compatibility scope of the browser, both the functions and layout are affected.</li> </ul>

## 4.4 Bandwidth Configurations

**Table 4-5** Bandwidth configuration requirements for NCE (Transport Domain), NCE (Access Domain), or NCE (IP Domain)

Type	Requirements
Network delay	<ul style="list-style-type: none"><li>• Between NCE and external systems (client, NE, and third-party arbitration site): &lt; 50 ms</li><li>• Between NCE and OSS: &lt; 20 ms</li><li>• Between NCE VM nodes: &lt; 10 ms</li><li>• Between the primary and secondary sites of the DR system: &lt;50 ms (If NCE contains the Controller, it is recommended that the network delay between the primary and secondary sites be less than 20 ms.)</li></ul>
Packet loss rate	<ul style="list-style-type: none"><li>• Between NCE and external systems (client, NE, OSS, and third-party arbitration site): &lt; 1%</li><li>• Between NCE VM nodes: &lt; 0.2%</li><li>• Between the primary and secondary sites of the DR system: &lt; 1% (If NCE contains the Controller, it is recommended that the packet loss rate between the primary and secondary sites be less than 0.1%.)</li></ul>
Bandwidth between VMs	≥1000 Mbit/s

Type	Requirements
Bandwidth between the server and clients	<p>Bandwidth for communication between the server and clients = Bandwidth between each client and the server x Number of clients x Coefficient:</p> <ul style="list-style-type: none"> <li>• The bandwidth between each client and the server is 10 Mbit/s, which is the maximum bandwidth required by a single client.</li> <li>• Number of clients: Plan the number of concurrent online clients based on the customer requirements. For example, if the management scale is 15,000 equivalent NEs, a maximum of 100 clients can be online at the same time. However, the customer may require a maximum of 64 clients to be online at the same time.</li> <li>• Coefficient: Generally, not all online clients require the maximum bandwidth of 10 Mbit/s. The recommended coefficient is 0.4 based on the empirical value of the maximum bandwidth required by 20% online clients.</li> </ul> <p><b>NOTE</b> In extreme scenarios where the 30,000 equivalent NEs are deployed on the Manager and the client/northbound network, southbound network, and DR network share the same network plane, the calculated total bandwidth may exceed the maximum bandwidth supported by the GE electrical ports on the server. Considering that the maximum bandwidth does not occur on all networks for communication at the same time, it is recommended that the total bandwidth be 1000 Mbit/s.</p>
Bandwidth between the server and OSS	<p>The bandwidth between each OSS and the NCE NBI is 10 Mbit/s or above.</p> <p>Bandwidth for communication between the server and OSSs = Bandwidth for communication between the server and each OSS × Number of OSSs For example, if three OSSs are connected to the REST NBI of the same NCE, the required bandwidth is 3 x 10 Mbit/s or above. If there are two OSSs, one is connected to the REST NBI of NCE, and the other is connected to the SNMP NBI of NCE, the required bandwidth is 10 Mbit/s +10 Mbit/s or above.</p>

Type	Requirements
Bandwidth between the server and NEs	<p>The Manager have different bandwidth requirements. The required minimum bandwidth is the sum of bandwidths for deploying the Manager, Controller, and Analyzer.</p> <ul style="list-style-type: none"> <li>Manager bandwidth CIR: <math>N &gt; 56</math>: 2048 kbit/s + <math>(N - 56) \times 0.5</math> kbit/s; <math>N \leq 56</math>: 2 Mbit/s PIR: <math>N &gt; 56</math>: 10240 kbit/s + <math>(N - 56) \times 5</math> kbit/s; <math>N \leq 56</math>: 10 Mbit/s</li> </ul> <p>In different networks, the 2 Mbit/s bandwidth may not meet the bandwidth requirement on the live network. In this case, you can use formulas to determine the CIR and PIR. Network-wide data synchronization, performance data collection, and batch upgrade require high bandwidth. Therefore, it is recommended that the live network bandwidth meet the PIR requirement.</p> <p><b>NOTE</b> N indicates the number of equivalent NEs.</p>
Bandwidth between the primary and secondary sites of the DR system (Manager)	<p>In a DR system, a replication private line is established between the primary and secondary sites for real-time data synchronization. The bandwidth requirements vary according to scenarios.</p> <ul style="list-style-type: none"> <li>Bandwidth planning for the scenario where performance data collection is not enabled on the NCE Manager: <a href="#">Table 4-6</a></li> <li>Bandwidth planning for the scenario where SNMP performance data collection is enabled on the NCE Manager: <a href="#">Table 4-7</a></li> <li>Bandwidth planning for the scenario where transport NE performance data collection is enabled on the NCE Manager: <a href="#">Table 4-8</a></li> </ul>
Bandwidth between the DR system and the third-party arbitration site	$\geq 2$ Mbit/s

**Table 4-6** Bandwidth between the primary and secondary sites of the NCE Manager DR system (without performance data collection)

Network Scale	Minimum Bandwidth	Recommended Bandwidth
< 2000 equivalent NEs	8 Mbit/s	12 Mbit/s
2000–6000 equivalent NEs	12 Mbit/s	30 Mbit/s

Network Scale	Minimum Bandwidth	Recommended Bandwidth
6000–15,000 equivalent NEs	30 Mbit/s	60 Mbit/s
15,000–30,000 equivalent NEs	60 Mbit/s	100 Mbit/s

**Table 4-7** Bandwidth between the primary and secondary sites of the NCE Manager DR system (with SNMP performance data collection)

Network Scale	Performance Collection Capability with Max/Min Data Aggregation Disabled (Unit: Max Equivalent Records/15 Minutes)	Minimum Bandwidth	Recommended Bandwidth
< 2000 equivalent NEs	20000	12 Mbit/s	20 Mbit/s
2000–6000 equivalent NEs	60000	24 Mbit/s	60 Mbit/s
6000–15,000 equivalent NEs	150000	56 Mbit/s	100 Mbit/s
15,000–30,000 equivalent NEs	150000	88 Mbit/s	200 Mbit/s

**Table 4-8** Bandwidth between the primary and secondary sites of the NCE Manager DR system (with transport NE performance data collection)

Network Scale	Minimum Bandwidth	Recommended Bandwidth
< 2000 equivalent NEs (number of performance monitoring instances: 20,000)	12 Mbit/s	20 Mbit/s
2000–6000 equivalent NEs (number of performance monitoring instances: 40,000)	18 Mbit/s	60 Mbit/s
6000–15,000 equivalent NEs (number of performance monitoring instances: 80,000)	40 Mbit/s	100 Mbit/s
15,000–30,000 equivalent NEs (number of performance monitoring instances: 100,000)	72 Mbit/s	200 Mbit/s

# 5 Functions and Features

---

NCE user-facing scenarios provide cloud-based network management, control, and analysis optimization.

[5.1 System and Common Functions](#)

[5.2 Network Management](#)

## 5.1 System and Common Functions

### 5.1.1 System Management

NCE interconnects with southbound systems quickly and achieves Single Sign On (SSO) to O&M interfaces. It supports global configuration in terms of Network Time Protocol (NTP) time synchronization and license management, software resource capability such as system monitoring and databases, and troubleshooting such as data backup and restore, system health check, and fault locating and data collection. This improves interconnection and management efficiency, helps forecast and detect potential risks in time, facilitates fault rectification, and therefore ensures stable and secure system running.

#### System Interconnection

- **Southbound interconnection:** Integrated with Huawei or third-party systems to quickly access NEs or virtual resources and obtain NE resources, alarm and performance data, and virtual resources required for NCE service provisioning or assurance. This improves interconnection efficiency.
  - Configuring and managing southbound drivers: Before interconnecting NCE with a southbound system, users need to import external drivers by means of driver lifecycle management and configure SNMP parameters so that SNMP alarms can be reported to quickly adapt to NEs and service models (resources, alarms, and performance) of the interconnected system. This achieves quick driver access and improves interconnection efficiency. Users can also query driver types and monitor and delete driver instances for unified driver management.
  - Interconnecting with a southbound system: Users can interconnect NCE with a Huawei or third-party system and update certificates to manage

NEs or virtual resources. After login, users can obtain basic information of the NEs, such as NE and port resources, alarms, and performance data, and collect VM, virtual networks, and virtual NEs. This ensures proper NCE service provisioning and assurance.

- **Single Sign On (SSO):** SSO is an access control policy between NCE and its southbound systems or between the upper-layer system and NCE. With a single login, users can access all mutually trusted systems. This implements seamless O&M interface interconnection between systems and improves O&M efficiency. The SSO system consists of servers and clients. The clients obtain certificates from the servers and deploy them. One server can interconnect with multiple clients to achieve unified authentication. After successfully logging in to the server, users can access all the clients without entering the username and password.

## System Configuration

- **Time synchronization:** NCE nodes are managed and maintained in a unified mode. Therefore, the Coordinated Universal Time (UTC) on each node must be the same to ensure that NCE can properly manage services and data on the nodes. An NTP-based external clock source is required to serve as the NTP server of NCE so that the system time can be adjusted at any time without manual intervention.
  - A maximum of 10 NTP servers can be added on NCE. Only one active NTP server can be configured, and the active NTP server is mandatory. In a disaster recovery (DR) system, the primary and secondary sites must use the same NTP server to ensure time consistency between the two sites.
  - After an active NTP server is configured, the OMP node synchronizes time with the active NTP server preferentially. Service nodes then synchronize time with the OMP node.
  - When the active NTP server fails, NCE selects an available NTP server from the standby NTP servers within 15 minutes and sets it as the active NTP server. If multiple NTP servers configured on NCE become invalid, the OMP node cannot synchronize time with the NTP server, and service nodes will synchronize time with the OMP node.
- **License management:** Updating and maintaining a license allow the system to properly run based on the features, versions, capacity, and validity period authorized in a license file.

License management allows users to initially load, update, and routinely maintain licenses.

- Initially loading a license

After the system is deployed, you need to load a license by importing license files so that you can use the system properly.

- Updating a license

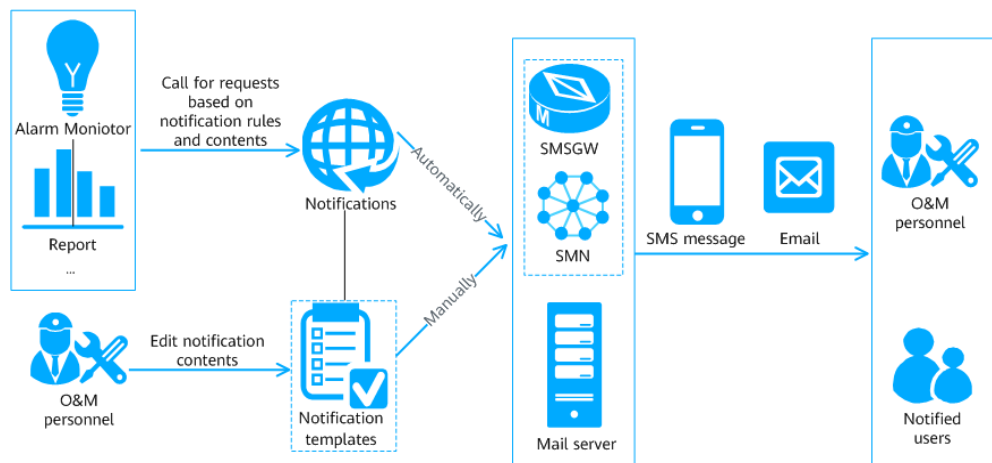
During O&M, you need to update a license file under any of the following conditions:

- The license is about to expire.
- The license has expired.



- The license is invalid.
  - The license control resource items or function control items do not meet service requirements.
  - The software service annual fee in the license is about to expire.
  - The software service annual fee in the license has expired.
- Routine license maintenance
- You need to query license information in the system from time to time, such as the expiration time, consumption, and capacity, so that you can quickly identify and resolve problems (for example, a license is about to expire or its capacity is insufficient).
- **Remote notification:** When O&M personnel are not on site due to business travel or off duty and cannot query significant alarms and service reports, remote notification is used to send SMS messages and emails to the O&M personnel.

**Figure 5-1** Remote notification methods



- Automatic and manual modes are supported.
- Automatic mode: The O&M personnel set the message content and message sending rules. Then, NCE automatically sends alarms and reports to relevant personnel in the form of SMS messages or emails through the short message service gateway (SMSGW) or mail server connected to NCE.
  - Manual mode: The O&M personnel manually edit message contents to be sent or use preset notification templates, and trigger NCE to send SMS messages and emails to relevant personnel so that they can obtain information about the alarms and reports.
- The notifications can be sent by SMS message or email.

**Table 5-1** Remote notification modes

Form	Sent By	Description
SMS message	SMSGW	A third-party SMSGW is used, and it is maintained by O&M personnel from the customer network.  Notifications allow O&M personnel to use a default SMSGW or reset SMSGW parameters, ensuring successful interconnection between the SMSGW and NCE.
	Simple Message Notification (SMN) server	The SMN server is a Huawei transit server. After SMN is deployed, parameters for interconnecting NCE with SMN can be set. After SMN parameters are set, SMSGW parameter settings will not take effect, and the SMN server will interconnect with the third-party SMSGW.
Email	Mail server	A third-party mail server is used, and it is maintained by O&M personnel from the customer network.  Notifications allow O&M personnel to set parameters for mail servers to establish communication between mail servers and NCE.

## System Monitoring

Global monitoring capability is supported to monitor NCE resource indicators such as services, processes, nodes, and databases. This helps conduct predictive analysis and detect potential risks in time. For key resources, the administrator can set thresholds to trigger alarms and handle exceptions promptly.

- **Service and process monitoring:** Monitors the service running status and indicators such as the CPU usage, memory usage, and number of handles. When a process in a service stops abnormally or becomes faulty, NCE attempts to restart the process. A maximum of 10 consecutive restarts are allowed. If the number is exceeded, an alarm is generated, requesting users to process the exception manually.
- **Node monitoring:** Monitors node indicators such as the CPU, virtual memory, physical memory, and disk partitions. If any resource of the node encounters an exception, the node is displayed as abnormal. If a key resource remains abnormal within a sampling period, an alarm is generated.
- **Database monitoring:** Monitors database indicators such as the space, memory, and disks. If any resource of the database encounters an exception, the database is displayed as abnormal. If a key resource remains abnormal within a sampling period, an alarm is generated.

## System Maintenance

- **System backup and restore:** Backs up and restores the dynamic data, OS, database, management plane, or application software of NCE. Data is backed

up in a timely manner. If any backup object is abnormal, you can use the corresponding backup file to recover the object to the normal state.

- **O&M management:** Provides system maintenance and management functions to help O&M personnel learn the health status of the system during system running and reduce running risks. If a system fault occurs, fault information can be collected for fault demarcation and locating to facilitate repair and reduce losses.
  - Health check: Checks and evaluates hardware, OSs, databases, networks, and NCE services to learn the health status, detect abnormal check items, and determine whether operation or running risks exist in NCE.
  - Data collection: Provides data collection templates based on fault scenarios, services, and directories. When a system fault occurs, O&M personnel can collect logs and database tables as required and analyze and locate the fault.
  - Quick fault demarcation: Each service operation in the system is implemented by invoking one or more services. During service operations, the system automatically collects statistics on service operation status, memory usage, and CPU usage for O&M personnel to quickly demarcate faults and analyze resource consumption.
  - Quick fault locating: This function provides default locating templates for automatic fault locating. O&M personnel select templates based on fault scenarios. This helps O&M personnel quickly obtain solutions and shorten the fault locating time.
  - System guard: System guard forwards critical and major alarms and alarms (including common alarms, OS alarms, hardware server alarms, and OMP alarms) that potentially affect the stable running of NCE from the O&M plane to the management plane, and displays a pop-up window to remind O&M personnel to view alarm details and handle alarms in a timely manner on the System Guard page, ensuring the normal running of NCE.
  - Unified Monitoring: The unified monitoring function monitors the real-time and historical data of NCE and compares and analyzes the data in multiple dimensions to provide data reference for O&M personnel.

## Help System

NCE provides a layered design for the help system adapting to user needs in diverse scenarios. The help system supports anytime, anywhere, and on-demand learning. A variety of help forms such as tooltips, panels, question mark tips, and Information Center are provided. All necessary information is directly displayed on the GUI. Information that is closely related to the current operation is folded. You can expand the information if necessary. Systematic learning information is placed in the Information Center.





### 5.1.2 Alarm Management

Alarm Management enables O&M personnel to centrally monitor NE, system services, and third-party system alarms and quickly locate and handle network faults, ensuring normal network operation.

## Alarm Severity

Alarm severities indicate the severities of faults. Alarms need to be handled depending on their severity. Alarm severities can also be redefined, as shown in [Table 5-2](#).

**Table 5-2** Alarm severities

Alarm Severity	Color	Description	Handling Policy
Critical		Services are affected. Corrective measures must be taken immediately.	The fault must be rectified immediately. Otherwise, services may be interrupted or the system may break down.
Major		Services are affected. If the fault is not rectified in a timely manner, serious consequences may occur.	Major alarms need to be handled in time. Otherwise, important services will be affected.
Minor		Indicates a minor impact on services. Problems of this severity may result in serious faults, and therefore corrective actions are required.	You need to find out the cause of the alarm and rectify the fault.
Warning		Indicates that a potential or imminent fault that affects services is detected, but services are not affected.	Warning alarms are handled based on network and NE running status.

Different handling policies apply to different alarm severities. You can change the severity of a specific alarm as required.

 **NOTE**

The severity of an alarm needs to be adjusted when the impact of the alarm becomes larger or smaller.

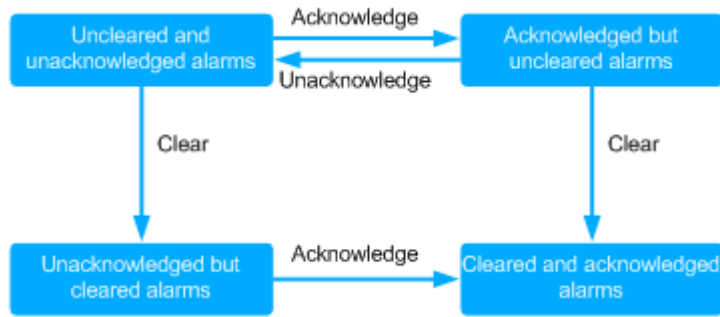
## Alarm Statuses

[Table 5-3](#) lists the alarm statuses. [Figure 5-2](#) lists the alarm status relationship.

**Table 5-3** Alarm statuses

Status Name	Alarm Status	Description
Acknowledgement status	Acknowledged and unacknowledged	<p>The initial acknowledgment status is <b>Unacknowledged</b>. A user who views an unacknowledged alarm and plans to handle it can acknowledge the alarm. When an alarm is acknowledged, its status changes to <b>Acknowledged</b>. Acknowledged alarms can be unacknowledged. When an alarm is unacknowledged, its status is restored to <b>Unacknowledged</b>. You can also configure auto acknowledgment rules to automatically acknowledge alarms.</p>
Clearance status	Cleared and uncleared	<p>The initial clearance status is <b>Uncleared</b>. When a fault that causes an alarm is rectified, a clearance notification is automatically reported to Alarm Management and the clearance status changes to <b>Cleared</b>. For some alarms, clearance notifications cannot be automatically reported. You need to manually clear these alarms after corresponding faults are rectified. The background color of cleared alarms is green.</p>
Maintenance status	Normal and maintenance	<p>The initial maintenance status is <b>Normal</b>. If the alarms are generated during commissioning and are not triggered by faults, you can set filter criteria to filter out maintenance alarms when monitoring or querying alarms.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The maintenance status corresponding to <b>Normal</b> is <b>NORMAL</b>.</li> <li>• The maintenance status corresponding to <b>Maintenance</b> is <b>Maintenance, Invalid status</b>.</li> </ul>

**Figure 5-2 Alarm status relationship**



Acknowledged and cleared alarms are moved to the historical alarm list, and a non-historical alarm is called a current alarm. **Table 5-4** shows the definition of an alarm.

**Table 5-4 Current alarms and historical alarms**

Name	Description
Current alarms	Current alarms include uncleared and unacknowledged alarms, acknowledged but uncleared alarms, and unacknowledged but cleared alarms. When monitoring current alarms, you can identify faults in time, operate accordingly, and notify maintenance personnel of these faults.
Historical alarms	Acknowledged and cleared alarms are historical alarms. You can analyze historical alarms to optimize system performance.

## Alarm and Event Types

**Table 5-5** lists the alarm and event types.

**Table 5-5 Alarm and event**

Name	Description	Differences Between Alarms and Events	Similarities
Alarm	Indicates a notification generated when the system or an MO is faulty.	<ul style="list-style-type: none"> <li>An alarm indicates that an exception or fault occurs in the system or MO. An event is a notification generated when the system or MO is running properly.</li> <li>Alarms must be handled. Otherwise, services will be abnormal due to these exceptions or faults. Events do not need to be handled and are used for analyzing and locating problems.</li> </ul>	Alarms and events are presented to users as notifications.

Name	Description	Differences Between Alarms and Events	Similarities
Event	Indicates a notification of status changes generated when the system or an MO is running properly.	<ul style="list-style-type: none"> <li>Users can acknowledge and clear alarms on the GUI. Users cannot acknowledge or clear events.</li> </ul>	

Alarms or events are displayed on the page when NEs, services, and interconnected third-party systems detect their exceptions or significant status changes. [Table 5-6](#) describes the types of alarms and events.

**Table 5-6** Alarm and event types

Type	Description
Communications alarm	Alarms caused by failures of the communications in an NE, between NEs, between an NE and a management system, or between management systems. Example: device communication interruption alarm
Quality of service alarm	Alarms caused by service quality deterioration. Example: device congestion alarm
Processing error alarm	Alarms caused by software or processing errors. Example: version mismatch alarm
Equipment alarm	Alarms caused by physical resource faults. Example: board fault alarm
Environment alarm	Alarms caused by problems related to the location of a device. Example: smoke alarms generated when smoke occurs in an equipment room
Integrity alarm	Alarms generated when requested operations are denied. Example: alarms caused by unauthorized modification, addition, and deletion of user information
Operation alarm	Alarms generated when the required services cannot run properly due to problems such as service unavailability, faults, or incorrect invocation. Example: service rejection, service exit, and procedural errors.
Physical resource alarm	Alarms generated when physical resources are damaged. Example: alarms caused by cable damage and intrusion into an equipment room

Type	Description
Security alarm	Alarms generated when security issues are detected by a security service or mechanism. Example: authentication failures, confidential disclosures, and unauthorized accesses
Time domain alarm	Alarms generated when an event occurs at improper time. Example: alarms caused by information delay, invalid key, or resource access at unauthorized time
Property change	Events generated when MO attributes change. Example: events caused by addition, reduction, and change of attributes
Object creation	Events generated when an MO instance is created.
Object deletion	Events generated when an MO instance is deleted.
Relationship change	Events generated when MO relationship attributes change.
State change	Events generated when MO status attributes change.
Route change	Events generated when routes change.
Protection switching	Alarms or events caused by the switchover.
Over limit	Alarms or events reported when the performance counter reaches the threshold.
File transfer status	Alarms or events reported when the file transfer succeeds or fails.
Backup status	Events generated when MO backup status changes.
Heart beat	Events generated when heartbeat notifications are sent.

## Alarm Handling Mechanisms

Alarm management provides three alarm handling mechanisms. For details, see [Table 5-7](#).

- Alarm merging rules improve alarm monitoring efficiency.
- Processing of the full current alarm cache is used to control the number of current alarms.
- Alarm dump rules are used to control the storage capacity of the database.



**Table 5-7** Alarm handling mechanisms

Mechanism	Description
Alarm merging rule	<p>To help you improve the efficiency of monitoring and handling alarms, alarm management provides alarm merging rules. Alarms with the same specified fields (such as location information and alarm ID) are merged into one alarm. This rule is used only for monitoring and viewing alarms on the <b>Current Alarms</b> page and takes effect only for current alarms. The specific implementation scheme is as follows:</p> <ul style="list-style-type: none"> <li>• If a newly reported alarm does not correspond to any previous reported alarm that meets the merging rule, the newly reported alarm is displayed as a merged alarm and the value of <b>Occurrences</b> is <b>1</b>.</li> <li>• If the newly reported alarm B and the previous reported alarm A meet the merging rule, alarm B and alarm A are merged into one alarm record and are sorted by clearance status (uncleared alarms are displayed first) and occurrence time in descending order. <ul style="list-style-type: none"> <li>If alarm A is displayed on top, it is still regarded as a merged alarm, and the <b>Occurrences</b> value of the merged alarm increases by one. Alarm B is regarded as an individual alarm.</li> <li>If alarm B is displayed on top, it is regarded as a merged alarm, and the <b>Occurrences</b> value of the merged alarm increases by one. Alarm A is regarded as an individual alarm.</li> </ul> </li> </ul> <p>In the alarm list, click <b>Occurrences</b> of an alarm, you can view the detailed information about the merged alarm and individual alarm.</p> <ul style="list-style-type: none"> <li>• If a merged alarm is cleared, it is converted into an individual alarm. All individual alarms will be sorted by clearance status (uncleared alarms are displayed first) and occurrence time in descending order. The first one is regarded as a merged alarm.</li> <li>• If a merged alarm or individual alarm is cleared and acknowledged, the alarm will be converted to a historical alarm and the value of <b>Occurrences</b> decreases by one.</li> </ul>

Mechanism	Description
Processing of the full current alarm cache	<p>To prevent excessive current alarms from deteriorating system performance, alarm management provides a full-alarm processing rule. When the number of current alarms in the database reaches the upper threshold, alarm management applies the following two rules to move some alarms to the historical-alarm list until the number of alarms falls to 90% of the upper threshold.</p> <ul style="list-style-type: none"><li>• The cleared alarms, acknowledged and uncleared ADMC alarms, acknowledged and uncleared ADAC alarms, and unacknowledged and uncleared alarms are moved to the historical-alarm list in sequence.</li><li>• The first reported alarms are moved to the historical-alarm list by time.</li></ul>
Alarm dump rule	<p>To avoid excessive alarm database data, the system processes events, masked alarms, and historical alarms every two minutes according to the following rules. The dumped alarms or events cannot be queried in the alarm or event list.</p> <ul style="list-style-type: none"><li>• If the database space usage reaches 80%, alarm management dumps the data in the database to files according to the sequence of occurrence time and data table type (event, masked alarm, or historical alarm). When the space usage after dumping reaches 80% of the usage before dumping, the dumping is stopped.</li><li>• The dumped file will be deleted after 180 days.</li><li>• If the total size of the dumped files exceeds 1 GB or the total number of files exceeds 1000, the system deletes the earliest files.</li></ul>

## Alarm Management Functions

Alarm management provides a variety of monitoring and processing rules. You can configure alarms or events to reduce the number of alarms, implement real-time alarm notification, and meet personalized monitoring requirements. Multiple monitoring pages provide users with various and convenient monitoring and processing methods. For routine maintenance of alarm data, a configurable assurance mechanism is provided to prevent reporting of new alarms from being affected when the database is full.

For details about the alarm or event rules that can be configured, see [Table 5-8](#).

**Table 5-8** Configuring alarm or event rules

Function	Description
Configuring alarms or events	<p>Provides alarm rules and visual management GUIs.</p> <ul style="list-style-type: none"> <li>● <b>Masking rule</b> During maintenance, testing, or deployment, the system or MO generates predictable alarms or events that do not need to be concerned and handled. You can set masking rules to mask these alarms or events so that these alarms or events are not displayed on the <b>Current Alarms</b> or <b>Event Logs</b> page. When setting a masking rule, you can choose to discard masked alarms or events, that is, these alarms or events are not saved in the alarm database, or display the masked alarms on the <b>Masked Alarms</b> page.</li> <li>● <b>Severity and type redefinition rule</b> To ensure the smooth running of network devices or key devices in a region, you can set redefinition rules to change the severity and type of alarms or events. For example, if an alarm is considered important, it can be set to a high-level alarm. O&amp;M personnel can then handle it first to provide high-quality network assurance services.</li> <li>● <b>Name redefinition rule</b> Some alarm or event names are technical and difficult to understand. You can redefine alarm or event names as required.</li> <li>● <b>Correlation rule</b> A correlation rule defines correlative relationships between alarms. Correlated alarms are the alarms whose causes are related. Among correlated alarms, one alarm is the root cause of the others. You can customize correlation rules, and enable and disable default correlation rules as required. When monitoring or viewing alarms, you can filter out correlative alarms and focus on only the root alarms that you want to handle.</li> <li>● <b>Intermittent/Toggling rule</b> When the interval between generation and clearance of an alarm is less than a specific period, the alarm is considered as an intermittent alarm. If the number of times that an alarm (with the same ID) is reported by the same alarm source in a specified period reaches the trigger condition, the toggling handling is started. After an intermittent/toggling rule is set, intermittent or toggling alarms can be discarded or masked to reduce interference caused by repetitive alarms.</li> <li>● <b>Aggregation rule</b> Repeated alarms or events are the alarms or events (with the same ID) reported by the same alarm or event source for multiple times. After an aggregation rule is set, the system</li> </ul>

Function	Description
	<p>automatically aggregates the repeated alarms or events reported within the specified period into one alarm. O&amp;M personnel can view the aggregated alarms on the alarm details page.</p> <ul style="list-style-type: none"> <li>● Setting events as ADMC alarms If you want to improve the significance of specific events, you can set them to auto detected manually cleared (ADMC) alarms. This type of alarms cannot be automatically cleared.</li> <li>● Auto acknowledgement rule After an auto acknowledgment rule is set, Alarm Management automatically acknowledges the current alarms in the cleared state according to a specified rule and moves the acknowledged alarms to the historical alarm list.</li> <li>● Northbound filtering rule On the live network, the upper-layer NMS often receives a large number of alarms. Network congestion and breakdown may occur due to overload, and users cannot quickly locate their concerned alarms. To solve this problem, users can set alarm northbound filtering rules in Alarm Management to determine whether to report the alarms that meet the rules to the upper-layer NMS.</li> </ul>
Alarm Notification	<p>Through the alarm notification function, alarm management can send the alarm or event information to you in real time by SMS message or email. In this way, you can learn the alarm or event information in real time during off-work hours and handle important alarms or events in time.</p>

Function	Description
Personalized Monitoring	<p>Alarm management provides multiple display modes or sound prompt rules for alarms and events. You can modify the rules of display mode and sound prompt as required to obtain the latest alarm or event information in different ways.</p> <ul style="list-style-type: none"> <li>• Color settings: You can set colors for different alarm or event severities and colors for selected alarms or events to easily identify the concerned and selected alarms or events.</li> <li>• Alarm sounds: You can set sounds for alarms at different severities to facilitate alarm monitoring.</li> <li>• Font colors: You can set font colors for read and unread alarms to distinguish alarms.</li> <li>• Highlight: If alarms at a severity are not handled within the specified period of time, that is, the alarm status remains unchanged, the alarms are highlighted in the alarm list according to the highlight settings.</li> <li>• Alarm display mode: You can set alarm display modes for alarms at different severities and in different states so that you can quickly identify concerned alarms.</li> <li>• The alarm box can use indicators of different colors and play different sounds based on NE alarm severities. You can set filter criteria for the alarm box. Alarms that match</li> </ul>

For details about how to monitor alarms or events and handle alarms, see [Table 5-9](#).

**Table 5-9** Monitoring alarms or events and handling alarms

Function	Description
Monitoring and Viewing Alarms or Events	<p>O&amp;M personnel can monitor alarms and view alarm or event information in alarm management in real time.</p> <ul style="list-style-type: none"> <li>● Alarm or event list <ul style="list-style-type: none"> <li>– Provides a current alarm list to push alarms to the <b>Current Alarms</b> page. O&amp;M personnel can monitor and handle alarms in real time using the list.</li> <li>– Provides an alarm log list. You can view current and historical alarms. By default, 20,000 alarms can be displayed.</li> <li>– Provides an event log list, which presents the event messages sent by devices to the system. By default, 20,000 events can be displayed.</li> </ul> </li> <li>● Statistics panel <p>On the <b>Current Alarms</b> page, the statistics panel is provided to display the following statistics:</p> <ul style="list-style-type: none"> <li>– <b>Top 10 Alarms:</b> Collects statistics on the top 10 alarms that are most frequently reported.</li> <li>– <b>Duration:</b> Collects statistics on the number of current alarms by duration.</li> <li>– <b>Top 10 Alarm Sources:</b> Collects statistics on the top 10 alarm sources with the largest number of current alarms.</li> <li>– <b>Severity:</b> Collects statistics on the total number of current alarms and the number of current alarms at each alarm severity.</li> <li>– <b>Status:</b> Collects statistics on the number of alarms by acknowledgement and clearance status.</li> </ul> </li> <li>● Alarm or event name group <p>You can add multiple alarm or event names to a name group to perform operations on them at a time.</p> </li> <li>● Object group <p>You can add multiple alarm or event sources to an object group to perform operations on them at a time.</p> </li> <li>● Alarm sounds and indicators <p>When a new alarm is reported, alarm management plays a sound. The alarm indicator that corresponds to the severity of the alarm starts to flash to remind you to handle alarms in a timely manner.</p> </li> <li>● Filter <p>You can set criteria to filter alarms that require special attention.</p> </li> <li>● Browsing alarms by status or severity <p>A page is divided into four areas to display current alarms by status or severity.</p> </li> </ul>

Function	Description
Handling Alarms	<p>You can use alarm management to handle alarms to facilitate troubleshooting. For example, specify alarm handlers and acknowledge or clear alarms. Alarm handling operations are as follows:</p> <ul style="list-style-type: none"> <li>• Viewing alarm details You can obtain key alarm information, including alarm names, repair recommendations, and location information, to facilitate fault diagnosis and troubleshooting.</li> <li>• Manually acknowledging an alarm Acknowledging an alarm indicates that the alarm is traced by a user, and other users do not need to pay attention to it. If you want other users to focus on the alarm again, you can unacknowledge the alarm. Manual alarm acknowledgement and unacknowledgement, and automatic acknowledgement by severity are supported in alarm management.</li> <li>• Recording experience After handling an alarm, the O&amp;M personnel can record the handling experience for future reference in a timely manner.</li> <li>• Manually clearing alarms If an alarm cannot be automatically cleared or the fault is rectified but the alarm is still in uncleared status, you can manually clear the alarm.</li> </ul>

**Table 5-10** describes the routine maintenance functions such as alarm data management.

**Table 5-10** Routine maintenance functions

Function	Description
Performance Optimization and Statistics	<p>By analyzing historical alarms and masked alarms and collecting statistics on the alarm data, you can learn the running status of devices and determine whether rules are properly set, and can also further analyze potential problems in the running of the devices using the statistics data.</p> <ul style="list-style-type: none"> <li>● View historical alarms and masked alarms. By analyzing historical alarms and masked alarms, you can learn device running statuses and determine whether rules are properly configured. <ul style="list-style-type: none"> <li>– Provides a historical alarm list, which displays 20,000 acknowledged and cleared alarms by default.</li> <li>– Provides a masked alarm list. This allows O&amp;M personnel to view masked alarms and determine whether masking rules are properly set. By default, 20,000 events can be displayed.</li> </ul> </li> <li>● Collect statistics on alarm logs. Statistics on alarm data can be collected based on specified criteria and displayed in charts so that you can analyze system faults.</li> </ul>
Managing Alarm or Event Data	<ul style="list-style-type: none"> <li>● Current alarm threshold warning When the number of current alarms reaches the upper limit, the system processes the full current alarm cache and moves current alarms to the historical-alarm list. To prevent important alarms from being moved to the historical alarm list, you can set a threshold for current alarms. When the number of current alarms reaches a specified threshold, an alarm is reported to prompt you to handle the current alarms.</li> <li>● Manually synchronizing alarms After a peer system is disconnected from the current system, alarms of the peer system cannot be reported to the current system. After the connection is restored, the alarms need to be synchronized with the current system to facilitate monitoring.</li> <li>● Current alarm lifecycle You can set the period for saving cleared and acknowledged alarms in the current alarm list to facilitate alarm monitoring.</li> </ul>
Managing Handling Experience	<p>After handling an alarm, record the handling information to the experience database for future reference or guidance. You can import or export experience records.</p>

### 5.1.3 Security Management



Security management involves user permissions, system security policies, and logs. Security management helps protect NCE against unauthorized user logins and therefore ensures system data security.

### 5.1.3.1 User Management

User Management ensures the security of user information and the system. By attaching users to roles and managing the permissions of roles, resource allocation is optimized and permission management is simplified, improving O&M efficiency.

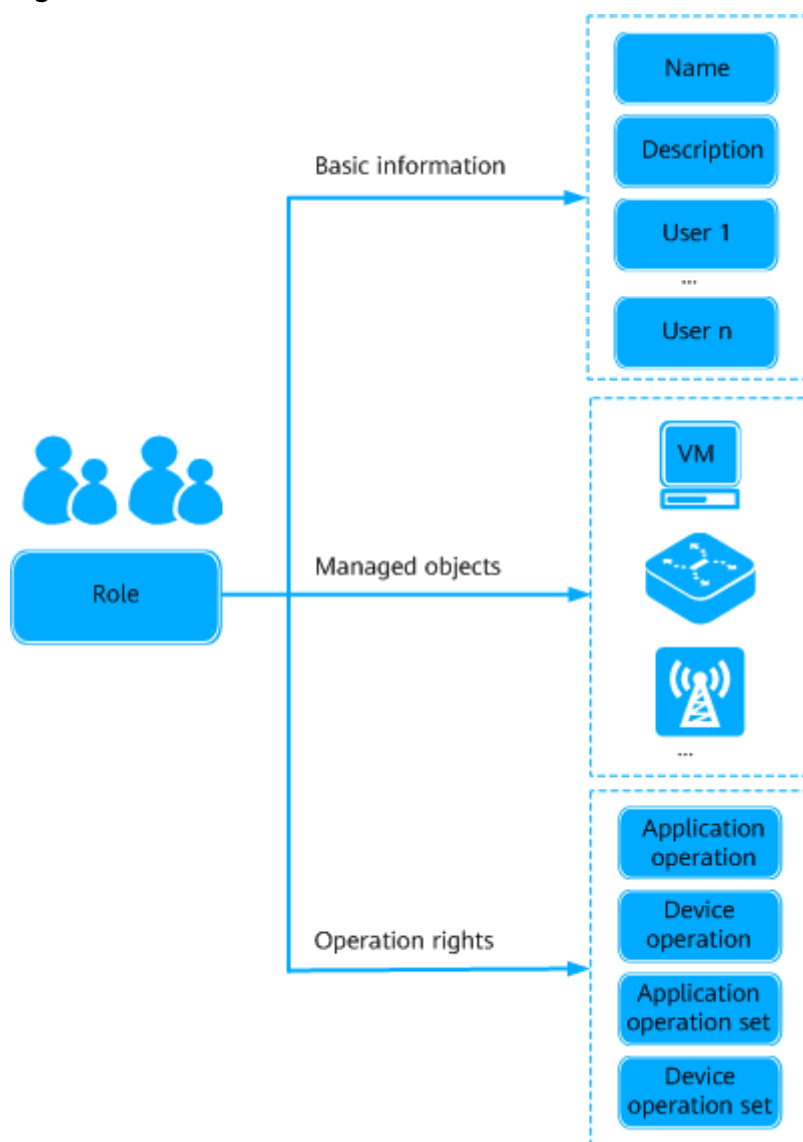
- Role-based authorization minimizes permissions and optimizes resource allocation.
- The permissions and resources in a region are managed by the region administrator, ensuring prompt maintenance of user permissions.
- Most users use the Authentication, Authorization, Accounting (AAA) system to implement centralized user management, authentication, and authorization. After interconnecting with the AAA system through remote authentication configuration, the system authenticates users on the AAA system to ensure that only authenticated users can log in to the system.

### User Management

- User
  - Information about a user includes a user name, password, and permissions.
  - User **admin** is the default user in the system, that is, the system administrator. User **admin** can manage all resources and has all operation rights. This user is attached to both the **Administrators** and **SManagers** roles.
  - The user who has the **User Management** permission in the default region is a security administrator.
  - The **Administrators** role has all the permissions except **User Management**. The user attached to this role is an administrator.
- Role

Users attached to a role have all the permissions granted to the role. You can quickly authorize a user by attaching the user to a role, facilitating permission management. [Figure 5-3](#) shows role information.

Figure 5-3 Role information



Users attached to a role have all the permissions granted to the role and can manage all the resources managed by the role. A user can be attached to multiple roles. If a user is attached to multiple roles, this user has all the permissions granted to the roles and can manage all the resources managed by the roles.

Default roles cannot be deleted and their permissions cannot be modified because the permissions are granted by the system. The system provides the following default roles:

**NOTICE**

Users attached to the **Administrators** or **SMManagers** roles have the operation rights for all resources in the system. Therefore, perform operations using these user accounts with caution. Do not perform any operations affecting system security. For example, do not share or distribute these user names and passwords.

Role Name	Description
Administrators	The user group has all the permissions except <b>User Management, Query Security Log, View Online Users,</b> and <b>Query Personal Security Log</b> . The user attached to this role is an administrator.
SMManagers	The user group has the <b>User Management, License Manager, View Online Users,</b> and <b>Query Security Log</b> permissions.
NBI User Group	The user group has the permission to configure the northbound interfaces such as SNMP, CORBA, XML, OMC, TEXT, and RESTful NBIs.
Guest	The domain of this user group is <b>All Objects</b> , and it has operation rights for default monitor operation sets. They can perform query operations, such as querying statistics, but cannot create or configure objects.
Maintenance Group	The domain of this user group is <b>All Objects</b> , and it has operation rights for default maintenance operation sets. In addition to the rights of the <b>Guests</b> and <b>Operator Group</b> groups, users in this group have the rights to create services and perform configurations that affect the running of the NCE and NEs. For example, they can search for protection subnets and trails, delete composite services, and reset boards.
Operator Group	The domain of this user group is <b>All Objects</b> , and it has operation rights for default operator operation sets. In addition to the rights of the <b>Guests group</b> , users in this group have the rights to modify, (rights to perform potentially service-affecting operations are not involved). For example, they can change alarm severities.
uTraffic User Group	When uTraffic interconnects with the NCE, uTraffic accounts will be created on the NCE to manage operation uTraffic rights on the NCE.

- Operation Rights and Operation Set

Operation sets are used to assign a set of operation rights to roles. Users attached to a role have the operation set of this role.

User Management provides two types of operation sets:

- Application operation set: a collection of operation rights for system functions, such as querying system logs and creating users.

The system provides the default application operation set **All Application Operations**. For security purposes, this operation set contains the operation rights for all the system functions except **User Management**, **Auditlog Manager**, and **License Manager**.

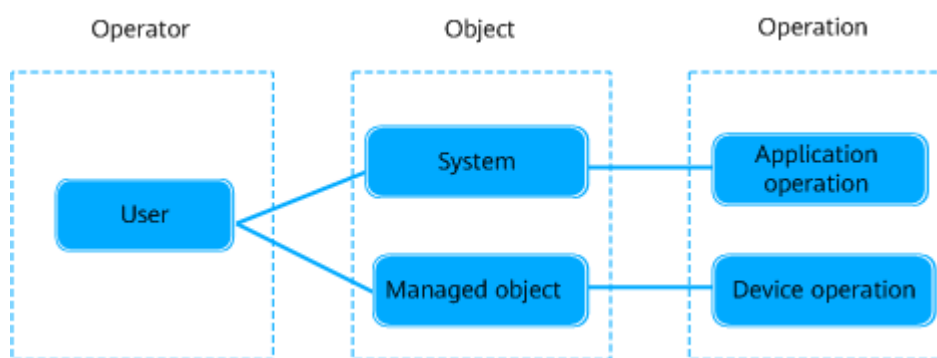
- Device operation set: a collection of operation rights for devices, such as starting and stopping switches.

The system provides the default device operation set **All Device Operations** that contains the operation rights for all the devices.

## Permission Management

A permission defines what operations a user can perform on what objects. Permission elements include an operator, operation objects, and operations as shown in [Figure 5-4](#).

**Figure 5-4** User Management permission



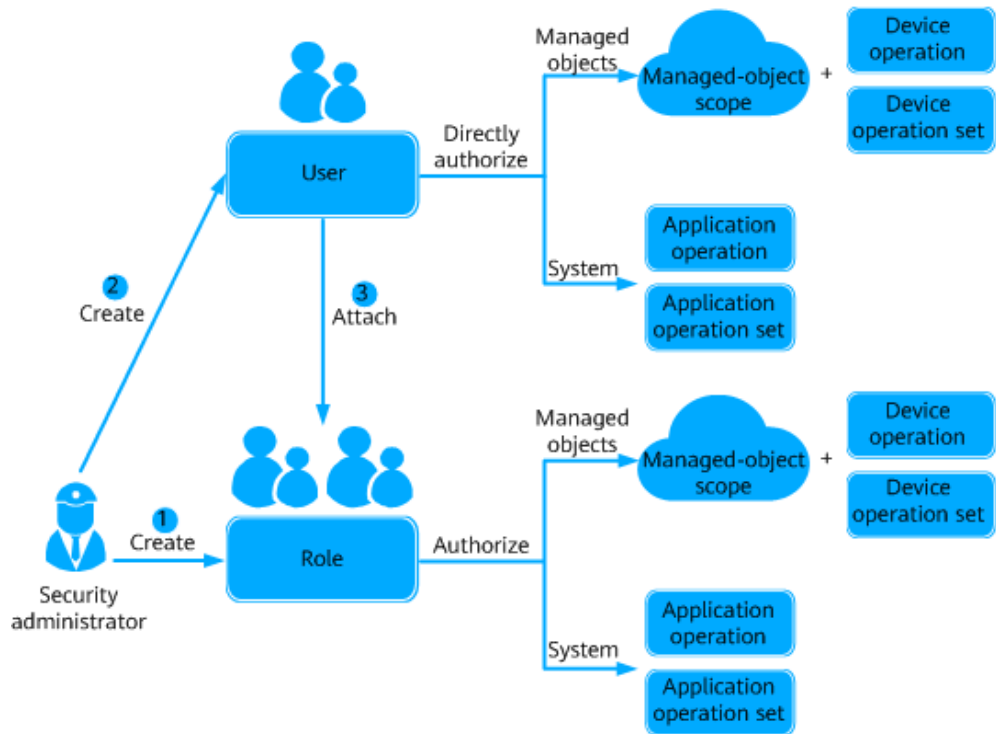
- Permission
  - Users act as operators.
  - Operation objects include the system and resources (physical and virtual resources, such as servers, network devices, and VMs) where users perform operations.
  - Operations include application operations and device operations. Application operations are performed on the system. Device operations are performed on resources.
- Authorization mechanism
 

Authorization is a process of granting permissions on certain objects to users. Authorization mechanism of User Management is as follows:

  - To authorize a user with an object on which this user needs to perform operations, add this object to the managed objects of the role that this user is attached to.
  - To authorize a user with an operation that this user needs to perform, add this operation to the operations for which the role that this user is attached to have operation rights.

[Figure 5-5](#) shows the authorization principles of User Management.

**Figure 5-5** User authorization principles of User Management



**NOTE**

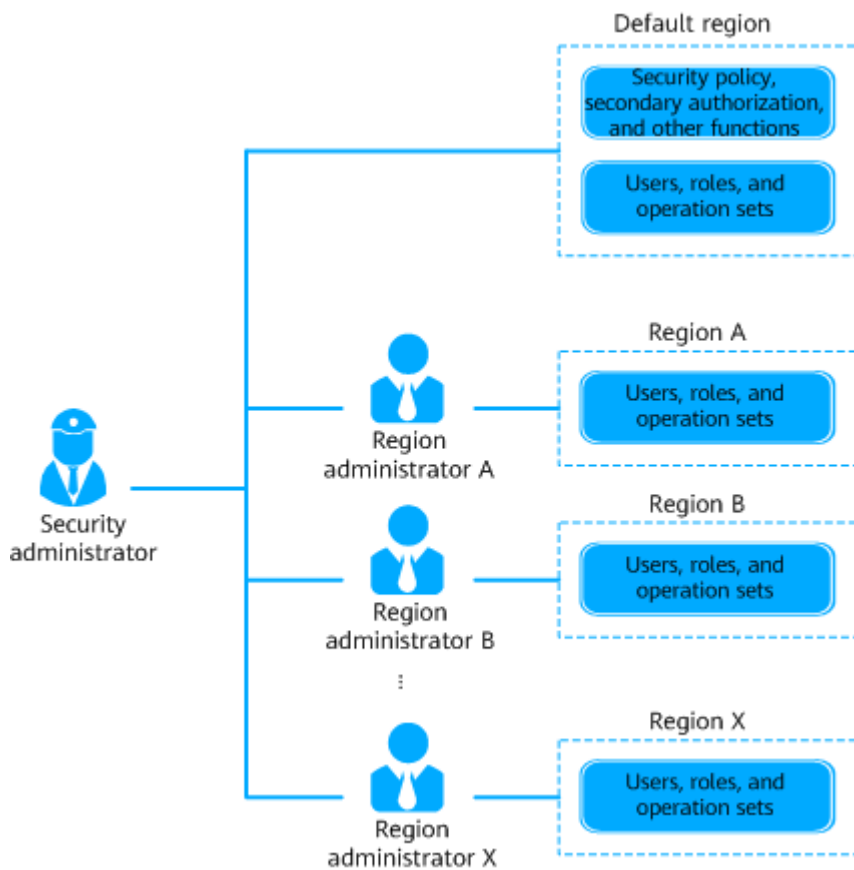
- Users can perform application operations and device operations. If only managed objects are configured for a role but no device operation is configured, users of this role can view the managed objects after logging in to the system but do not have the operation rights for the managed objects.
- If **Assign rights to users directly** is selected, permissions can be directly granted to users.
- Authorization method  
The authorization method of user management grants permissions by attaching a user to a role. After the security administrator sets role permissions (including managed objects and operation rights), the security administrator attaches the user to a role so that the user has the permissions of this role. If **Assign rights to users directly** is selected, permissions can be directly granted to users.  
User authorization allows security administrators to implement authorization for all users in a post at one time. If the employees of a post are changed, security administrators can delete the original user from the role and add the new user to authorize the new user.
- Secondary authorization  
Secondary authorization policies are required to ensure that users can cautiously perform operations that are dangerous or have major impact. Operations specified in these policies are prohibited or can be performed only by users who have the **Secondary Authorization Authentication** permission and pass the secondary authorization.

## Regions Management

Regions can be classified by geographic location or resource usage. Users can be authorized based on regions.

Security administrators can create different regions based on service requirements to implement regional rights-based management. After a region is created, the system automatically creates a region administrator role *Region name\_SMManager* for the new region. Security administrators need to set parameters on the **Mandate-Operation Rights** and **Mandate-Managed Objects** tab pages for the region administrator so that the region administrator can manage the users, roles, objects, and operation sets in this region based on the settings.

Figure 5-6 Region administrator



- Security administrator permissions and region administrator permissions  
Security administrators have all the permissions in the system. Region administrator permissions are set by security administrators based on service requirements.
- Region administrator permissions and permissions of roles in the region  
The permissions and managed objects set for a region administrator on the **Mandate-Operation Rights** and **Mandate-Managed Objects** tab pages can be assigned by the region administrator to roles in the region.

## User Maintenance and Monitoring

During user permission maintenance, you can view and modify user, role, and operation set information, and monitor user sessions and operations in real time. This ensures system security.

- Common operations for user information maintenance include viewing user information, deleting users, exporting user information, and modifying user information.
- Common operations for role information maintenance include viewing role information, deleting roles, exporting role information, and modifying role information.
- Common operations for operation set information maintenance include viewing operation set information, deleting operation sets, and modifying operation set information. You can modify user information (such as **Max. online sessions** and **Login time policy**) in batches to improve system security.
- Personal settings involve periodically changing personal data such as the user password, telephone number, and email address. This improves user security.

### NOTE

- When users modify their personal data, such as mobile numbers and email addresses, they are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of their company, to ensure that the personal data of users is fully protected.
- To ensure the security of personal data, such as mobile numbers and email addresses, these data is anonymized on the GUI, and HTTPS encryption transmission channels are used.
- Resetting a User Password: If a user other than **admin** loses the password or cannot change the password, this user needs to contact security administrators to reset the password.

---

### NOTICE

- You are not allowed to reset the password of user **admin**. If you forget the password of user **admin**, it cannot be retrieved and you can only reinstall the system. Therefore, ensure that you memorize the password of user **admin**.
  - For account security purposes, it is recommended that third-party system access users contact the security administrator to periodically reset their passwords.
- 
- User monitoring: User monitoring monitors resource access behavior of users, including session monitoring (online status) and operation monitoring. If a user performs an unauthorized or dangerous operation, the system allows security administrators to forcibly log out the user. This function allows security administrators to prevent user accesses and ensure system security.

## Security Policies

Security Policies allow you to set access control rules for users. This function improves O&M efficiency and prevents unauthorized users from performing

malicious operations in the system to ensure system security. The security policy function allows you to set account policies, password policies, login IP address control policies, and login time control policies.

- **Account policies:** An account policy includes the minimum user name length and user login policies. Appropriate setting of an account policy improves system access security. The account policy is set by security administrators and takes effect for all users.
- **Password policies:** A password policy includes the password complexity, change interval, and character limitation. Appropriate setting of a password policy prevents users from setting weak passwords or using a password for a long period of time, improving system access security. The password policy is set by security administrators and takes effect for all users. A new password policy does not affect the configured password.
- **Login IP address control policies:** A client IP address control policy provides a control mechanism for checking the accessibility of the IP address used by an external access request during system operation. After an IP address control policy is set and applied, users are allowed to log in to the system only using IP addresses within a specified IP address range.
- **Login time control policies:** A login time control policy provides a control mechanism for checking the validity time of an external access request during system operation. After a login time control policy is set and applied, users are allowed to log in to the system only within the specified period.

### 5.1.3.2 Log Management

Log Management records logs and allows user to query and export logs, and create, export, and import operation log templates. In this way, users can obtain the information about their operations performed in the system and the system running status in real time. Log Forwarding Settings reports audit logs and logs reported by other applications to the Syslog server for users to query and analyze.

#### Scenario

Log Management is used when you need to perform routine maintenance, locate and troubleshoot faults, trace historical logs, and query operation logs across systems.

- **Routine maintenance**  
You need to view logs during routine maintenance. If there are logs recording failed, partially successful, or unknown operations, or logs in Risk level, analyze the exception causes and troubleshoot the faults.
- **Fault locating and troubleshooting**  
To locate and troubleshoot faults occurring during system running, you can analyze logs to detect whether risk-level operations or operations that affect system security are performed.
- **Historical log tracing**  
Logs are stored in the database after being generated. The system periodically dumps logs from the database to a hard disk for sufficient database space. The system periodically deletes the dumped logs from the hard disk for sufficient disk space. To ensure the integrity and traceability of logs, you can forward these logs to the Syslog server.



- Cross-system operation log query  
If you need to query operation logs meeting the same criteria on different systems, you can set filter criteria on one of the systems, save these criteria as a template, and import the template to other systems.

## Log Types

Log Management allows the system to automatically record the information about operations performed by users in the system and the system running status.

Log Management records five types of logs. [Table 5-11](#) describes the log types.

**Table 5-11** Log types

Type	Definition	Triggered By	Purpose	Level
Security log	Records user operations performed in the system that affect system security.	Operations performed by users (including third-party system access users) attached to the <b>SMManagers</b> role, such as: <ul style="list-style-type: none"> <li>• Creating a user</li> <li>• Changing a password</li> </ul>	Detect security issues and risks.	<ul style="list-style-type: none"> <li>• Risk</li> <li>• Minor</li> <li>• Warning</li> </ul>
System log	Records system operations or tasks.	System operations, such as: <ul style="list-style-type: none"> <li>• Unlocking a user</li> <li>• Starting a scheduled task.</li> </ul>	Analyze the system running status and rectify faults.	<ul style="list-style-type: none"> <li>• Risk</li> <li>• Minor</li> <li>• Warning</li> </ul>
Operation log	Records user operations performed in the system that do not affect system security.	User (including third-party system access users) operations, such as: <ul style="list-style-type: none"> <li>• Exporting current alarms.</li> <li>• Creating a subnet.</li> </ul>	Trace and analyze user operations.	<ul style="list-style-type: none"> <li>• Risk</li> <li>• Minor</li> <li>• Warning</li> </ul>

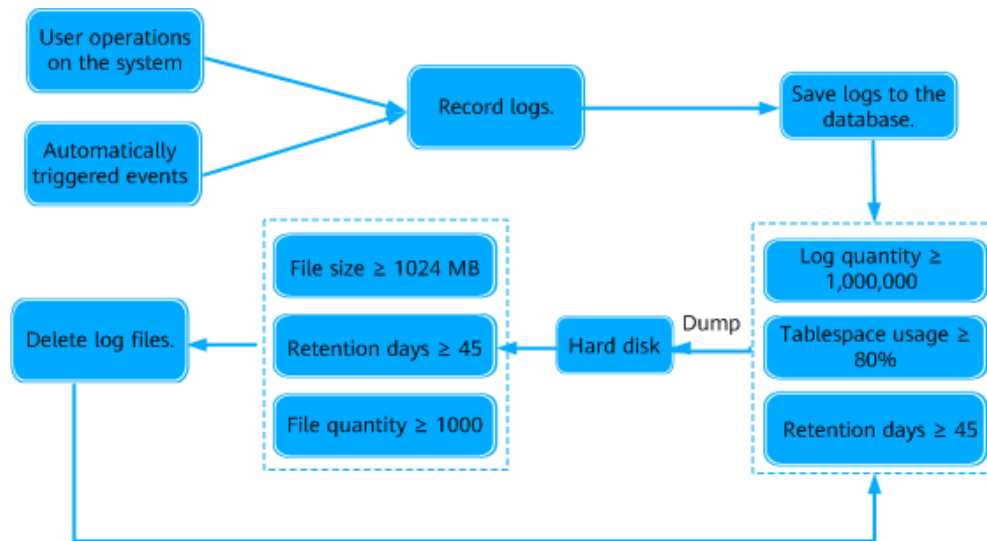
Type	Definition	Triggered By	Purpose	Level
NE syslog run log	Syslog run logs record running information about managed NEs.	System operations.	You can view the NE syslog run logs on the NCE, rather than viewing them on each NE. The NCE allows users to browse syslog run logs of IP NEs. <b>NOTE</b> This function applies to NCE (IP Domain).	Warning, Error
NE syslog operation log	Syslog operation logs record operation logs about managed NEs.	System operations.	You can view the NE syslog operation logs on the NCE, rather than viewing them on each NE. The NCE allows users to browse syslog operation logs of access NEs. <b>NOTE</b> This function applies to NCE (Access Domain).	Warning, Error

## Log Management

When operations are performed by users in the system or events are triggered by the system, Log Management records logs and saves the logs to the Log Management database for users to view on the GUI. In addition, Log Management can automatically dump the logs from the database to the hard disk.

**Figure 5-7** shows the principles of Log Management.

**Figure 5-7 Principles of Log Management**



Logs can be dumped in Task Management or in Log Management.

- **Log dump in Task Management**  
Log dump tasks in Task Management are classified into manual dump and database capacity management tasks. The logs dumped in Task Management are saved in the `/opt/oss/share/NCE/SMLogLicService/var/ThresholdExport/Log` directory on the hard disk of the server.
- **Log dump in Log Management**  
To ensure sufficient database space, the system checks logs in the database every hour, saves logs meeting the requirements as .csv or .zip files to the `/opt/oss/share/NCE/XXXService/dump` directory on the hard disk of a server. The dumped logs are automatically deleted from the database.  
To ensure sufficient disk space, the system checks log files in the database every hour and deletes log files meeting the requirements from the hard disk.

**NOTE**

- *XXXService* can be SMLogLicService or MCCCommonService.
- Conditions for dumping logs in Log Management: The number of logs in the database exceeds 1 million, the size of the logs in the database exceeds 80% of the capacity, or the number of days for storing the logs exceeds 45 days.  
A maximum of 1 million logs are stored in the database. If the database space of Log Management is greater than or equal to 16 GB, you can contact Huawei technical support to set this parameter to 4 million. When the maximum number of logs in the database is set to 4 million, logs exceeding 4 million will be dumped.
- Conditions for deleting log files that are dumped in Log Management: The size of the log files is greater than 1024 MB, the log files are stored for more than 45 days, or the total number of log files exceeds 1000.
- The values in the preceding conditions for dumping logs and deleting log files are default values.

To trace user operations, system operations, and system tasks, you can forward concerned logs to the Syslog server.

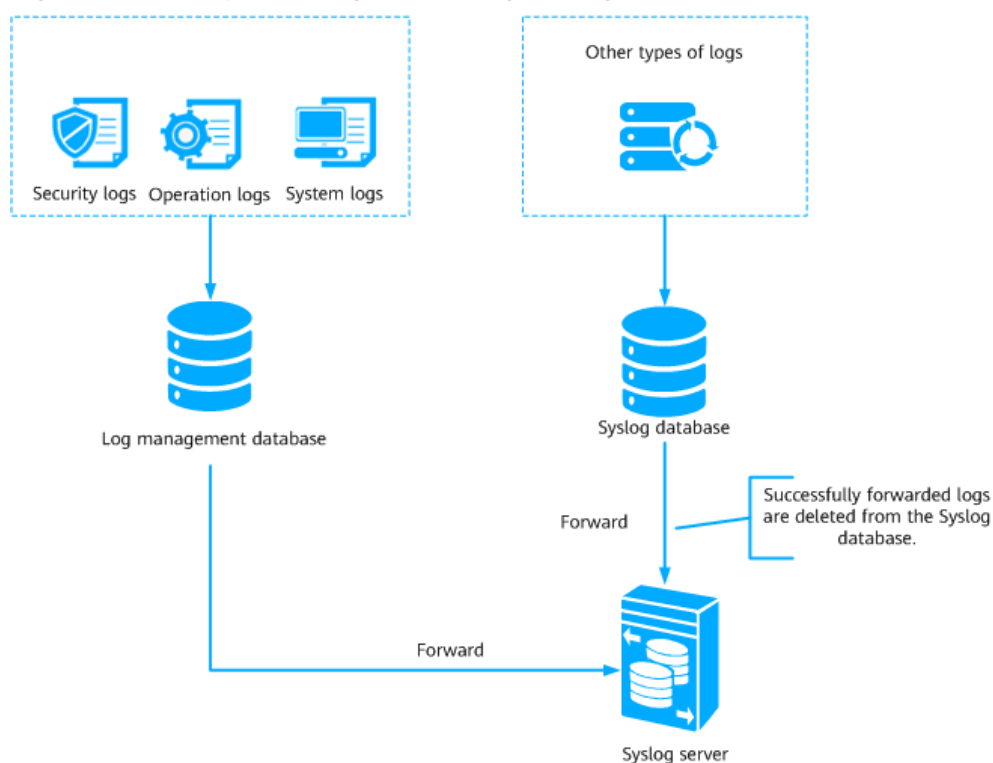
## Log Forwarding

Log Forwarding Settings is used when users need to trace the logs recorded by Log Management, and query and analyze the logs recorded by Log Management and the logs of other functions (such as NE Syslog run logs and NE Syslog operation logs) in real time.

- Users need to permanently store the logs recorded by Log Management so that they can trace the logs to locate problems or rectify faults.
- Users need to query and analyze the logs recorded by Log Management and the logs of other functions (such as NE Syslog run logs and NE Syslog operation logs) in real time on Syslog servers so that they can centrally manage the logs and detect and handle potential security risks in a timely manner.

Figure 5-8 shows the principles of Log Forwarding Settings.

Figure 5-8 Principles of Log Forwarding Settings



## 5.2 Network Management

NCE provides improved NE- and network-level security management, topology management, alarm management, performance management, inventory management, and software management. It can manage all NEs on Huawei transport networks, IP networks, access networks, and obtain third-party device information over NETCONF, SNMP, and ICMP to manage third-party devices. This meets customer requirements for network convergence and service growth.

## 5.2.1 Basic Functions

This topic presents an overview of basic functions and features of NCE.

**Table 5-12** Overview of functions and features of NCE

Function or Feature	Description
Security management	<p>Security management ensures the security of NCE through user management, login management, rights- and domain-based management, and other security policies. Security management also includes log management, which manages logs about logins, user operations, and running of NCE to provide a comprehensive security solution.</p> <p>For details, see <a href="#">5.1.3 Security Management</a>.</p>
NE communication parameter management	<p>NCE communicates with managed NEs successfully only after the connection parameters are correctly set.</p> <p>Users can perform the following operations to manage NE communication parameters on NCE:</p> <ul style="list-style-type: none"> <li>• Query and set the SNMP parameters;</li> <li>• Manage the default SNMP parameter template;</li> <li>• Query and set the NE Telnet/STelnet parameters;</li> <li>• Configure the Telnet/STelnet parameters in batches;</li> <li>• Manage the Telnet/STelnet parameter template;</li> <li>• Manage the FTP/TFTP/SFTP parameter template;</li> <li>• Manage the NETCONF parameter template;</li> <li>• Query and set the NE NETCONF parameters;</li> <li>• Set CloudOpera CSM Communication.</li> </ul>
Topology management	<p>In topology management, the managed NEs and their connections are displayed in a topology view. Users can learn the network structure and monitor the operating status of the entire network in real time by browsing the topology view.</p> <p>For details, see <a href="#">5.2.1.1 Topology Management</a>.</p>
DCN management	<p>NCE communicates with NEs and manages and maintains network nodes through a data communication network (DCN).</p> <p>For details, see <a href="#">5.2.1.2 DCN Management</a>.</p>
Alarm management	<p>Alarm management enables O&amp;M personnel to centrally monitor NE, system service, and third-party system alarms and quickly locate and handle network faults, ensuring normal network operation.</p> <p>For details, see <a href="#">5.1.2 Alarm Management</a>.</p>

Function or Feature	Description
Performance management	<p>The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. In addition, network efficiency needs to be measured in terms of the throughput rate, resource usage, and error rate. Performance management enables users to detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented. In addition, high-precision (<math>10^{-6}</math>) performance measurement based on service packets is implemented to collect performance indicators, including the packet loss rate, delay, and jitter.</p> <p>For details, see <a href="#">5.2.1.3 Performance Management</a>.</p>
Inventory management	<p>NCE provides the functions of collecting, querying, printing, and exporting network-wide physical resources and service resources in a unified manner. This helps users obtain resource information on the entire network in a convenient, quick, and accurate manner to support service planning, routine maintenance, NE warranty, and network reconstruction.</p> <p>For details, see <a href="#">5.2.1.4 Inventory Management</a>.</p>
NE software management	<p>NE Software Management is an independent subsystem of NCE. The subsystem is used to manage NE data and upgrade or downgrade NE software. Managing NE data includes data saving and backup as well as policy management. Upgrading or downgrading NE software includes loading, activation, restoration, task management, and software library management.</p> <p>For details, see <a href="#">5.2.1.5 NE Software Management</a>.</p>
Centralized task management	<p>Centralized task management is a task management mechanism that manages and coordinates all scheduled tasks in a unified management GUI. Two types of tasks are managed in the centralized task management mode: system scheduled tasks (periodic) and custom scheduled tasks (one-off). The two types of tasks can run automatically at a scheduled time. Users can set parameters and browse the task status, progress, and results.</p>
NE template management	<p>NE template management allows users to bulk configure NEs by using configuration templates. This makes NE configuration faster and easier. Repetitive and labor-intensive data entry for NE configurations can be avoided by using templates that automatically fill in the parameter values of the NEs.</p>
NE data configuration and management	<p>NCE supports batch configuration of NE services by using configuration templates, importing data sheets, and loading configuration files. NCE also supports the backup, restoration, and synchronization of NCE data and NE data. With this function, services can be provisioned quickly on the GUI.</p>

### 5.2.1.1 Topology Management

In topology management, the managed NEs and their connections are displayed in a topology view. Users can learn the network structure and monitor the operating status of the entire network in real time by browsing the topology view.

NCE provides the physical view, clock view, and custom view to help users monitor the operating status of the entire network conveniently.

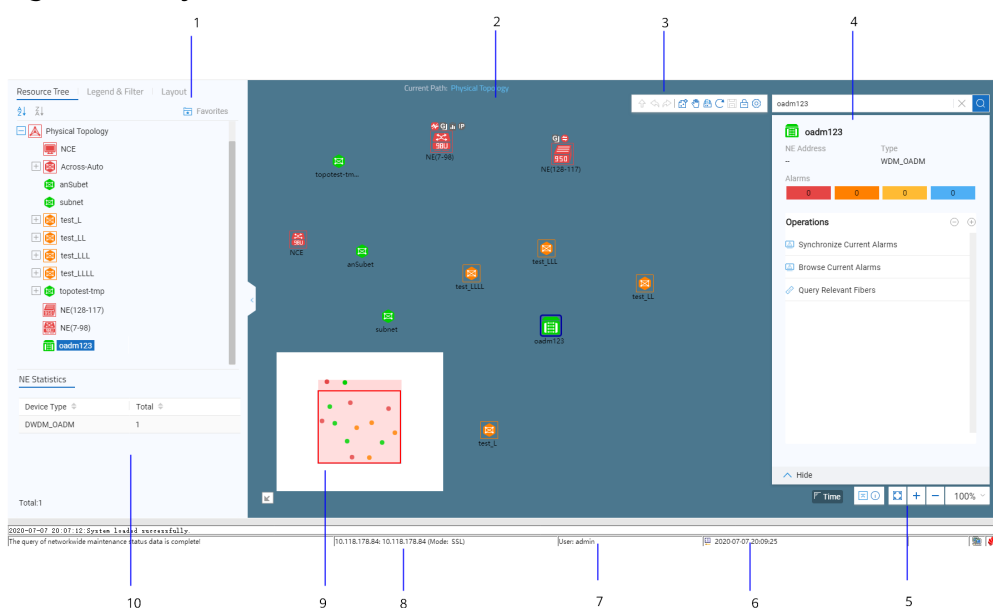
NCE also offers service topology management for various end-to-end services such as VPLS, PWE3, L3VPN, E-AGGR, and tunnel services. Service topology allows users to view and configure services easily.

### Physical View and Its Functions

The physical view of NCE consists of a navigation tree on the left and a view on the right. The navigation tree shows the network hierarchy. The view displays the objects at different coordinates on the background map, which helps identify the locations of deployed objects. Users can set a background image for the topology view. NCE supports multiple formats of images.

Figure 5-9 shows the physical view of NCE and its functions.

Figure 5-9 Physical view and its function



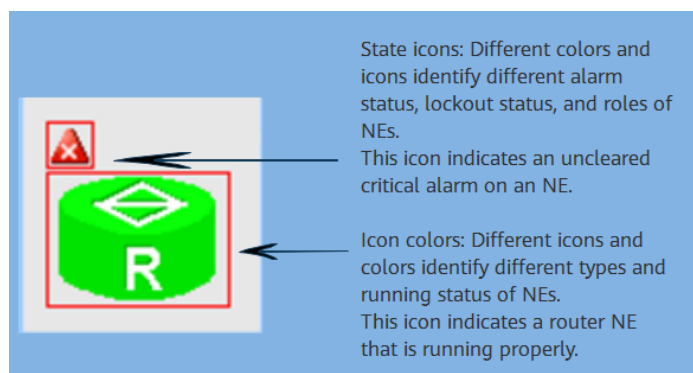
<p>1: Pane on the left</p> <ul style="list-style-type: none"> <li>Resources: All subnets managed by the NCE are displayed. Using this tree, users can locate the required subnet quickly.</li> <li>Legend &amp; Filter: Users can set the display types of the objects in a view. To view the descriptions of legends and the object attributes in the view.</li> <li>Toolbox: Provides the functions of creating subnets and setting topology object layouts.</li> </ul>	<p>2: Topology view</p> <p>In this area, all NEs, links and subnets managed by NCE are displayed. In the physical topology, users can:</p> <ul style="list-style-type: none"> <li>Create subnets, NEs, and links, configure NE data, browse fibers/cables, delete topology objects, browse current alarms, and synchronize NE configuration data.</li> <li>Check NE statuses and communication status using the filter tree and legends.</li> <li>Locate NEs.</li> </ul>	<p>3 &amp; 5: Tool bar</p> <p>Provides functions such as saving topology locations, locking or unlocking views, refreshing views, topology display settings, exporting views, printing views, and zooming in or out views.</p>
<p>4: Search &amp; information panel</p> <p>Users can search for topology objects, view NE, subnet, and connection information in the information panel, and add common operations.</p>	<p>6: System time on the client</p>	<p>7: User name of the logged-in user</p>
<p>8: Server name that is set on the client and the IP address of the server</p>	<p>9: Overview</p> <p>Users can locate the area displayed in the topology view easily.</p>	<p>10: NEs in current view</p> <p>Double-clicking a subnet will display the number of NEs and the status and names of the NEs in the selected subnet.</p> <p>By default, the NE information on the root node of the physical topology is displayed.</p>

## Alarm Display

In the topology view, alarms are displayed in different colors or icons to indicate different status of the subnets and NEs. The default method is color-coded display.



**Figure 5-10** Alarm display in the topology view



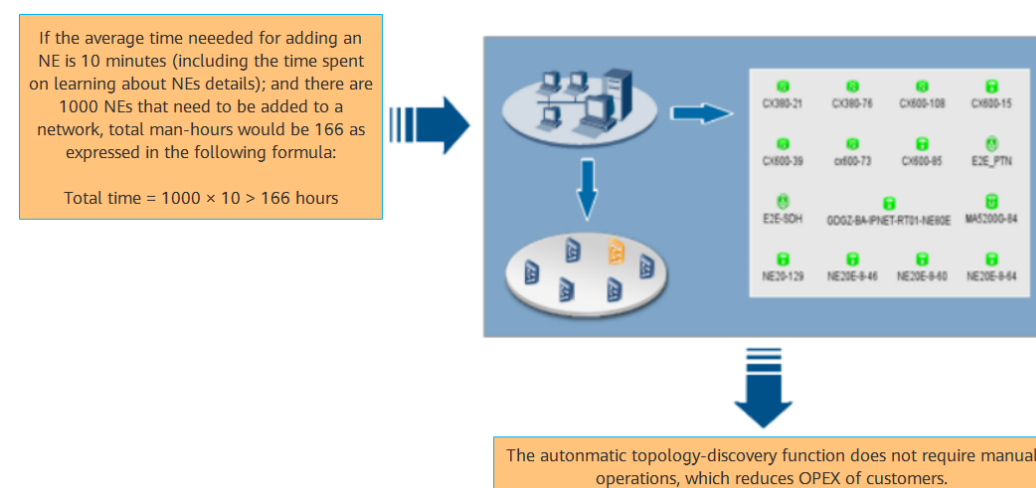
The alarm display in the topology view has the following features:

- The color of a topological node indicates the operating status (such as normal, unknown, or offline) and alarm status of the monitored NE.
- When an NE generates multiple alarms of different severities, the color or icon that indicates the highest alarm severity of these alarms is displayed in the topology view.
- When multiple nodes in a subnet generate alarms, the subnet is displayed in the color or icon that indicates the highest alarm severity of these alarms.
- Users can switch to the current alarm window of an NE using the shortcut menu of the NE node. In addition, users can query the details of current alarms on the NE Panel.

## Automatic Topology-Discovery

NCE provides automatic topology-discovery to automatically add NEs to the topology view, which helps reduce the operation expenditure (OPEX).

**Figure 5-11** Illustration of the automatic topology-discovery function



1. A wizard is provided to instruct users to set the parameters required for the automatic discovery, such as NE type, SNMP parameters, and the IP address range.

2. When parameters are set, NCE searches for the required NEs in the specified network segments according to the preset conditions. All NEs from Huawei and other vendors that meet the conditions will be displayed in the topology view. Meanwhile, the basic configuration data of these NEs is uploaded, which simplifies configuration.
3. Users can pause the discovery at any time. If the discovery fails, the cause of failure is provided when the discovery ends.

NCE supports the following automatic topology-discovery functions:

- Creating NEs in batches
  - Batch creation of SNMP/ICMP-based NEs: When NCE communicates with these NEs successfully, it can search out the required NEs by IP address or by network segment and then bulk create these NEs.  
SNMP/ICMP-based NEs involve:
    - routers series
    - switches series
    - security series
    - access series
    - OSN 9800 (V8) series
  - Batch creation of transport/PTN NEs: Based on the IP address, network segment, or network service access point (NSAP) address of a GNE, NCE can automatically search out all the NEs that communicate with the GNE and bulk creates these NEs.
  - Batch import of NEs: Security GNEs, service monitoring GNEs, and security virtual network (SVN) series security NEs periodically send proactive registration messages that contain the IP addresses of NEs to the NCE server. With proactive registration management, NCE can bulk create these NEs after receiving the messages.
- Automatically discovering NEs: NEs can be automatically discovered and created on NCE and NE configuration data can be uploaded automatically to NCE.

#### NOTE

NCE provides a secure channel for discovering NEs. The channel supports the following NE versions:

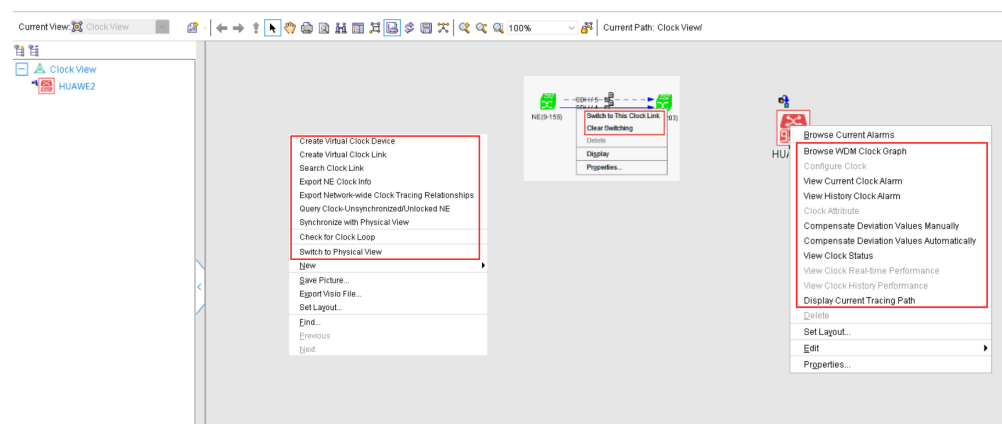
- V600R009C00 and later versions of PTN 6900, NE series, and CX series NEs
- V100R007C00 and later versions of PTN series NEs (excluding PTN 7900)
- V100R005C00 and later versions of RTN 300 series NEs, V100R008C00 and later versions of RTN 900 series NEs
- Scheduling NE searches: NCE can search for specified NE types in specified network segments at scheduled intervals and automatically add discovered NEs to the topology view. The NE types include routers, switches, and security and access NEs.
- Automatically creating fibers/cables/microwave links or links: NCE can search for new fibers/cables/microwave links and links in batches and automatically add them to the topology view.

## Clock View and Its Functions

In the clock view, users can perform the following operations: set NE clocks, query the network-wide clock synchronization status, search for clock tracing relationships, synchronize with the physical view, view the master clock ID, query clock attributes, and view the clock lock status. NCE supports passive optical network (PON) clock, physical layer clock, PTP clock, ACR clock and ATR clock. In the clock view, a variety of NEs can be displayed, such as:

- MSTP series, NG WDM series, RTN series
- OLT series, ONU series, MxU series
- PTN series, NE40E routers, ATN series and CX600 NEs

**Figure 5-12** Clock view and its functions



<p>Discovering the clock topology automatically: NCE can search for clock links between all NEs by NE or by clock link type on the entire network to display their clock tracing relationships. When the clock source traced by NEs has changed, users need to re-search for the clock tracing relationship.</p>	<p>Viewing the clock topology: When NCE has automatically discovered the clock topology, users can view clock tracing relationships on the entire network. To adjust the clock topology, users can manually create and delete topological nodes and links.</p>	<p>Configuring clocks: In the clock configuration window of the NE Explorer, users can configure NE clocks, including PON clock, physical layer clock, PTP clock, ACR clock, ATR clock, and PON clock. The clock configuration function varies depending on the NE type.</p>
--	--	--

<p>Monitoring the change of clocks:</p> <p>When an NE or a link fails or a switch of clock sources occurs in a network, NCE automatically updates the clock tracing relationships and the clock synchronization status in the topology view. The clock alarms generated on the NE where a clock change occurs help users locate the fault.</p>	<p>Switching clocks manually:</p> <p>Users can select a clock link and set its clock tracing relationship as the current clock tracing relationships of the NE.</p>	<p>Synchronizing with the physical view:</p> <p>Users can synchronize the coordinate positions of NEs and subnets in the clock view with the corresponding coordinate positions in the physical view. In addition, the subnets that have clock NEs are also synchronized from the physical view to the clock view. The empty subnets in the clock view are deleted.</p>
<p>Querying clock attributes:</p> <p>Users can query the type, hop count, and port name for clocks traced by the current NE, and view the compensation value for clocks traced by the port.</p>	<p>Querying the clock status:</p> <p>Users can query specific configurations of the clock NE. This facilitates troubleshooting when the NE is abnormal.</p>	<p>Querying clock loops:</p> <p>Users can query clock loops for network-wide clock tracing relationships. If there are clock loops, users can double-click a record in the query result list to locate related NEs in the clock view. This enables users to modify incorrect clock configurations on NEs.</p>
<p>Redirecting to the physical view:</p> <p>Users can be redirected from the clock view to the corresponding subnet in the physical view. If the subnet does not exist in the physical view, the root node will be displayed.</p>	<p>Redirecting to the clock view:</p> <p>Users can be redirected to the corresponding subnet in the clock view. If the subnet does not exist in the clock view, the root node will be displayed.</p>	<p>Viewing master clock ID:</p> <p>When users hover the pointer over a clock NE where clock tracing relationships exist, a tooltip pops up, displaying the NE's clock mode, master clock ID, port status, and other information.</p>

<p>Viewing the cable transmission warp report:</p> <p>NCE allows users to query cable transmission warp values for PTP clock links between NEs. Users can easily find the sites with large warp values and perform measurement only for these sites.</p>	<p>Querying clock-unsynchronized/unlocked NEs:</p> <p>Users can search for clock NEs in the unsynchronized or unlocked state. Such NEs are listed in the lower pane. In this list, users can select desired NEs and export their data.</p>	<p>Browsing real-time or historical clock performance:</p> <p>Users can query clock performance status in the performance monitoring window displayed.</p>
<p>The clock view can display NEs copied in the physical root view and their clock tracing relationships. Copied NEs own the same clock tracing relationships as the source NE.</p>	<p>Querying clock tracing trails:</p> <p>NCE highlights the current clock tracing trails of clock NEs. When a fault occurs, users do not need to draw the clock tracing trails between NEs manually. This improves fault diagnosis efficiency.</p>	<p>Exporting NE clock information:</p> <p>Users can export the clock information about one or all NEs to a specified directory.</p>

## Custom View

The custom view is a subset of the main topology view. The network entities can be NEs, NCEs, and subnets. Typically, network management personnel need to customize views, and choose network entities within their management scope from the main topology view.

**Figure 5-13** Custom View



### 5.2.1.2 DCN Management

NCE communicates with NEs and manages and maintains network nodes through a DCN.

In a DCN, both NCE and NEs are considered as nodes. These nodes are connected to each other through Ethernet or data communications channels (DCCs). The DCN between NCE and the managed network is usually divided into two parts:

- DCN between the NCE server and NEs: Usually, a LAN or WAN is adopted for DCN communication between the NCE server and NEs. In an actual network, the NCE server and NEs may be located on different floors of the same building, in different buildings, or in different cities. Therefore, NCE usually communicates with NEs through an external DCN that consists of equipment such as switches and routers. The DCN is referred to as an external DCN.
- DCN between NEs: NEs can communicate with the NCE in inband networking mode or outband networking mode. As the DCN between the NCE server and NEs is external, the DCN between NEs is referred to as an internal DCN.

Huawei's NEs support DCN networking through the following communication protocols:

- HWECC. Data transmitted in the DCC is encapsulated through HWECC. HWECC is a private communication protocol developed by Huawei for DCN networking of transmission NEs.
- TCP/IP (IP over DCC). Data transmitted in the DCC is encapsulated through Transmission Control Protocol/Internet Protocol (TCP/IP).
- OSI (OSI over DCC). Data transmitted in the DCC is encapsulated through Open Systems Interconnection (OSI).

#### NOTE

- All of Huawei's transmission NEs support HWECC, and the physical transmission channels support D1 to D3 bytes by default. If the NE ID is set, ECC communication can be conducted by only inserting optical fibers. Because HWECC is a proprietary protocol, it cannot meet the requirement for managing the network consisting of devices from different vendors.
- IP and OSI are standard communication protocols, which enable the management of hybrid device networking. In addition, these two standard protocols can be adopted on networks consisting of only Huawei's transmission devices. In the case of a hybrid network consisting of transmission NEs from different vendors that do not support IP or OSI, Huawei provides solutions such as transparent transmission of DCC bytes and Ethernet service channels' transparent transmission of management information.

### DCN functions supported by NCE (Transport Domain)

NCE provides DCN management functions for MSTP, WDM, RTN, and PTN products, which include:

- Modify gateway NE (GNE) parameters.
- Change the GNE of a non-GNE.
- Set a secondary GNE for a non-GNE.
- Convert a GNE to a non-GNE.
- Convert a non-GNE to a GNE.

- Check the GNE switching status.
- Test the communication between NCE and a GNE.
- Check the network communication status.

In addition, the DCC view is provided to display the DCC network in a topology where relationships between NEs are intuitively shown. The DCC view offers the following DCN management functions:

- Check the communication status and relationships between NEs based on the status of DCC links and DCC subnets
- Synchronize data from the main topology to the DCC view, including the network-wide DCC data and DCC subnet data
- Save the DCC view at a time point as a snapshot to facilitate maintenance and troubleshooting
- Switch to the **DCN Management** window of NE Explorer for setting the DCN attributes of NEs
- GUI-based troubleshooting functions
  - **Ping** function to test the connection status between an NE and its GNE
  - **Trace route** function to test the route connection status of the DCC channel between two NEs
  - **Test Reachable NEs** function to test reachable NEs for an NE whose communication with others is unstable (In the scenarios of DCC storms, users can perform this test to find out two NEs that should not have communication and then locate faults using a traceroute test.)
  - **ECC Fault Recovery Wizard** that provides troubleshooting suggestions on embedded control channel (ECC) storms and rapid connection reset to improve fault rectification efficiency

## DCN functions supported by NCE (IP Domain)

The following DCN management functions are provided for ATN and CX series NEs:

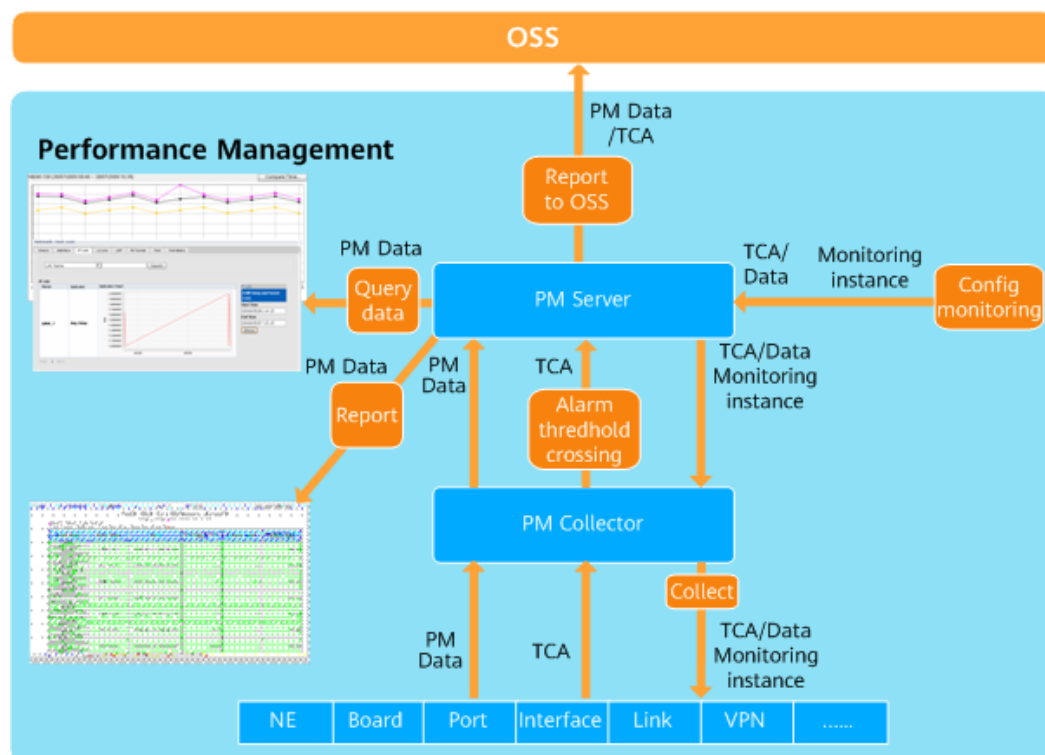
- Automatically add non-gateway NEs to NCE in batches. Users do not need to plan data before ATN series NEs are powered on and added to NCE for management.
- Show the running status and connection status of NEs in the DCN view.

### 5.2.1.3 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. In addition, network efficiency needs to be measured in terms of the throughput rate, resource usage, and error rate. Performance management enables users to detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented. In addition, high-precision ( $10^{-6}$ ) performance measurement based on service packets is implemented to collect performance indicators, including the packet loss rate, delay, and jitter.

NCE provides a GUI for monitoring key network indicators and display statistics about collected performance data.

**Figure 5-14** Performance management process



NCE provides performance monitoring functions at both the NE and network levels. This function is applicable to access NEs, router/switch NEs and transport NEs. When a performance instance is created, NCE can collect performance data from NEs at specified intervals.

- **Monitoring NE performance.** This function supports the following NE-level performance indicators:
  - CPU usage
  - Memory usage
  - Hard disk usage
- **Monitoring network traffic.** This function is used to collect traffic statistics of network ports, including:
  - Inbound traffic
  - Outbound traffic
  - Packet error rate
- **Monitoring SLA data.** This function supports multiple types of SLA data, including:
  - Delay, jitter, and loss rate of ICMP, TCP, UDP, and SNMP packets
  - Connection delay and download speed of Internet services such as HTTP and FTP
- **Collecting interface-based traffic and performance indicators.** This function supports interface-based traffic in BGP/MPLS VPN, VPLS, and PWE3



services, and performance indicators such as delay, packet loss rate, and jitter in BGP/MPLS VPN SLA service. Performance indicators vary depending on the NE type.

- **Setting performance thresholds.** This function allows users to set thresholds for specific performance indicators. NCE also provides default global settings for batch configuration. The following thresholds can be set:
  - Upper and lower thresholds
  - Alarm thresholds
- **Maintaining data.** With this function, users can:
  - Save performance data
  - Dump performance data
  - Regularly compress performance data

## Performance Data Collection

NCE supports the following performance collection modes:

- Collection based on SNMP

### NOTE

- NEs must respond to collection requests sent from NCE in 0.05s. Otherwise, the actual performance collection capability compromises.
- The performance collection capability listed in the preceding table is based on SNMPv1 and SNMPv2c. The SNMPv3-based performance collection capability achieves only two thirds. For example, on a large-scale network, the performance collection capability for SNMPv1 and SNMPv2c is 150,000, and for SNMPv3 is 100,000 when max/min data aggregation is disabled. SNMPv1 and SNMPv2c are insecure protocol, it is recommended to use a more secure SNMPv3 protocol.
- Bulk collection based on a file transfer protocol, which is usually used for large-capacity performance management.
- Collection based on Qx, a protocol developed by Huawei, which can be used for MSTP, WDM, RTN, PTN, and OTN equipment.

**Table 5-13** describes the performance collection capabilities.

**Table 5-13** Performance collection capabilities

<b>Network Scale</b>	<b>SNMP Performance Collection Capability with Max/Min Data Aggregation Disabled (Unit: Max Equivalent Records/15 Minutes)</b>	<b>SNMP Performance Collection Capability with Max/Min Data Aggregation Enabled (Unit: Max Equivalent Records/15 Minutes)</b>	<b>Bulk Performance Collection Capability (Unit: Max Equivalent Records/15 Minutes)</b>	<b>Qx Performance Collection Capability (Unit: Max Equivalent Records/15 Minutes, NCE Polling Period: 30 Minutes)</b>
Less than 500 equivalent NEs	5,000	3,000	<ul style="list-style-type: none"> <li>• IP equipment: 16,000</li> <li>• Access equipment: 66,000</li> </ul>	5000
500-2,000 equivalent NEs	20,000	13,000	<ul style="list-style-type: none"> <li>• IP equipment: 66,000</li> <li>• Access equipment: 266000</li> </ul>	20,000
2,000-6,000 equivalent NEs	60,000	40,000	<ul style="list-style-type: none"> <li>• IP equipment: 200,000</li> <li>• Access equipment: 800,000</li> </ul>	40,000
6,000-15,000 equivalent NEs	150,000	100,000	<ul style="list-style-type: none"> <li>• IP equipment: 500,000</li> <li>• Access equipment: 2,000,000</li> </ul>	80,000
15,000-30,000 equivalent NEs	150,000	100,000	<ul style="list-style-type: none"> <li>• IP equipment: 500,000</li> <li>• Access equipment: 2,000,000</li> </ul>	100,000

 **NOTE**

An equivalent record is a basic unit to describe the performance collection capability of the PMS.

## Performance Monitoring Policy

- Customize the performance threshold template. Specifically, users can customize a maximum of 16 performance threshold templates in addition to the default template.
- Select the performance threshold template for an NE and set the performance thresholds.
- Customize the RMON performance attribute template.
- Set the performance thresholds for a specified board.
- Set the start and end time for monitoring NE performance.
- Set whether to prompt unavailable time and threshold-crossing events in a timely manner.
- Set the start and end time for monitoring Ethernet performance.
- Set the monitoring status of Ethernet performance events.
- Set the ATM performance monitoring time.
- Set the ATM performance monitoring period.
- Set the monitoring status of ATM performance events.
- Set real-time ATM performance monitoring.
- Set performance thresholds by ports or channels.

## SDH Performance Monitoring

- View the SDH current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, unavailable time, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of ATM ports in real time, and view the historical performance data of ATM ports.
- Monitor the performance of ATM VPs and VCs in real time, and view the historical performance data of ATM VPs and VCs.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.
- View the Ethernet performance data in charts or tables.
- Monitor the Ethernet RMON performance.
- Manage lower-order performance of boards.

## WDM Performance Monitoring

- View the WDM current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, unavailable time, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.

- View the Ethernet performance data in charts or tables.
- Monitor the Ethernet RMON performance.

### RTN Performance Monitoring

- View the RTN current 15-minute and 24-hour performance data, historical 15-minute and 24-hour performance data, unavailable time, and 15-minute and 24-hour threshold-crossing events.
- Monitor the performance of Ethernet ports in real time, and view the historical performance data of Ethernet ports.
- View the Ethernet performance data in tables.
- Monitor the Ethernet RMON performance.

### PTN Performance Monitoring

- View the performance of a specified Ethernet service.
- View the performance of a specified pseudo wire (PW).
- View the performance of a specified ML PPP.
- View the performance of a specified tunnel.
- View the performance of a specified circuit emulation service (CES).
- View specified quality of service (QoS) indicators.
- View the performance of specified PW OAM.
- View the performance of specified MPLS OAM.
- View the performance of specified Ethernet OAM.
- View the performance of a specified ATM PWE3 service.
- View the performance of a specified Layer 2 virtual private network (L2VPN) service.
- View the performance of a specified ATM IMA service.
- View the performance of a specified SDH-like service.
- View the performance of a specified regenerator section, multiplex section, and higher-order channel.
- View the performance of a specified lower-order channel.
- View the performance of a specified E1.
- View the performance of a specified laser.
- View the performance of a specified management layer.
- Monitor the Ethernet RMON performance.
- Reset the performance register on a board.

### Performance Data Dumping

The storage duration of performance data varies depending on the collection period. If the collection period is 5 minutes, 10 minutes, or 30 minutes, performance data generated only in the last day is saved by default. If the collection period is 1 hour or 1 day, performance data generated only in the last 8 days or 30 days is saved by default.

You can save performance data to a file automatically or manually.

For manual dumping, the conditions for an immediate dump must be set.

For automatic dumping, the following items must be set:

- Conditions for overflow dumping
- Conditions for periodic dumping
- Directory of dump files

## Performance Data Analysis

- Analyze historical performance data.
- Forecast long-term and medium-term performance according to the empirical formula created based on the historical performance data of optical transceivers.
  - If the performance indicator value is available, the time for generating the value and the deviation range can be calculated.
  - If the time is available, the performance indicator value at that time and the deviation range can be calculated.

## Performance Register Resetting

Board, ATM, and Ethernet performance registers can be reset.

## Performance Monitoring Template Management

A performance monitoring template contains a collection of performance indicators that are classified into various indicator groups. Users can manage a performance monitoring task easily by setting such a template.

There are different types of performance monitoring templates. Some may contain indicators and indicator groups of network resources, while others may contain both indicators and indicator thresholds.

## SLA Template

This function enables users to configure SLA parameters in a template. This saves operation time for configuring SLA parameters when creating an instance.

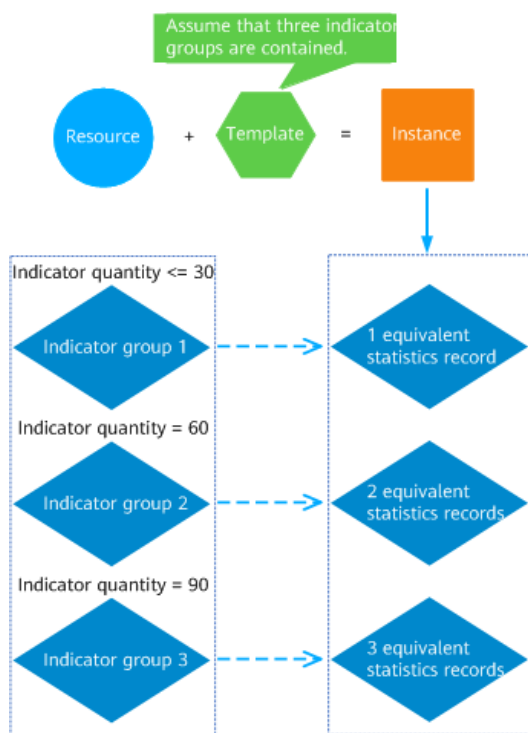
## Monitoring Instance Management

A monitoring instance consists of monitored resources and the monitoring template. By creating an instance, users can collect data of certain resource performance indicators. A template can contain multiple indicator groups. [Figure 5-15](#) shows the relationship between templates, instances, indicator groups, and equivalent records.

**NOTE**

- Resource: A model of telecom resource such as device, card, port, or link in the performance management domain. A resource can be either a physical or logical entity. Logical resources contain physical resources. A resource has specific performance indicators. A performance monitoring system collects indicator values for resources.
- Template: A collection of indicators classified into indicator groups. Users can configure templates to manage performance monitoring tasks easily.
- Indicator group: An indicator group consists of one or more indicators with similar properties.
- Indicator: A performance indicator defines a specific aspect of performance of the associated resource, for example, traffic, availability, and CPU usage. Performance indicator values are calculated based on the performance data collected from the monitored resource. A performance indicator has properties, such as the data type, precision value (only for float), maximum value, and minimum value.

**Figure 5-15** Relationships between a resource, a template, and an instance



- An indicator group that contains no more than 30 indicators equals an equivalent statistics record.
- For an indicator group with over 30 indicators, the conversion algorithm is as follows:  
 $\text{Number of indicators} / 30$   
 If the remainder is less than 15, the remainder equals 0.5 equivalent record. Total number of equivalent records = Integer of (number of indicators/30) + 0.5  
 If the remainder is greater than or equal to 15, the remainder equals 1 equivalent record. Total number of equivalent records = Integer of (number of indicators/30) + 1  
 For example, if an indicator group has 32 indicators, the integer of (number of indicators/30) is 1 and the remainder is 2. The total number of equivalent records is 1.5.

Monitoring instances enable users to collect performance data for resources of specified equipment according to a preset monitoring template and scheduling policy. One monitoring instance collects data for only one resource. Users can perform the following operations on NCE:

- Create monitoring instances for the IP SLA from resources such as NEs, boards, ports, and links to PTN and third-party equipment.
- Modify monitoring instances.
- Query monitoring instances.
- Delete monitoring instances.
- Suspend monitoring instances.
- Resume monitoring instances.
- Synchronize resources corresponding to monitoring instances.
- Query thresholds.
- Query the VPN SLA test result.
- Export instance information.
- Collect statistics about instances.
- Display KPIs.

## Scheduled Task

A schedule task specifies the time range and period for collecting performance data. Users can configure a scheduling policy for resources when creating or modifying a monitoring instance.

## Historical Performance Data

Users can collect network performance data within a specified period and save the data in multiple formats. Historical performance data provides reference for predicting changes in network performance.

NCE can query performance data by parameters such as the NE name, time, and performance data type. Currently, 5-minute, 10-minute, 15-minute, 30-minute, 1-hour and 1-day historical performance data can be queried. Users can view the historical performance data of a network in a line chart or table. The line chart allows the query result to be saved in .csv format, and the table allows the query result to be saved in .csv, .html, .pdf, .txt, and .xml formats. For example, if performance data is saved in CSV format, the result will be similar to [Figure 5-16](#).

**Figure 5-16** Save result

1					
2					
3	Browse Historical Performance Data				
4	Save Time: 04/11/2017 18:16:28				
5	User Name:admin				
6					
7					
8	Total 84 Records				
9					
10	Resource Name	Collection Time	Granularity	CPU Occupancy(%)	Slot Temperature(C)
11	10.185.215.3/Fr:04/10/2017	20:45:15	Min	6	45
12	10.185.215.3/Fr:04/10/2017	21:00:15	Min	7	45
13	10.185.215.3/Fr:04/10/2017	21:15:15	Min	6	45
14	10.185.215.3/Fr:04/10/2017	21:30:15	Min	6	45
15	10.185.215.3/Fr:04/10/2017	21:45:15	Min	7	45
16	10.185.215.3/Fr:04/10/2017	22:00:15	Min	6	45
17	10.185.215.3/Fr:04/10/2017	22:15:15	Min	6	45
18	10.185.215.3/Fr:04/10/2017	22:30:15	Min	6	45
19	10.185.215.3/Fr:04/10/2017	22:45:15	Min	6	45
20	10.185.215.3/Fr:04/10/2017	23:00:15	Min	6	45
21	10.185.215.3/Fr:04/10/2017	23:15:15	Min	6	45
22	10.185.215.3/Fr:04/10/2017	23:30:15	Min	6	45
23	10.185.215.3/Fr:04/10/2017	23:45:15	Min	6	45

In addition, users can compare performance data in different periods in a line chart or bar chart or compare the indicators of different resources in a chart.

Users can choose whether to view historical performance of a resource in one chart or multiple charts.

## Real-Time Performance Data

Users can view real-time performance data in a table, line chart, or bar chart, and save performance data in file formats of CSV, HTML, PDF, TXT, and XML.

Users can also set the default display mode as line chart, bar chart, or table.

## Data Lifecycle Management

Users can back up performance data to a specified storage medium manually or automatically when excessive performance data is saved in the database of NCE.

Data can be dumped in the following two ways:

- Automatic dumping: Performance data is dumped automatically based on preset parameters, such as period (number of days) and database usage.
- Manual dumping: Performance data is dumped based on user-defined conditions, such as file type.

## Network Performance Monitoring

Users can view the performance data of NEs, interfaces, IP links, L2 links, static, tunnels, dynamic tunnels, and test cases on the same network by network group. In addition, users can perform various tests on a network, such as UDP jitter test and FTP ping test, to evaluate the quality of networks and services and analyze the correlation between the quality of networks and services.

- Create a network group.



Users can group the monitoring instances of resources of different types on the same network according to customized rules, such as an area-based rule or service-based rule. This facilitates performance data browsing and comparison.

- Analyze interface performance trends.

When network interface indicators are set, a performance trend graph of the current time or of the past 12 hours can be generated. The graph helps users understand the general interface performance trend.

- View the results of network monitoring instances.

Users can view the results of network monitoring instances to obtain information about network-related indicators, evaluate network performance, and analyze the correlation between indicators and network performance.

## TCA Threshold Setting

NCE allows users to set thresholds for performance indicators using a threshold crossing alert (TCA) monitoring template and then use the template to monitor TCAs for resources. NCE generates a TCA when the performance indicator value exceeds the defined threshold in the TCA monitoring template.

## Database Size Calculator

NCE can calculate the required database space based on the number of collection instances (number of interface resources), collection period, lifecycle and the number of indicators of each instance. In addition, NCE can calculate the performance data lifecycle based on the number of collection instances (number of interface resources), collection period, number of indicators of each instance, and available database space.

### 5.2.1.4 Inventory Management

NCE provides the functions of collecting, querying and exporting network-wide physical resources (including virtual NEs and third-party NEs) and service resources. The resources can be exported to XLS, XLSX, TXT, HTML, or CSV files in a unified manner. This helps users obtain resource information on the entire network in a convenient, quick, and accurate manner to support service planning, routine maintenance, NE warranty, and network reconstruction.

- Physical resources (such as equipment rooms, NEs, ports, optical/electrical modules, and passive devices) and logical resources on the entire network can be managed or maintained in unified and hierarchical mode. You can easily query and export various types of resources of multi-layer attributes. You can also customize filter criteria to query data on the live network, which improves resource maintenance efficiency.

NE Name	NE Type (MPU Type)	NE IP Address	Software Version	NE MAC Address	NE ID	Fibers/Cables	Slot
NE(113-211)D&O^AEM196	OptiX PTN 960	10.137.110.211	V100R007C00SPC100		113-211	0	RO
NE(9-323)	OptiX BWS 1600G	129.9.1.67	5.8.7.20		9-323	0	RO
NE(29-207)	OptiX OSN 1800 V	9.173.29.207	V100R009C00SPC200		29-207	0	00I
NE(29-203)	OptiX OSN 9800 U32	9.173.29.203	V100R007C00SPC200		29-203	0	00I
NE(29-227)	OptiX OSN 1800 I E	9.173.29.227	V100R009C00SPC200		29-227	0	00I
NE(29-226)	OptiX OSN 1800 I E	9.173.29.226	V100R009C00SPC200		29-226	0	00I
NE(29-223)	OptiX OSN 9800	9.173.29.223	V100R007C00SPC200		29-223	39	00I
NE(29-221)	OptiX OSN 9800	9.173.29.221	V100R007C00SPC200		29-221	0	
NE(29-202)	OptiX OSN 9800 U32	9.173.29.202	V100R007C00SPC200		29-202	0	RO
NE(29-222)	OptiX OSN 9800	9.173.29.222	V100R007C00SPC200		29-222	38	

- You can customize categories to make statistics of physical resources from multiple aspects, and export inventory reports for equipment rooms, racks, subracks, NEs, boards, subboards, ports, optical/electrical modules, slot usage and passive origin component. This helps you learn various types of resources on the entire network, provides reference for E2E operation and maintenance, and improves resource usage.

NE Type (MPU Type)	Quantity
HUAWEI OSN902	1
OptiX OSN 8800	2
OptiX OSN 6800	1
OptiX OSN 8800 T16	1
OptiX OSN 8800 T32	8
OptiX PTN 7900-32	1
OptiX PTN 3900	2
OptiX RTN 950	24
OptiX OSN 9800 P32	2
OptiX BWS 1600G	4

You can customize categories to query network-wide resources from multiple aspects in unified mode and make statistics for the resources. This provides reference for E2E operation and maintenance.

- Business planning: You can make statistics for the NEs, used slots, ports, and optical modules to learn the online NEs, slot usage, idle ports, optical splitting, and remaining bandwidth.
- Routine maintenance: You can query racks, NEs, boards, and ports to learn the running status of the rack power supply and NEs, software version of NEs and boards, service configurations, and port rate.
- NE warranty: You can query NEs and boards to learn the NEs created in the specified time, or hardware and software versions of boards.

- Network reconstruction: You can make statistics for NEs by customizing categories to learn the NE types, quantities, and positions.

The following table provides the functions of each type of physical and logical resources, inventory query results, and categories supported by the inventory reports.

**Table 5-14** Inventory functions, resource query, and report statistics

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
Physical resources	Equipment Rooms	Creates, modifies, deletes an equipment room and queries, exports, or makes statistics of equipment room information.	Equipment Room Name, Site, Country, Province, City, Location, Room Number, Cabling Mode, Antistatic Floor, Thickness of Antistatic Floor(mm) and Remarks.	Site, Country&Province&City, Country&Province&City&Room Number, Cabling Mode and Customize Statistics.
	Racks	Creates, modifies, deletes a rack and queries, exports, or makes statistics of rack information.	Rack Name, Equipment Room Name, Rack Type, Rack Height (mm), Rack Width(mm), Rack Depth(mm), Power Box Type, Voltage(V), Number of Batteries, Internal Battery, Internal Power Supply, Internal MDF, Internal Transmission, Number of Shelves and Remarks.	Rack Type, Height, Width, Depth, Height&Width&Depth, Power Box Type, Voltage and Customize Statistics.

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	NEs	Sets queries and exports NE information, makes statistics of NEs by NE or subnet, and makes statistics of equivalent NEs.	NE Name, NE Type(MPU Type), NE IP Address, Software Version, NE MAC Address, NE ID, Fibers/Cables, Subnet, Subnet Path, Subrack Type, NE Subtype, Communication Status, Administrative Status, Physical Location, Created On, NE Alias, Remarks, Patch Version list, LSR ID, Gateway Type, Gateway, Gateway IP, Optical NE and Life Cycle Status.	NE Type(MPU Type), Software Version, NE Type(MPU Type)&Software Version, Equivalent NE and Customize Statistics.

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Subracks	Sets queries and exports subrack information, and makes statistics of subracks by NE or subnet.	NE Name, Subrack Name, Subrack Type, NE ID, NE IP Address, Software Version, SN(Bar Code), Subnet, Subnet Path, Subrack ID, Subrack Status, Subrack Alias, PN(BOM Code), Description, Manufactured on, Equipment Room Name, Rack Name, Subrack Number and Remarks.	Subrack Type, Equipment Room, Rack, NE Type(MPU Type) and Customize Statistics.

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Boards	Sets queries and exports board information, and makes statistics of boards by NE or subnet.	NE Name, Board Full Name, Board Name, Board Type, NE ID, NE IP Address, NE Type(MPU Type), Subrack Type, Subrack ID, Slot ID, Hardware Version, Software Version, SN(Bar Code), Board Alias, Remarks, Model, Rev(Issue Number), FPGA Version, BIOS Version, Board Status, Protection Role, PSTQ, PN(BOM Code), Administrative Status, Description, Manufacture On and Create On.	Board Type, Board Type&Hardware Version, Board Type&Software Version and Customize Statistics.

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Subboards	Sets queries, exports, or makes statistics of subboard information.	NE Name, NE Type(MPU Type), Subboard Full Name, Subboard Name, Subboard Type, Subrack ID, Slot Number, Subslot Number, Hardware Version, Software Version, SN(Bar Code), Subboard Status, Subrack Alias, Description, Remarks, PN(BOM Code), Manufacture On, Model and Rev(Issue Number).	Subboard Type, Subboard Type&Hardware Version, Subboard Type&Software Version and Customize Statistics.

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Ports	Sets queries, exports, or makes statistics of port information.	NE Name, NE Type(MPU Type), Shelf Number, Slot Number, SubSlot Number, Port Number, Phone Number, Port Full Name, Port Name, Port Type, Port Rate (kbit/s), Port Level, Administrative Status, Operational Status, Port Alias, and Remarks.	Port Type



Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Optical/ Electrical Module	Sets user labels for the optical/ electrical module, and queries, exports, or makes statistics of optical/ electrical module information.	<ul style="list-style-type: none"> <li>• SFP Information : Port, SFP Type, Fiber/Cable Type, Logical Type, Physical Type, SN(Bar Code), CLEI Code, PN(BOM Code/Item), Model, Rev(Issue Number), Manufacturer, Date of Manufacture, User Label, Description, and User-defined Info.</li> <li>• Router and Switch Optical/Electrical Module: Serial No., Optical/Electrical Type, NE Name, Port Name, Port Description, Port Type, Receive Optical Power (dBm), Reference Receive Optical</li> </ul>	Wave Length (nm), NE Name+Wave Length (nm)

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
			Power (dBm), Reference Receive Time, Receive Status, Upper Threshold for Receive Optical Power (dBm), Lower Threshold for Receive Optical Power (dBm), Transmit Optical Power (dBm), Reference Transmit Optical Power (dBm), Reference Transmit Time, Transmit Status, Upper Threshold for Transmit Optical Power (dBm), Lower Threshold for Transmit Optical Power (dBm), SingleMode	

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
			/ MultiMode, Speed (Mbit/s), Wave Length (nm), Transmission Distance (m), Fiber Type, Manufacturer, Optical Mode Authentication, Port Remark, Port Custom Column, Optical Direction Type, Vender PN, Model, Rev(Issue Number).	
	Slot Used Statistics	Makes statistics of total slots and used slots by NE type and NE, so that you can determine the board capacity and future expansion.	NEs, NE Type, NE Name, Total Slot Count, Used Slot Count, Vacant Slot Count, Slot Usage %	NE Type(MPU Type), NE

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Passive Origin Component	Makes statistics of dispersion compensation module (DCM) information to manage DCM passive devices. This is supported only by NCE (Transport Domain).	NE, Serial Number, DCM Name, BOM, Barcode, Compensation Distance(km), IN Port, OUT Port, Location, Vendor, Description, Remark	-
Logical resources	Fiber/Cable Pipe	Adds multiple fibers and cables to a pipe for management. Fiber/cable pipe management is supported when the platinum service is used. Pipe management involves creating, deleting, or querying a fiber/cable pipe, and adding or removing fibers and cables to or from a fiber/cable pipe.	Pipe Name, Pipe Memo, Creation Time, Creator, Fiber Count	-

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Link	Manages and maintains virtual links, Layer 2 Links, and IP links, involving creating a link, adding a link to a link group, and viewing links and link alarms.	Alarm Severity, Link Name, Link Type, Network Protocol Type, Source NE, Source IP, Source Port, Source Port IP, Source Port Alias, Sink NE, Sink IP, Sink Port, Sink Port IP, Sink Port Alias, Link Level, Link Rate (bit/s), Remaining Upstream Bandwidth (Kbit/s), Remaining Downstream Bandwidth (Kbit/s), Build Time, Remarks, User Label, Owner, weight.	-

Category	Resource	Function	Queried or Exported Inventory Information	Default Statistics Categories of the Inventory Report
	Electronic Labels	NCE exports electronic labels of devices that comply with the new IBMS script specifications and saves the data in XML files. This helps maintenance personnel view and manage network inventory resources in the IBMS.	-	-

### 5.2.1.5 NE Software Management

NE Software Management is used to manage NE data and upgrade or downgrade NE software. Managing NE data includes data saving and backup as well as policy management. Upgrading or downgrading NE software includes loading, activation, restoration, task management, and software library management. For security purposes, users are advised to use SFTP as the transfer protocol between NCE and NEs.

The main function is listed as follows.

- **Saving:** After the configuration is complete, the configuration data is saved in the memory or hard disks of NEs so that the data will not be lost during restart. NCE saves data in the following ways:
  - Manually performing the save operation
  - Automatically performing the save task
  - Automatically performing the save policy
- **Backup:** Backs up NE data (such as configuration data or databases) to storage devices other than NEs. The backup data is used for restoring NE data. If NCE has the permissions to manage the NE and the loading, backup, or restoration operation is not being performed on the NE, the NE will accept the request to back up the data. NCE then transmits the contents to be backed up to the specified backup directory on the server by using the transfer protocol. The backup data can also be backed up to the client, or to a third-part server. The allowed size of backup files depends on the space size

of the disk where the backup directory is located. NCE backs up data in the following ways:

- Manually performing the backup operation
- Automatically performing the backup task
- Automatically performing the backup policy
- Policy management: Setting policies in advance enables NCE to perform operations on NEs periodically or when trigger conditions are met. This is applicable to routine NE maintenance. A policy is periodic and is used for operations that are performed frequently, such as data saving and data backup. Users can select a policy based on the scenarios at the sites.
- Loading: Software is loaded for NE upgrade. If NCE has the permissions to manage NE upgrade and the loading, backup, or restoration operation is not being performed on the NE, the NE will accept the request to load the software. NCE then transmits the contents to be loaded to the NE by using the transfer protocol. NCE loads data in the following ways:
  - Automatically loading by creating a task
  - Automatically loading through an automatic upgrade task
- Activating: A newly loaded NE can be activated to take effect. If NCE has the permissions to manage NE upgrade and the loading, backup, or restoration operation is not being performed on the NE, the NE will accept the request to be activated. NCE activates the NE automatically through an automatic upgrade task.
- Restoration: An NE can be restored using the backup NE data. If NCE has the permissions to manage NE upgrade and the loading, backup, or restoration operation is not being performed on the NE, the NE will accept the request to restore the NE data. NCE then transmits the contents to be restored to the NE by using the transfer protocol. NCE restores data in the following ways:
  - Manually performing the restoration operation
  - Automatically performing the restoration task
- Task management: NCE encapsulates all operations into tasks. By creating an upgrade task or a downgrade task for software or a patch, users can upgrade or downgrade the software or patch in one-click mode or at the scheduled time. A task is not periodic and is used for operations that are not performed frequently, such as data upgrading. Users can select a task based on the scenarios at the sites.
- Software library management: The software used for NE upgrade can be managed in a centralized manner. For example, users can upload NE software from the NCE client or NCE server to the software library. In this manner, the process of loading software is simple and fast.
- NE license management: NE license management involves querying, applying for, installing, and changing an NE License. In addition, you can adjust the capacities defined in the license. The license controls the validity period or functions of an NE. Therefore, users need to view the license status and change the expired license. Otherwise, services will be affected.

## 5.2.2 Transport Network Management

## 5.2.2.1 Transport NE Service Management

### Basic Service Management for Transport NEs

NCE supports the following series of transport NEs: SDH, RTN, WDM, SDH ASON, and WDM ASON.

### WDM ASON Deployment

**Intelligent OD optical-layer management solution:** The NCE provides the OD optical-layer intelligent management solution. The Optical Doctor (OD) system performs online OSNR monitoring, performance monitoring, and performance optimization for 10G, 40G, and 100G wavelengths, improving optical-layer maintenance capabilities.

### Intelligent Microwave Deployment and Mobile O&M

- **Offline configuration:** Before microwave deployment, you need to use the offline configuration tool to set offline NE parameters based on the network planning information and then generate NE parameter scripts. During microwave deployment, you only need to bring the script file to the site and deliver the script file through a USB flash drive or the Web LCT. In this way, you can migrate and deploy a large number of NEs.
- **Software instrument test:** The NCE provides the software meter test capability. The software implements frequency scanning, software commissioning, and remote acceptance, replacing traditional meters, reducing costs, and improving device deployment efficiency. In addition, the NCE test result can be used to generate a remote software instrument acceptance report in one-click manner, instead of manual writing.
- **Hop management:** In the case of hop management, you can set parameters for devices at both ends of a microwave link in the same window. In addition, the association between two NEs is implemented based on key parameters, which improves the efficiency of setting microwave link parameters.
- **Mobile O&M:** Microwave mobile O&M analyzes network access scenarios of new microwave devices and uses smartphones to manage sites, deliver service scripts, and manage passive components. This simplifies operations on site engineering delivery, such as microwave deployment and site resources, effectively reducing engineering delivery and maintenance costs.

### WDM Service Adjustment

- **Optical-layer board replacement:** You can use the expansion wizard to quickly replace optical-layer boards, migrate optical fibers and services from a board to another board, and ensure smooth service migration. Board changes during the expansion from 10G to 100G are automatically synchronized, improving operation efficiency.
- **Batch service switching:** You can determine whether a fiber is protected by selecting all services of the fiber. Then, you can switch services from the fiber to another fiber in batches based on the check result.



## MSTP Service Adjustment

- **Transport board replacement:** Through a software algorithm, a board can be replaced with another board. In this way, services and parameters can be smoothly migrated.
- **Transport NE replacement:** In the network service adjustment scenario, a software algorithm is used to smoothly migrate services from an NE to another NE instead of manually migrating services one by one. In this way, NE services are quickly migrated.
- **Link capacity upgrade:** In the network service adjustment scenario, the line boards on both sides of the link to be upgraded are replaced without interrupting the current service. In this way, the link capacity can be upgraded. In addition, a software algorithm is used to smoothly upgrade the original service capacity.

## Data Migration

**Script import and export:** The NCE supports the following functions:

- Importing and exporting basic SDH NE data
- Importing and exporting basic OTN NE configuration data
- Preconfiguring SDH/EOS features for OTNs
- Exporting and downloading scripts

## Visualized DCN Management

The NCE communicates with NEs through the DCN and manages and maintains network nodes.

- **DCN management based on tables/views:** The NCE can manage and maintain DCN links of NEs in tables or views to locate and analyze faults.
- **DCN subnet synchronization:** By querying DCC link connectivity on the entire network, the NCE can automatically discover DCC subnets and display them in a visualized manner. In addition, the NCE supports the display of logical fibers and ECC links between NEs.
- **Network health evaluation:** The NCE provides DCC network health evaluation, monitoring, and DCC network risk assessment.
- **Snapshot of the DCN view:** You can manually and periodically save DCC view snapshots and locate faults based on the snapshots.
- **All-gateway management:** The NCE supports the management of all GNEs.

### 5.2.2.2 Transport Network Service Management

#### E2E OTN Service Management and Service-level Fault Diagnosis

The NCE supports E2E fast provisioning of OTN network services and troubleshooting of OTN network faults with just one click.

- **E2E service provisioning:** Only two steps are required for E2E OTN service provisioning. Only the optical-layer OCh layer and electrical-layer client layer need to be created to implement automatic creation of point-to-point cross-

connections and optical cross-connections. You can disregard the specific OTN layer. This simplifies service provisioning, reduces engineers' skill requirements, and improves service provisioning efficiency.

- During OTN service provisioning, wizard-based OTN network service troubleshooting provides clear fault points and fault causes to enable you to quickly demarcate and locate faults, improving O&M efficiency.
- By using service alarms, you can diagnose service-level faults with just one click and quickly identify inter-network or intra-network faults. The troubleshooting duration is reduced from 1 hour to 5 minutes.

## E2E Management of Transport Packet Services

The NCE provides E2E service configuration and service path visualization. It improves network O&M efficiency by supporting the following services on transport NEs:

- visualized E2E provisioning and
- management of PWE3 services
- VPLS services
- Native Ethernet services
- L3VPN services

## Transport Packet Service Performance Monitoring and Fault Diagnosis

The NCE supports E2E service configuration, one-click connectivity commissioning, one-click performance commissioning, instrument-free tests, performance statistics, one-click service diagnosis, loopback detection, and service path visualization. E2E configuration of native ETH/PWE3/VPLS/L3VPN/ composite services is implemented. One-click service diagnosis and visualized service paths improve the efficiency of transport packet service O&M.

- **Test and diagnosis:** The NCE provides the following functions:
  - Connectivity test of service, PW, and TNL for E-Line and E-LAN services
  - One-click configuration of LM and DM functions
  - Testing of packet loss and delay
  - Testing of throughput, packet loss rate, delay, and long-term packet loss rate of native Ethernet and MPLS services
- **One-click service diagnosis:** Layered fault diagnosis of service, PW, TNL, and ports of E-Line and E-LAN services is provided. In addition, diagnosis reports are provided to specify a fault to the specific looped point so that alarms can be reported to automatically disable the looped point.
- **Visualized service path troubleshooting:** Based on VLANs, the NCE quickly depicts the transmission service path. It allows you to query the real-time path of a MAC address on the transport network based on the base stations' MAC addresses. Loopback detection is performed based on service paths, and service loopback points are displayed in a view. You can query the performance statistics of the VUNI, PW, LSP, and port where the service is located based on services. You can also query ERPS in real time based on service paths and generate tree ring network protocol status.

## E2E RTN Service Management

E2E RTN services are supported, including TDM, EoS, E-Line, E-LAN, E-Line\_E-LAN, and PWE3 services and tunnels. They can be uniformly created and managed. In addition, E2E service templates are provided.

## 5.2.3 Access Network Management

### Access NEs

NCE supports the following series of access NEs: FTTx, DSLAM, MSAN, BITS, EDFA, and RPS.

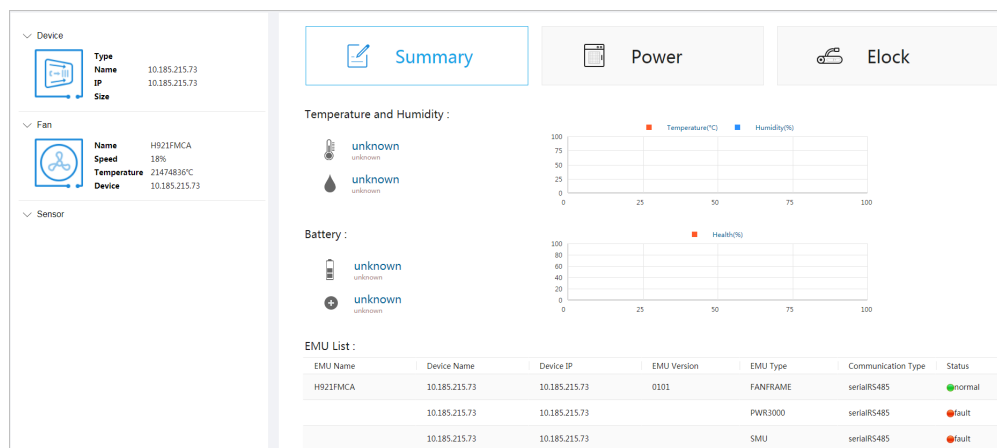
NCE can manage NEs on a NAT network. To ensure normal communication between NEs and the NCE server, you need to configure NAT on NCE.

### FTTx PnP

- **Configuration script application:** When maintenance personnel use commands to configure a device, the configuration commands can be written into a batch processing script and applied to the device from NCE. In this way, commands are issued in batches.
- **Automatic recovery after replacement:** If a remote MxU becomes faulty, onsite personnel can replace it. After the replacement, NCE automatically upgrades the software and restores configurations without requiring manual operations.
- **PnP deployment:** MxUs are usually installed in harsh environments (for example, in manholes or on poles). To simplify work for deployment personnel, NCE automatically upgrades software and applies configurations to powered-on MxUs.
- **Remote acceptance of broadband, narrowband, and IPTV services:** After deployment or troubleshooting, NCE can be used to perform remote acceptance for broadband, narrowband, and IPTV services. Software commissioning engineers do not need to visit the site.

### Intelligent FTTx Site Management

The intelligent site management solution can be used for FTTx sites. Sensor components are used to avert black-box management, remotely monitor site status in a visualized way, simplify door lock rights management, and remotely detect batteries. Site asset management, visualized site monitoring, and remote operations reduce the number of site visits, facilitate remote site maintenance, and save on maintenance costs.



## Remote Diagnosis

- **FTTC/B diagnosis view:** This view displays E2E links from CPE UNIs to OLT upstream ports to implement one-stop NE and link status monitoring and fault diagnosis. With this view, FTTC/B troubleshooting is simplified.
- **FTTH diagnosis view:** This view displays E2E links from ONT UNIs to OLT upstream ports to implement one-stop NE and link status monitoring and fault diagnosis. With this view, FTTH troubleshooting is simplified.
- **Remote emulation testing:** Maintenance personnel can remotely diagnose faults on voice, broadband, and other services.
- **Intelligent alarm analysis:** Alarm compression, correlation analysis, and other methods are provided to reduce the alarm quantity and help users identify root causes.
- **NE data verification:** NE configuration data is verified against the data planned by carriers to avoid data inconsistency and the resultant service problems.
- **ONT video quality diagnosis:** Faults of IPTV+cooperated OTT videos can be quickly diagnosed and demarcated. NCE collects quality indicators in real time, displays them in a visualized manner, and compares them to quickly demarcate faults.

## PON Leased Line O&M

You can customize a PON private line view by configuring the ONU type, ONU name matching rule, and ONU name keyword.

After the configuration is complete, you can view the overall information about ONUs (including the total number of ONUs, number of online ONUs, number of offline ONUs, and number of ONUs that contain alarms) in the PON private line view. In addition, you can view the details and alarm details of any ONU in the view.

## 5.2.4 IP Network Management

## 5.2.4.1 NE Management

### IP NEs

NCE supports the following series of IP NEs: PTN, NE, ATN, CX, service gateway, R/AR, switch, voice gateway, and security.

### PnP

Plug-and-play (PnP) facilitates remote commissioning and basic configuration of NEs in batches, freeing engineers from going to sites and greatly improving the deployment efficiency.

#### Scenario

PnP is used for making scripts and configuring NEs during deployment. It provides a rich set of system-defined templates, where users need to set only a few of parameters for generating basic NE scripts. DCN remote commissioning eliminates the need for planning before NE power-on, and NEs are automatically added to NCE for management.

During deployment, PnP is mainly used for remotely commissioning newly added NEs and bringing them online so that NCE can manage these NEs. PnP applies basic configurations to NEs in different networking scenarios to complete batch NE deployment.

#### Automatically Available DCN

- Connections are automatically established between NCE and NEs based on the automatically available DCN. Scripts are automatically generated based on the planning sheet.
- After NEs go online, templates are planned based on scenarios to implement PnP.
  - Templates can be customized based on L2+L3 and HVPN service scenarios.
  - The management IP addresses, NNI IP addresses, and IGP parameters can be automatically allocated for online NEs.

#### Custom deployment solution

Create a customization template based on the site scenario information and typical configuration, customize template parameter IDs and expressions, and create a deployment template group for the site scenario.

- Export the service planning table based on the deployment template and fill in the planning data. The custom deployment solution allows you to import device configuration planning information (such as NE addresses and interface IP addresses) in batches and customize the sequence of parameters in the planning table.
- NCE supports the import of device command scripts, the setting of parameter correlation between different device role templates, and the creation of scenario-based custom service deployment templates.

Basic and service configuration scripts are generated at the same time. With the DCN, devices can go online while configurations are applied.

## IP Network Troubleshooting

IP network troubleshooting helps users quickly locate faults in service paths, improving O&M efficiency.

IP network troubleshooting provides the following functions:

- **Unicast service path visualization:** E2E service paths and backup paths are displayed in the topology view. Backup paths support five backup modes: primary/secondary PW, VRRP, E-APS, TE hot standby, and VPN FRR. Paths are displayed at the service, tunnel, IP, and link layers. If a path is incomplete or used as a backup path, a message will be displayed asking users whether to display the historical paths that are complete and not used as backup paths.
- **Multicast service path visualization:** NCE can discover shared paths and shortest paths, and paths are displayed at the service, IP, and link layers.
- **Display of NE and link status:** After users select an NE or link in the topology view, the NE performance data or the link type, source, and sink are displayed. The performance data, alarm information, and optical module information of all NEs and links in the topology view are displayed on tab pages in the details area to help users with preliminary fault locating.
- **Fast fault diagnosis:** After users click **Quick Diagnosis**, path and service check items are executed layer by layer. The check results are displayed in a table. If a check item is abnormal, it is highlighted in red and handling suggestions are provided for it. Clicking an underscored record opens the associated window in the NE Explorer where users can quickly rectify faults.
- **Fault detection:** Faults can be detected through packet comparison, port loopback tests, ping tests, interface packet loss/bit error collection, TDM PW statistics, path detection, smart ping, ACL traffic statistics, or fault information collection, or by using the MultiCast Tools or IGP Source Tracing tool.

## IP Network Assurance

NCE provides various functions, such as network health checking, intelligent troubleshooting based on path visualization, automatic locating of top N typical alarms, and network-level alarm correlation. This greatly reduces skill requirements for fault locating. The average fault locating time is reduced from more than 1 hour to 10 minutes.

- **IP NE health check:** IP NE health status can be checked efficiently and automatically. Checking a single NE (optical power and IP address) only needs several seconds. The check efficiency is greatly improved because users no longer need to manually check configurations. In addition, this function reduces the potential faults caused by improper basic configurations.
- **PTN network health check:** This tool provides a centralized GUI for checking and viewing network running indicators. During routine maintenance, users can compare the current and historical network running statuses to detect risks and rectify faults in advance.
- **Intelligent troubleshooting based on path visualization:** NCE supports protection path discovery, covering five protection schemes (primary/secondary PW, VPN FRR, VRRP, E-APS, and TE hot standby) on the live network. It can also discover and display primary and backup paths to meet fault locating requirements during service switching. Paths are displayed by layer (including service, tunnel, route, and link layers) so that specific fault

locations can be easily identified. Path discovery in the VPLS and HVPLS scenarios and visualized fault locating based on paths are provided. NCE automatically determines the diagnosis process based on MBB scenarios and fault types (such as interruption, deterioration, and clock switching). It provides up to 300 check items, covering key MBB features and improving check accuracy and efficiency.

- **Automatic locating of top N alarms:** For top N alarms, NCE automatically selects check methods, completes fault diagnosis with just one click, and provides rectification suggestions.
- **Network-level alarm correlation:** By analyzing the alarms reported by IP NEs within a period, NCE identifies root alarms and correlative alarms based on rules and displays them to the maintenance personnel.

### 5.2.4.2 IP Service Management

NCE supports centralized and unified management of virtual private network (VPN) services, such as tunnels, L3VPN services, VPLS services, PWE3 services, and composite services. Specific functions include service provisioning, service monitoring, and service diagnosis.

### Service Provisioning

NCE provides a user-friendly graphical user interface (GUI) on which you can complete all service configuration operations. Parameters for multiple NEs can be automatically generated by using service templates. User configuration results can be previewed in the topology before being applied.

- FlexE Channel
  - Creating FlexE Channels.
  - Creating FlexE Channel Protection Groups.
- Dynamic Tunnel
  - Provision SR-TE and RSVP-TE tunnels.
  - Configure tunnel separation groups.
- SR Policy Tunnel
  - Provision SR policy tunnels.
  - Select the color attribute for SR policy tunnels.
  - Configure candidate paths.
- Static Tunnel
  - Deploy Static LSP or Static CR LSP services to implement MPLS access schemes.
  - Configure the link bandwidth threshold.  
During the establishment of a static CR LSP calculation path, the U2000 can generate a link weight based on the remaining link bandwidth and the threshold, achieving traffic balance.
- Dynamic L3VPN service
  - Provision dynamic unicast and multicast L3VPN services.
  - Provision services through templates.

- Create tunnels upon service creation.
- VPLS service
  - Manage VPLS services in Label Distribution Protocol (LDP) signaling (Martini) mode.
  - Manage VPLS services in Border Gateway Protocol (BGP) signaling (Kompella) mode.
  - Manage VPLS services for interworking of different virtual switch instances (VSIs).
- PWE3 service
  - Configure static and dynamic PWE3 services.
  - Manage PWE3 services in circuit emulation service (CES), asynchronous transfer mode (ATM), Ethernet (ETH), IP over PW, networking function (ATM IWF), or heterogeneous interworking mode.
  - Configure management PW.
  - Back up pseudo wire (PW) configurations.
  - Configure PW FRR.
  - Configure CES FPS.
- Composite service

You can manage the following composite services: **Customize**, **H-VPLS**, and **PWE3 in Dynamic L3VPN**. Different creation methods are provided for them.

  - **Customized**: Services can be combined in various types, including VPLS +PWE3, VPLS+L3VPN, PWE3+L3VPN, OptionA VPLS, OptionA PWE3, OptionA L3VPN, PWE3+PWE3. Users need to manually create or select existing services, and create a connection point to combine them into a composite service.
  - **H-VPLS**: After an NE is added to NCE as a VPLS node, PWE3 node, or PW switching node, NCE will automatically create the desired H-VPLS composite service over the NE.
  - **PWE3 in Dynamic L3VPN**: NCE automatically creates qualified PWE3+L3VPN services after the gateway IP address is set, the dynamic L3VPN is selected, and PWE3 is added.

## Automatic Service Discovery

The E2E service or tunnel data deployed on the network can be restored to NCE through service discovery so that these services can be managed in an E2E manner. This not only saves time but avoids the impact of misoperation on the original services.

- Static tunnels, VPLS services, PWE3 services, aggregation services, and composite services can be automatically discovered based on preset policies.
- Dynamic tunnels, and dynamic L3VPN services can be automatically discovered based on service templates.

## 360-Degree Service View

Clear and visible service status and service object relationships: Services are associated with tunnels, and tunnels are associated with routes. NCE clearly



displays the hierarchical object and bearer relationships, which facilitates fault locating and troubleshooting.

## **Service Diagnosis**

Diagnostic tools are used to check network connectivity and locate faults. You can generate diagnostic tasks according to selected services and directly perform operations on NEs in topology views. Diagnostic results can be directly displayed.

## **Service Check and Test**

- Configuration check: NCE can check consistency of VPN service configurations at different sites and show configuration error locations.
- Service continuity check: NCE can check service connectivity by means of ping and trace route tests, and locate faulty NEs.
- Protocol status test: NCE can check service protocol status and forwarding tables, and display error information to help you locate faults.

---

# 6 High Availability

---

During system running, unexpected faults may occur due to external environments, misoperations, or system factors. For these unknown risks, NCE provides hardware, software, and system-level availability protection solutions, which recover the system from faults to minimize the damage to the system.

## 6.1 Local HA

In the on-premises scenario, NCE provides detailed HA protection solutions for the hardware, virtualization layer, and application layer of a single site. These solutions can prevent unknown risks caused by hardware or software faults and ensure secure and stable running of NCE.

## 6.2 Disaster Recovery Solutions

Disaster Recovery solutions are provided to prevent unknown risks on the entire system and ensure secure and stable running of NCE.

## 6.1 Local HA

In the on-premises scenario, NCE provides detailed HA protection solutions for the hardware, virtualization layer, and application layer of a single site. These solutions can prevent unknown risks caused by hardware or software faults and ensure secure and stable running of NCE.

## HA of Application Layer

**Table 6-1** HA solutions for the application layer

Protection Solution	Description	Protection Capability
HA of application services	<p>Automatic switchover of application services in the manager+controller +analyzer deployment scenarios:</p> <ul style="list-style-type: none"> <li>Virtual nodes are deployed in active/standby mode: When the active and standby nodes are running properly, only the services on the active node are running. When the service monitor detects that the service processes on the active node are faulty, the service ports on the standby node are automatically enabled and the service instances on the standby node are started to provide services.</li> <li>Virtual nodes are deployed in cluster mode: When cluster nodes are running properly, each node is in the multi-active state. If one node fails, other nodes share the load capability of the faulty node to provide services for external systems in a balanced manner.</li> </ul>	switchover duration <= 5 minutes
	<p>Process restart: Process status is monitored in real time. If a process is stopped or faulty, a maximum of 10 consecutive attempts will be made to restart it. If all the attempts fail, an alarm will be reported to inform users of manual troubleshooting.</p>	Process restart time <= 5 minutes
Data HA	<p>Backup and restore: The backup and restore function is provided for data. Data is backed up in time. If data becomes abnormal, users can restore them to the normal state by using backup files.</p>	Restoration duration <= 60 minutes

Protection Solution	Description	Protection Capability
	Automatic database switchover: When the primary and secondary nodes (such as the DB nodes) are running properly, the database on the primary node is readable and writable, and the secondary database is read-only. However, if the primary node fails, the secondary node will take over service provisioning. The primary/secondary switchover does not affect services.	<ul style="list-style-type: none"> <li>● RPO = 1 minute</li> <li>● RTO = 1 minute</li> </ul>
<p>Notes:</p> <ol style="list-style-type: none"> <li>1. Recovery Point Objective (RPO): A service switchover policy that ensures the least data loss. It tasks the data recovery point as the objective and ensures that the data used for the service switchover is the latest backup data.</li> <li>2. Recovery Time Objective (RTO): The maximum acceptable amount of time for restoring a network or application and regaining access to data after an unexpected interruption.</li> </ol>		

## 6.2 Disaster Recovery Solutions

Disaster Recovery solutions are provided to prevent unknown risks on the entire system and ensure secure and stable running of NCE.

**Table 6-2** HA solutions at the DR system

Protection Solution	Description	Protection Capability
Active/standby switchover	NCE is deployed on primary and secondary sites. Data in each database is synchronized from the primary site to the secondary site based on the synchronization policy. If the primary site fails, users can immediately start the secondary site for using NCE.	<ul style="list-style-type: none"> <li>● RPO = 1 minute</li> <li>● RTO = 15 minutes</li> </ul>
Active/standby monitoring	If the heartbeat and replication links become abnormal, an alarm will be reported to inform users of manual troubleshooting.	N/A

Protection Solution	Description	Protection Capability
<p>Notes:</p> <ol style="list-style-type: none"> <li>1. Recovery Point Objective (RPO): A service switchover policy that ensures the least data loss. It tasks the data recovery point as the objective and ensures that the data used for the service switchover is the latest backup data.</li> <li>2. Recovery Time Objective (RTO): The maximum acceptable amount of time for restoring a network or application and regaining access to data after an unexpected interruption.</li> </ol>		

 **NOTE**

Historical performance data is not synchronized between the primary and secondary sites.

**Table 6-3** Scenario comparison of NCE DR solutions (manager)

DR Solution	Scenario
Automatic switchover (with the arbitration service)	There are three equipment rooms, and the statuses of the primary and secondary sites need to be monitored in real time. After a site-level fault occurs, an active/standby switchover needs to be quickly implemented to restore services.
Automatic switchover (without the arbitration service)	There are two equipment rooms, and the statuses of the primary and secondary sites need to be monitored in real time. After a site-level fault occurs, an active/standby switchover needs to be quickly implemented to restore services. In addition, services can bear the risks caused by the dual-active state.
Manual switchover	There are two equipment rooms, and the statuses of the primary and secondary sites are manually monitored. After a site-level fault occurs, the system does not have high requirements on the fault rectification time. Manual O&M plane can be performed.

## Manual Switchover

### Solution introduction:

The primary and secondary sites communicate with each other through heartbeat links and detect the status of the peer site in real time. The primary site synchronizes product data to the secondary site in real time through the data replication link to ensure product data consistency between the primary and secondary sites.

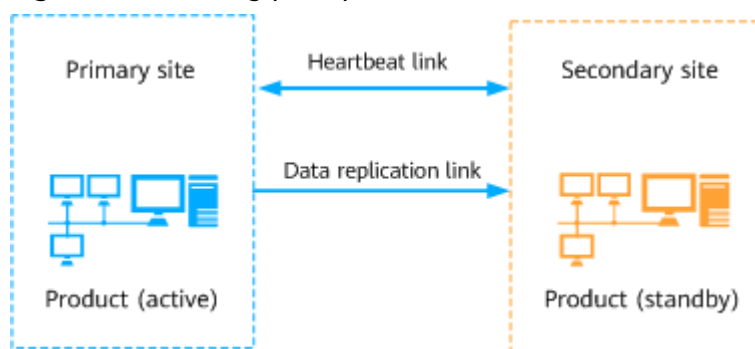
When a disaster occurs at the primary site, perform the takeover operation at the secondary site. The secondary site becomes the active site and provides services externally. The primary site becomes standby.

**Manual switchover trigger conditions:**

- The disaster such as an earthquake, fire, or power failure occurs at the primary site caused the system as a whole to be unable to provide services.
- The primary site is faulty, causing some key nodes to be damaged and unable to provide corresponding services. For example, database node (DB) corruption, platform service node (Common\_Service) corruption, management domain service node (NMS) corruption, control domain service node (Controller or TController) corruption.

**Solution schematic diagram:**

**Figure 6-1** Working principle of manual switchover in the DR system



The DR network can reuse the original network of NCE to reduce the network configuration of the primary and secondary sites.

**Table 6-4** DR network configuration

DR Link	IP Address	Network Plane
Data replication link	Replication IP address	DR network <b>NOTE</b> The DR network can reuse the inter-node communication network or northbound network or use an independent network.
Heartbeat link	Heartbeat IP address	DR network. The heartbeat IP address and replication IP address must be on the same network plane.

**Automatic Switchover (Without Arbitration Service)**

**Solution introduction:**

The primary and secondary sites communicate with each other through heartbeat links and detect the status of the peer site in real time. The primary site synchronizes product data to the secondary site in real time through the data replication link to ensure product data consistency between the primary and secondary sites.

If the primary site is powered off unexpectedly, the hardware is faulty, or the system breaks down, and the fault is not rectified within the specified time, the secondary site automatically becomes active and the primary site becomes standby after the fault is rectified.

If only the heartbeat link between the primary and secondary sites is interrupted, the secondary site automatically becomes active. In this case, the DR system is in the dual-active state and generates related alarms. However, both the primary and secondary sites are running properly.

- If the heartbeat link is recovered within 2 hours, about 3 to 5 minutes later the system enters the dual-active negotiation mode. The active site before the heartbeat link is interrupted automatically works as the active site, and the other site becomes the standby site. After the heartbeat status is normal and the active/standby relationship at the sites is restored to stable, the system automatically synchronizes full data of the product at the active site to the standby site to restore the product status. In addition, the product data at the active site is consistent with that at the standby site.
- If the heartbeat link is recovered after 2 hours, the system does not automatically perform an active/standby switchover. Users may perform operations at the two sites in the dual-active state and the automatic switchover may cause data loss. Determine whether to manually switch the active and standby sites based on the site requirements.

#### Automatic switchover trigger conditions:

- A disaster such as an earthquake, fire, or power failure occurs at the primary site, and the fault is not rectified within the specified time.
- In the manager+controller+analyzer compact deployment and manager deployment scenarios:
  - If any of the default key microservices of the system is faulty, the DR system triggers an automatic switchover to ensure normal service running. For details about the list of key microservices, see the **Pivotal Microservice** column in the **Processes and Services** sheet of *NCE Process and Service List*.

#### NOTE

To obtain *NCE Process and Service List*, perform the following steps:

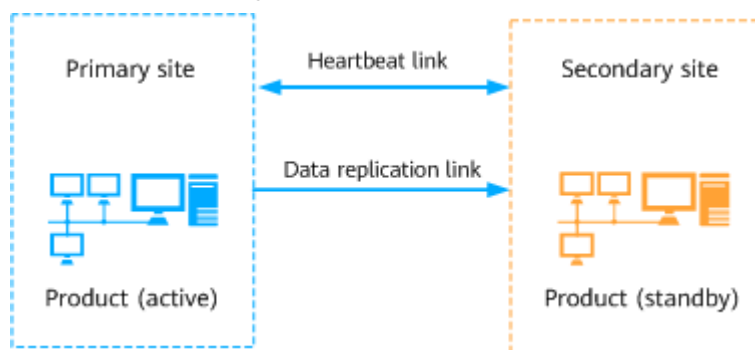
- For carrier users, log in to <https://support.huawei.com/carrier>. Search for "iMaster NCE" on the homepage. On the iMaster NCE page, search for "Common Documents". *Process and Service List* is contained in *Common Documents*.
- For enterprise user, log in to <https://support.huawei.com/enterprise>. Search for iMaster NCE on the homepage. On the iMaster NCE page, search for "Common Documents". *Process and Service List* is contained in *Common Documents*.
- If the service network (southbound or northbound network) is faulty due to a network port fault on the server, the system automatically triggers a switchover.
- If all database instances are faulty, the system automatically triggers a switchover.

**NOTE**

- Manager+Controller+Analyzer deployment scenarios, nodes and application services are deployed in active/standby or cluster mode, and local protection is configured. Key microservice failover, server service network ports failover and all database instances failover are not separately configured.
- The priorities of triggering an automatic switchover are as follows: All database instances are faulty > Server service network ports are faulty > Key microservices are faulty. If all database instances at the secondary site are faulty, an automatic switchover is not triggered even if key microservices at the primary site are faulty.

**Solution schematic diagram:**

**Figure 6-2** Working principle of automatic switchover (without the arbitration service) in the DR system



The DR network can reuse the original network of NCE to reduce the network configuration of the primary and secondary sites.

**Table 6-5** DR network configuration

DR Link	IP Address	Network Plane
Data replication link	Replication IP address	DR network <b>NOTE</b> The DR network can reuse the inter-node communication network or northbound network or use an independent network.
Heartbeat link	Heartbeat IP address	DR network. The heartbeat IP address and replication IP address must be on the same network plane.

**Automatic Switchover (with Arbitration Service)**

**Solution introduction:**

The arbitration service periodically checks the connectivity between the primary, secondary, and third-party site, and share the check results through arbitration site communication link. When the network connection is abnormal or a site fault causes an arbitration heartbeat exception, the arbitration service selects the



optimal site in the network based on the internal algorithms to perform an active/standby switchover.

#### Automatic switchover trigger conditions:

- A disaster such as an earthquake, fire, or power failure occurs at the primary site, and the fault is not rectified within the specified time.
- The heartbeat link between the primary and secondary sites is interrupted, and the arbitration site communication link between the primary site and the third-party site is interrupted.
- In the manager+controller+analyzer compact deployment and manager deployment scenarios:
  - If any of the default key microservices of the system is faulty, the DR system triggers an automatic switchover to ensure normal service running. For details about the list of key microservices, see the **Pivotal Microservice** column in the **Processes and Services** sheet of *NCE Process and Service List*.

#### NOTE

To obtain *NCE Process and Service List*, perform the following steps:

- For carrier users, log in to <https://support.huawei.com/carrier>. Search for "iMaster NCE" on the homepage. On the iMaster NCE page, search for "Common Documents". *Process and Service List* is contained in *Common Documents*.
- For enterprise user, log in to <https://support.huawei.com/enterprise>. Search for iMaster NCE on the homepage. On the iMaster NCE page, search for "Common Documents". *Process and Service List* is contained in *Common Documents*.
- If the service network (southbound or northbound network) is faulty due to a network port fault on the server, the system automatically triggers a switchover.
- If all database instances are faulty, the system automatically triggers a switchover.

#### NOTE

- Manager+Controller+Analyzer deployment scenarios, nodes and application services are deployed in active/standby or cluster mode, and local protection is configured. Key microservice failover, server service network ports failover and all database instances failover are not separately configured.
- The priorities of triggering an automatic switchover are as follows: All database instances are faulty > Server service network ports are faulty > Key microservices are faulty. If all database instances at the secondary site are faulty, an automatic switchover is not triggered even if key microservices at the primary site are faulty.

#### Arbitration service deployment:

- The CPU architecture of the primary site, secondary site and third-party site is required to be consistent. If the primary and secondary sites are ARM architecture servers, the third-party site is also required to be ARM architecture server.
- If the customer provides the hardware that meet the requirements as the third-party site, the third-party site must be exclusively occupied by the arbitration service and cannot be shared with other services.

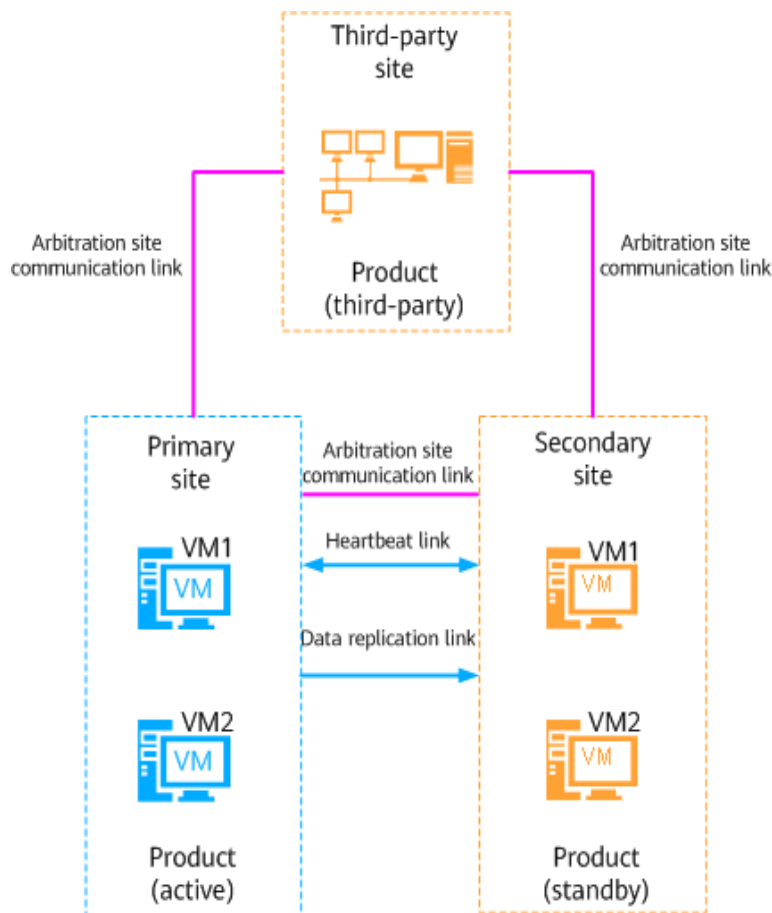
- One NCE DR system corresponds to one arbitration service at the third-party site. If multiple NCE DR systems exist on the live network, multiple arbitration services can be deployed at the same third-party site to reduce costs. A maximum of 10 arbitration services can be co-deployed at a third-party site, and the arbitration services of multiple software versions can be co-deployed. If a third-party site is faulty, all arbitration services at the third-party site cannot run properly. In this case, you need to reinstall all arbitration services.

 **NOTE**

When multiple arbitration services are deployed at a third-party site, the OS of the third-party site can trace only one external clock source. To ensure that the time of the third-party site is the same as that of all primary and secondary sites, the clocks of multiple DR systems must be the same.

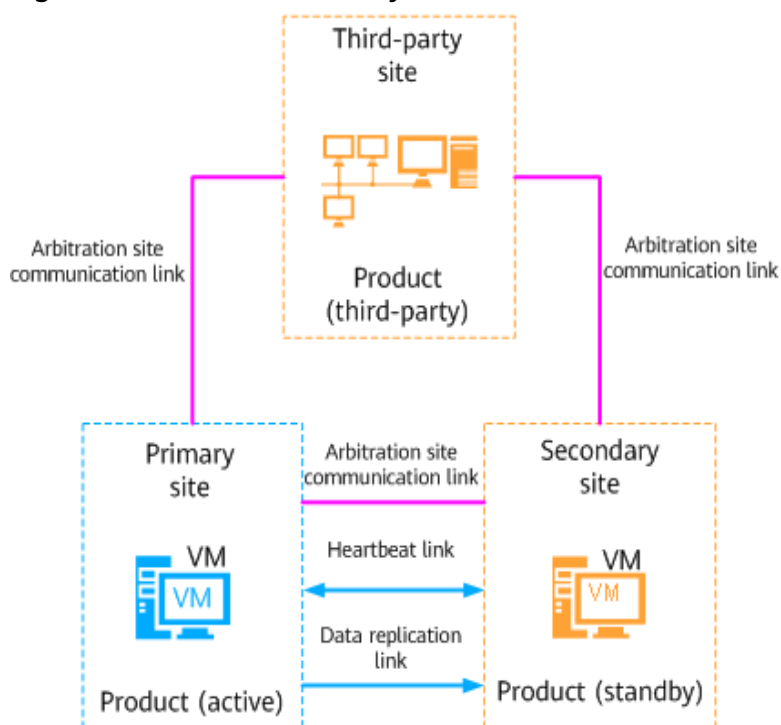
- NCE in Manager+Controller+Analyzer deployment scenarios adopts five-node arbitration service deployment. The arbitration service is deployed at three sites in 2+2+1 mode.
  - Two arbitration nodes are deployed at both the primary site and secondary site. It is recommended that the two arbitration nodes be deployed on the Common\_Service node. The arbitration nodes between the two sites are mutually protected. One arbitration node is deployed at the third-party site.
  - ETCD is deployed on the five arbitration nodes to form an etcd cluster. Monitor is deployed on the four nodes of the primary site and secondary site, which monitors the network connectivity between sites and saves the results in the etcd cluster.

Figure 6-3 A five-node DR system



- NCE in manager+controller+analyzer compact deployment and manager deployment scenarios adopts three-node arbitration service deployment. The arbitration service is deployed at three sites in 1+1+1 mode.
  - One arbitration node is deployed at the primary site. One arbitration node is deployed at the secondary site. It is required that the arbitration node be deployed on the Common\_Service node in manager+controller+analyzer compact deployment scenarios, and the arbitration node be deployed on the NMS\_Server node in manager deployment scenarios. One arbitration node is deployed at the third-party site.
  - ETCD is deployed on the three arbitration nodes to form an etcd cluster. Monitor is deployed on the two nodes of the primary site and secondary site, which monitors the network connectivity between sites and saves the results in the etcd cluster.

**Figure 6-4** A three-node DR system



The DR network can reuse the original network of NCE to reduce the network configuration of the primary and secondary sites.

**Table 6-6** DR network configuration

DR Link	IP Address	Network Plane
Data replication link	Replication IP address	DR network <b>NOTE</b> The DR network can reuse the inter-node communication network or northbound network or use an independent network.
Heartbeat link	Heartbeat IP address	DR network. The heartbeat IP address and replication IP address must be on the same network plane.

DR Link	IP Address	Network Plane
Arbitration site communication link	arbitration site communication IP address	<p>DR network</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>• The DR network can reuse the inter-node communication network or northbound network or use an independent network.</li><li>• It is not recommended that the arbitration site communication link reuse the northbound network. If the arbitration site communication link reuses the northbound network and both of them break down, the arbitration service cannot run properly. As a result, an exception may occur during automatic switchover. In this case, you cannot log in to the NCE management plane that is connected through the northbound network and therefore cannot manually switch over the system. The system cannot be restored in time.</li></ul>

# 7 Security

---

NCE uses the security architecture design that complies with industry standards and practices to ensure system, network, and application security from multiple layers.

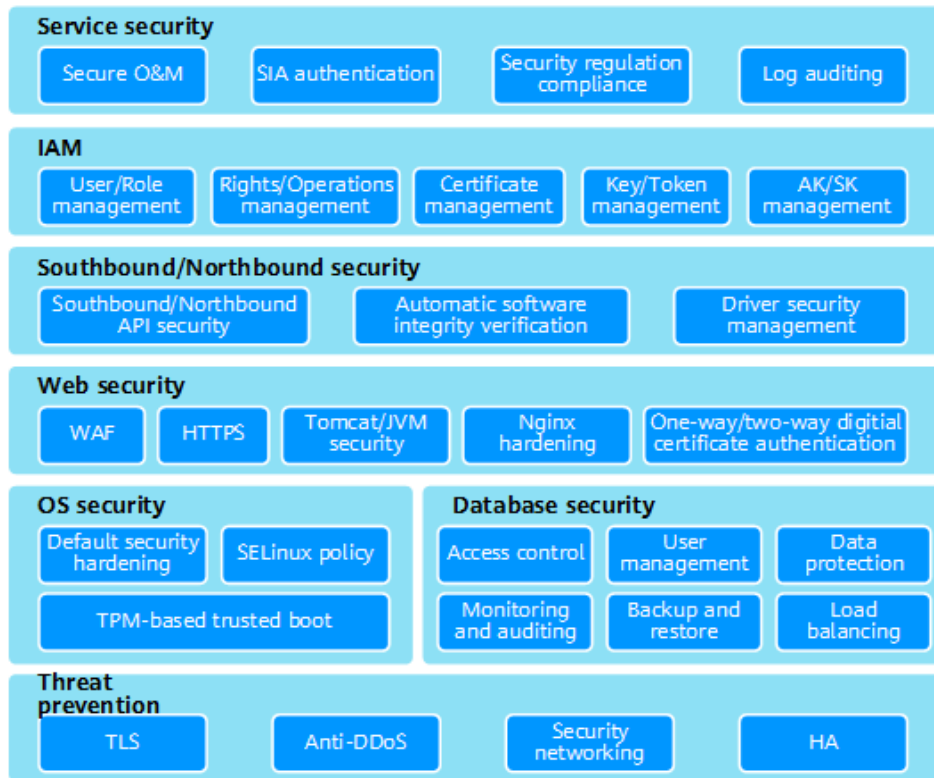
[7.1 Security Architecture](#)

[7.2 Security Functions](#)

## 7.1 Security Architecture

NCE security architecture consists of service security, authentication and access control management, API security, driver security, web security, operating system (OS) security, database security, and basic security threat prevention.

Figure 7-1 NCE security architecture



- Service security: secure O&M, SIA authentication, security regulation compliance, and log auditing.
- IAM (authentication and access control management): user management, role-based access control, policy management, token management, and user access credential management.
- Southbound and northbound security: API security, authentication and authorization, forcible access policy, log recording and auditing, and drive security management.
- Web service security: certificate management, service running environment Tomcat/JVM security, load balancing LVS&Nginx, and Redis memory database security hardening.
- OS security: system hardening, SELinux, and TPM-based trusted boot.
- Database security: user management, access control, data protection, monitoring and auditing, backup and restore, and load balancing.
- Basic security protection: TLS, anti-DDoS policy, interface access rate control, load protection, attack detection, security analysis, security zone allocation, and HA solution.

## 7.2 Security Functions

NCE security management aims to protect the confidentiality, integrity, and availability of products, services, and user data carried by the products and services and to ensure traceability and anti-attack capabilities in compliance with applicable laws. NCE provides multiple security functions to achieve these goals.

 **CAUTION**

- Designated computer principle: Using a designated server to install and run the NCE is recommended. This server must be separated from other office servers. Using a NCE server to act as an email server or handle emails from a public network is not recommended.
- Minimum installation principle: Installation of mandatory system applications and auxiliary tools only on the server that runs the NCE is recommended. Do not install software downloaded from unauthorized websites, unofficial software releases, software for testing, or any unnecessary applications of any kind.

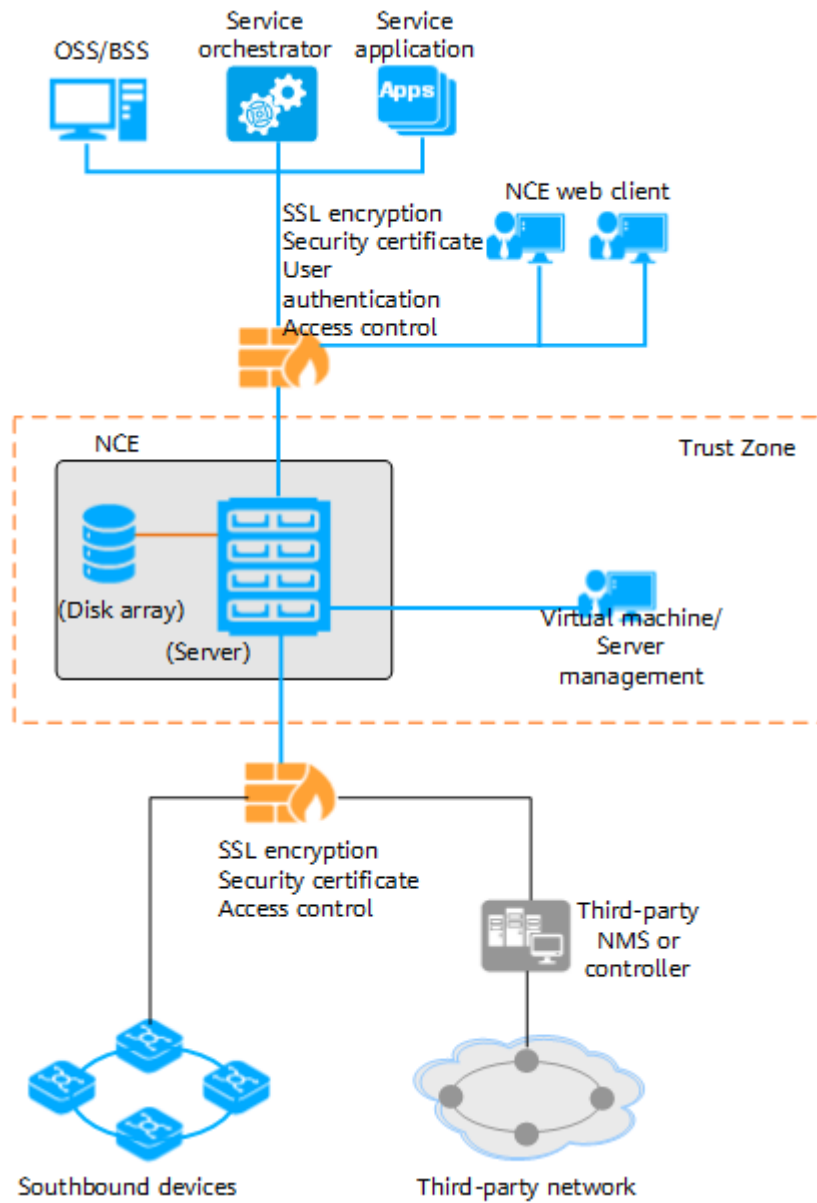
**Table 7-1** NCE security functions

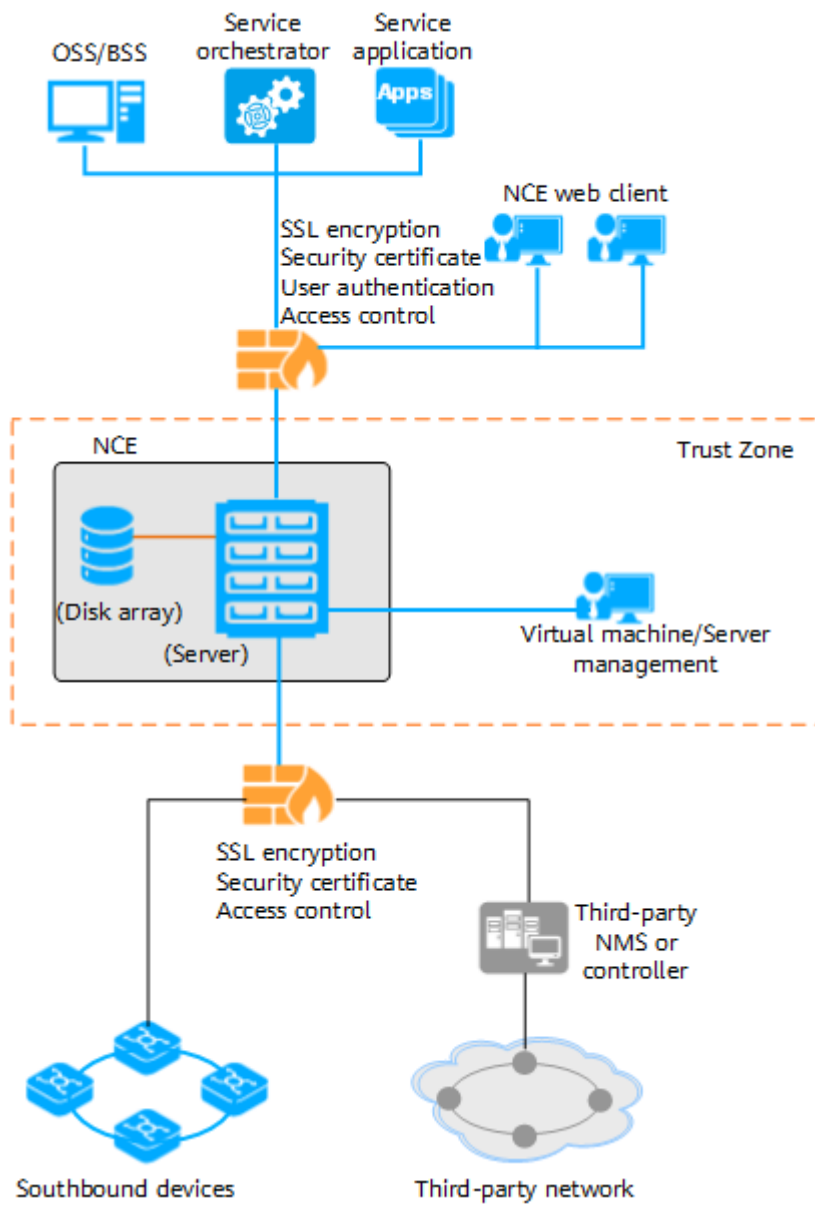
Security Function	Description
Area isolation	<ul style="list-style-type: none"> <li>• Internal communication and external communication are isolated and are controlled by different buses.</li> <li>• The management plane and O&amp;M plane are isolated, and access control is implemented through different interfaces and users.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The management plane refers to the plane that manages NCE software and hardware resources.</li> <li>• The O&amp;M plane refers to the plane that uses NCE to perform O&amp;M operations on networks and devices.</li> </ul>
User management	NCE can manage the roles, permissions, and access policies of system users.
Log management	NCE can manage operation logs, system logs, security logs, NE logs, and northbound logs and, dump Syslog logs.



Security Function	Description
Authentication and authorization management	<ul style="list-style-type: none"> <li>• The user passwords of the management plane and O&amp;M plane are encrypted and stored using the PBKDF2 irreversible algorithms.</li> <li>• NCE can interconnect with authentication, authorization, and accounting (AAA) systems such as the RADIUS or LDAP system, and manage and authenticate O&amp;M users in a unified manner.</li> <li>• NCE provides SSO authentication services based on CAS and SAML and supports northbound interconnection and integration authentication.</li> <li>• Digital certificates are used for identity authentication. Different certificates are used for northbound communication, southbound communication, internal communication, and interconnection with third-party systems, and the interconnections are isolated from each other. Certificate replacement and certificate lifecycle management are supported.</li> <li>• The SIA token is used for access control between services.</li> </ul>
Transmission security	Both internal and external transmission channels use security protocols such as HTTPS, TLS, SSH, SNMPv3, and SFTP.
OS security	SELinux is used to harden OS security, system service restrictions are minimized, and insecure services are disabled.
Database security	A dedicated low-permission system account is used to run the database, and database access permissions are restricted.
Sensitive data security	<ul style="list-style-type: none"> <li>• The PBKDF2 algorithm is used to securely store user passwords.</li> <li>• The AES128 or AES256 algorithm is used to encrypted and stored sensitive data.</li> <li>• In SSH communication, the DH or ECDH algorithm is used to exchange keys, and AES128-CTR, AES192-CTR, or AES256-CTR are used to encrypt data.</li> </ul>
Software integrity protection	NCE uses a software integrity protection solution equipped with CMS and OpenPGP. CMS is automatically called during software package installation and upgrade. OpenPGP is used when software package integrity needs to be manually verified.
Communication security	<ul style="list-style-type: none"> <li>• NCE supports the web application firewall (WAF).</li> <li>• NCE supports load balancing, traffic control, and access control.</li> <li>• NCE supports anti-DDoS.</li> </ul>
Network security	Network isolation and firewall deployment are used to ensure network security, as shown in <a href="#">Figure 7-2</a> .

**Figure 7-2** NCE networking security (on-premises deployment where southbound and northbound networks are isolated)





**NOTE**

If only NCE management components are deployed, no disk array is involved.

# 8 Personal Data and Privacy Protection

Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and many other international and regional laws and treaties. Privacy protection is a part of Huawei's fulfillment of social responsibilities. Huawei fully understands the importance of privacy protection and uses privacy protection as one of the company's highest guidelines, and complies with applicable privacy protection and personal data protection laws and regulations in all operating countries. Privacy includes space, psychology, and personal data. Privacy protection in Huawei products involves personal data.

## 8.1 Personal Data Scenarios

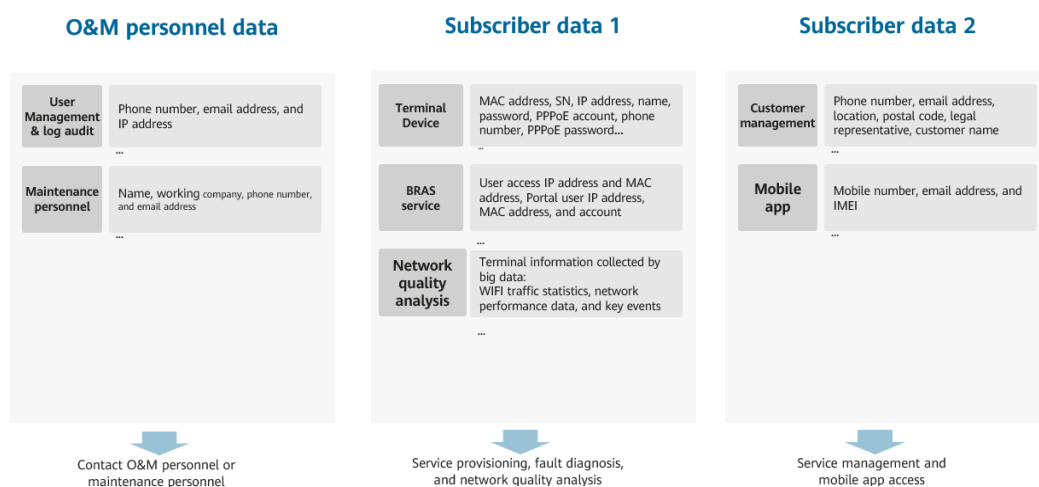
### 8.2 Principles and Key Technologies

### 8.3 Lifecycle Management

### 8.4 Privacy Protection Roles

## 8.1 Personal Data Scenarios

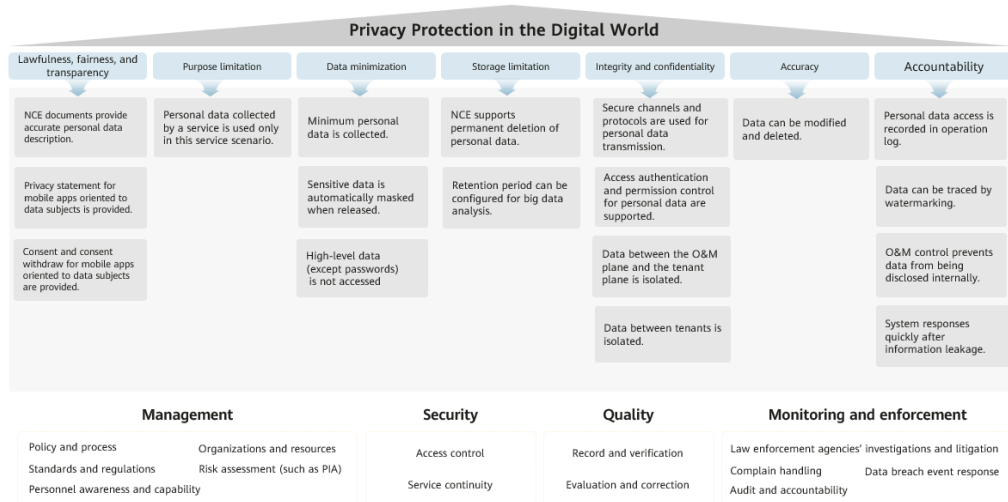
Figure 8-1 Main scope and scenarios of personal data in NCE



The preceding figure shows the personal data and usage in the current NCE version. For details about the personal data scope and protection measures, see "Subscriber Personal Data Protection" in *Network Cloud Engine Product Documentation*.

## 8.2 Principles and Key Technologies

Figure 8-2 Key technologies of NCE privacy protection



NCE complies with the following principles when processing personal data:

- **Lawfulness, fairness and transparency:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Huawei shall apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects concerned.
- **Storage limitation:** Personal data shall be kept for no longer than is necessary for the purposes for which the personal data is processed.
- **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date; Proper measures must be taken to promptly delete or correct inaccurate personal data based on the purpose of data processing.
- **Accountability:** The data controller must be responsible for and demonstrate compliance with the preceding principles.

## 8.3 Lifecycle Management

Based on the lifecycle of personal data in Generally Accepted Privacy Principles (GAPP), the roles (data controller, data processor, or device supplier) in different scenarios can be identified to meet compliance requirements in each phase.

Lifecycle	Compliance Requirement
<b>Notification to data subjects</b>	<ul style="list-style-type: none"> <li>Inform data subjects of the types of the data to be collected, processing purposes, methods, data subject rights, and security measures.</li> </ul>
<b>Data subjects' choice and consent</b>	<ul style="list-style-type: none"> <li>Personal data collection should be based on the consent of the data subject, written authorization from the customer, or other legal reasons.</li> <li>Grant the data subject the right to choose and ensure that the "consent" can be revoked.</li> </ul>
<b>Collection</b>	<ul style="list-style-type: none"> <li>Collect the least amount of personal data as possible based on purpose relevancy and necessity.</li> <li>If the data is collected from a third party, make sure that it is collected in a legal manner.</li> </ul>
<b>Use, retention, and disposal</b>	<ul style="list-style-type: none"> <li>Ensure that the purpose, methods and storage duration of personal data are consistent with of which the data subject is informed and with the scope authorized by the customer.</li> <li>Ensure the accuracy, integrity, and relevance of personal data based on personal data processing purposes.</li> <li>Provide a security protection mechanism for personal data to prevent unauthorized or improper use, abuse, and disclosure of personal data.</li> </ul>
<b>Disclosure to third parties</b>	<ul style="list-style-type: none"> <li>Suppliers and partners (third parties) that process personal data shall be properly certified based on risks to ensure that they can provide security measures for personal data processing. In addition, third parties shall be required on the contract to provide the same level of data protection as Huawei.</li> <li>Third parties shall not handle personal data beyond contract and instructions.</li> <li>When jointly handle personal data with a third party , the responsibilities of each party shall be specified in the contract.</li> </ul>

<p><b>Legal transfer of user data</b></p>	<ul style="list-style-type: none"> <li>• Before transferring personal data across borders, consult with the corresponding data protection officer (DPO) or legal affairs department.</li> <li>• Before personal data is transferred out of the European Economic Area (EEA), a data transfer agreement required by the EU shall be signed or customer's explicit consent shall be obtained. The entity that receives personal data shall comply with the basic principles of personal data processing to provide sufficient privacy protection.</li> </ul>
<p><b>Data subject access</b></p>	<ul style="list-style-type: none"> <li>• As a data controller, provide a reasonable access mechanism for data subjects and allow them to update, destroy, or transfer personal data if necessary.</li> </ul>

## 8.4 Privacy Protection Roles

**Carriers** are responsible for O&M and operation of products and determine the purpose and method of personal data processing. They are **data controllers**. Huawei is responsible for product delivery and is an **equipment provider**.

# 9 Specifications

NCE specifications include performance specifications, NE management capabilities, and service management capabilities.

## [9.1 System-Wide Performance Specifications](#)

### [9.2 NE Management Capabilities and Maximum Concurrent Client Connections](#)

### [9.3 Service Management Capabilities](#)

### [9.4 Equivalent Coefficients](#)

### [9.5 Equivalent Routes](#)

## 9.1 System-Wide Performance Specifications

### Basic Capabilities

**Table 9-1** Performance Indicators

Category	Indicator	Value
System startup and shutdown	System startup time (70% of the management capacity)	≤ 10 minutes
	System shutdown time (70% of the management capacity)	≤ 10 minutes
System database	Database restoration time	≤ 60 minutes
Protection performance	Application layer protection	<ul style="list-style-type: none"><li>Recovery point objective (RPO) = 0 seconds</li><li>Recovery time objective (RTO) ≤ 5 minutes</li></ul>
	Database protection	<ul style="list-style-type: none"><li>RPO = 60 seconds</li><li>RTO ≤ 60 seconds</li></ul>



Category	Indicator	Value
	1:N blade cluster	<ul style="list-style-type: none"> <li>RPO = 0 seconds</li> <li>RTO ≤ 15 minutes</li> </ul>
	Disaster recovery	<ul style="list-style-type: none"> <li>RPO = 60 seconds</li> <li>RTO ≤ 15 minutes</li> </ul>
Log capacity	Operation logs and system logs	≤ 1,000,000 Storage duration in database: 90 days
NE upgrade	Concurrent NE upgrades	≤ 60

## Alarm Management Capabilities

**Table 9-2** Alarm management indicators

Indicator	Value
Alarm response speed	In normal circumstances, alarms are displayed on NCE within 10 seconds after they are generated on NEs.
Alarm handling capability	Normally, <ul style="list-style-type: none"> <li>100 alarms/second when NCE manages NEs in all domains</li> <li>50 alarms/second when NCE manages only access NEs</li> <li>100 alarms/second when NCE manages only IP or transport NEs</li> </ul> In peak hours, <ul style="list-style-type: none"> <li>No alarm loss within 15 seconds when not more than 1000 alarms are reported per second</li> </ul>
Historical alarm storage duration in database	180 days

**Table 9-3** Relationship between the alarm capacity and the NE management scale

Management Scale	Maximum Current Alarms (unit: 10,000)	Maximum Historical Alarms (unit: 10,000)
2000	2	100
6000	5	200
15000	10	400
30000	10	400
50000	20	800

Management Scale	Maximum Current Alarms (unit: 10,000)	Maximum Historical Alarms (unit: 10,000)
80000	30	1200
80000	30	1200

 NOTE

For details about the NE management scale of NCE, see [9.2 NE Management Capabilities and Maximum Concurrent Client Connections](#).

## Topology Capabilities

Indicator	Value
Links in the current topology	≤ 200,000
Subnets	The number of subnets is not limited. Each subnet can contain a maximum of 500 physical NEs at a maximum of six layers. 200 physical NEs are recommended.
HWECC and IP over DCC networking capacity	<ul style="list-style-type: none"> <li>• GNEs: ≤ 3000</li> </ul> <p><b>NOTE</b> A single instance can manage 500 GNEs.</p> <ul style="list-style-type: none"> <li>• NEs managed by each GNE: ≤ 128 (50 is recommended)</li> </ul>

## User Management Capabilities

Indicator	Value
Users	≤ 2000
User groups	≤ 500
Object sets	≤ 100
Operation sets	≤ 255

## Southbound Performance Collection Capabilities

### NOTE

- The PMS performance data can be collected in SNMP, Bulk, or Qx mode. The maximum number of equivalent records that can be collected in each mode are as follows (in the unit of maximum equivalent records/15 minutes):
  - SNMP mode: 150,000
  - Bulk mode: 500,000
  - Qx mode: 100,000
- If multiple collection methods are used, conversion is required. For example, if SNMP +Bulk is used for collection and 50,000 records are collected in SNMP mode, the number of records collected in Bulk mode can be calculated as follows:  

$$X=50/15 \times (15 - 5) \approx 33$$

**Table 9-4** PMS performance collection indicators (transport domain)

Collection Mode	With Max/Min Data Aggregation	Equivalent NEs	Collection Capability (Maximum Equivalent Records/15 Minutes)
SNMP	N	2,000	20,000
SNMP	Y	2,000	13,000
SNMP	N	6,000	60,000
SNMP	Y	6,000	40,000
SNMP	N	15,000	150,000
SNMP	Y	15,000	100,000
SNMP	N	30,000	150,000
SNMP	Y	30,000	100,000
SNMP	N	50,000	150,000
SNMP	Y	50,000	100,000
Qx	-	2,000	20,000
Qx	-	6,000	40,000
Qx	-	15,000	80,000
Qx	-	30,000	100,000
Qx	-	50,000	100,000

**Table 9-5** PMS performance collection indicators (IP domain)

Collection Mode	With Max/Min Data Aggregation	Equivalent NEs	Collection Capability (Maximum Equivalent Records/15 Minutes)
SNMP	N	2,000	20,000

Collection Mode	With Max/Min Data Aggregation	Equivalent NEs	Collection Capability (Maximum Equivalent Records/15 Minutes)
SNMP	Y	2,000	13,000
SNMP	N	6,000	60,000
SNMP	Y	6,000	40,000
SNMP	N	15,000	150,000
SNMP	Y	15,000	100,000
SNMP	N	30,000	150,000
SNMP	Y	30,000	100,000
SNMP	N	50,000	150,000
SNMP	Y	50,000	100,000
BULK	N	2,000	66,000
BULK	Y	2,000	44,022
BULK	N	6,000	200,000
BULK	Y	6,000	133,400
BULK	N	15,000	500,000
BULK	Y	15,000	333,500
BULK	N	30,000	500,000
BULK	Y	30,000	333,500
BULK	N	50,000	500,000
BULK	Y	50,000	333,500
Qx	-	2,000	20,000
Qx	-	6,000	40,000
Qx	-	15,000	80,000
Qx	-	30,000	100,000
Qx	-	50,000	100,000

**Table 9-6** PMS performance collection indicators (access domain)

Collection Mode	With Max/Min Data Aggregation	Equivalent NEs	Collection Capability (Maximum Equivalent Records/15 Minutes)
SNMP	N	2,000	20,000

Collection Mode	With Max/Min Data Aggregation	Equivalent NEs	Collection Capability (Maximum Equivalent Records/15 Minutes)
SNMP	Y	2,000	13,000
SNMP	N	6,000	60,000
SNMP	Y	6,000	40,000
SNMP	N	15,000	150,000
SNMP	Y	15,000	100,000
SNMP	N	30,000	150,000
SNMP	Y	30,000	100,000
SNMP	N	50,000	150,000
SNMP	Y	50,000	100,000
SNMP	N	80,000	150,000
SNMP	Y	80,000	100,000
BULK	N	2,000	266,000
BULK	Y	2,000	177,422
BULK	N	6,000	800,000
BULK	Y	6,000	533,600
BULK	N	15,000	2,000,000
BULK	Y	15,000	1,334,000
BULK	N	30,000	2,000,000
BULK	Y	30,000	1,334,000
BULK	N	50,000	2,000,000
BULK	Y	50,000	1,334,000
BULK	N	80,000	2,000,000
BULK	Y	80,000	1,334,000

## NBI Capabilities

Table 9-7 NBI concurrency indicators

Protocol	Maximum Concurrent Requests
CORBA	4

Protocol	Maximum Concurrent Requests
XML	20
RESTful	10
TL1	30

 **NOTE**

For CORBA, XML, and REST, the number of concurrent requests refers to the maximum number of interfaces that OSSs can invoke. The number is collected among all OSSs and interfaces. For example, if the number is 4, it is probable that one OSS invokes four interfaces (a, b, c, d) at the same time, or four OSSs invoke one interface (a) at the same time.

**Table 9-8** OSS connection indicators

Protocol	Maximum OSS Connections
SNMP	A maximum of 10 OSSs can be connected to NCE.
TEXT	<ul style="list-style-type: none"> <li>As the FTP/SFTP client, NCE transmits files to only one OSS.</li> <li>As the FTP/SFTP server, NCE can be accessed by a maximum of three OSSs.</li> </ul>

 **NOTE**

For SNMP and TEXT, the number of NCE connections is collected by OSS.

## 9.2 NE Management Capabilities and Maximum Concurrent Client Connections

The number of equivalent NEs, number of clients, and number of physical NEs are key indicators for measuring the NE management capability of NCE. The management capabilities of NCE vary with hardware configurations.

**Table 9-9** Maximum NE management capability and client connection indicators (transport domain)

Component	Maximum Physical NEs	Maximum Equivalent NEs	Maximum Concurrent Client Connections
Manager	N/A	2,000	32
Manager	N/A	6,000	64

Component	Maximum Physical NEs	Maximum Equivalent NEs	Maximum Concurrent Client Connections
Manager	N/A	15,000	100
Manager	N/A	30,000	200

**Table 9-10** Maximum NE management capability and client connection indicators (IP domain)

Maximum Physical NEs	Maximum Equivalent NEs	Maximum Concurrent Client Connections
N/A	2,000	32
N/A	6,000	64
N/A	15,000	100
N/A	30,000	200

**Table 9-11** Maximum NE management capability and client connection indicators (Access Manager)

Sub-domain	Maximum Physical Nodes	Maximum Equivalent NEs	Maximum Concurrent Client Connections
FTTH	200,000 lines	2,000	32
FTTH	600,000 lines	6,000	64
FTTH	1,200,000 lines on no more than 30,000 physical NEs	15,000	100
FTTH	2,400,000 lines on no more than 60,000 physical NEs <b>NOTE</b> In a certain scenario, 4,000,000 lines on no more than 60,000 NEs are supported.	30,000	200
FTTB/C	200,000 lines	2,000	32
FTTB/C	600,000 lines	6,000	64
FTTB/C	1,200,000 lines on no more than 30,000 physical NEs	15,000	100

Sub-domain	Maximum Physical Nodes	Maximum Equivalent NEs	Maximum Concurrent Client Connections
FTTB/C	2,000,000 lines on no more than 30,000 physical NEs	30,000	200
DSLAM/MSAN	500,000 lines	2,000	32
DSLAM/MSAN	1,000,000 lines	6,000	64
DSLAM/MSAN	1,920,000 lines on no more than 30,000 physical NEs	15,000	100
DSLAM/MSAN	4,000,000 lines on no more than 60,000 physical NEs	30,000	200

 **NOTE**

The NCE-CrossDomain scenario is a combination of IP, T, and FAN domains, including IP+T+FAN, IP+T, T+FAN, and IP+FAN scenarios.

**Table 9-12** Maximum NE management capability and client connection indicators (NCE-CrossDomain)

Component	Maximum Physical NEs	Maximum Equivalent NEs Maximum Concurrent Client Connections
The number of equivalent NEs must meet the requirement.	2,000	32
The number of equivalent NEs must meet the requirement.	6,000	64
The number of equivalent NEs must meet the requirement.	15,000	100
The number of equivalent NEs must meet the requirement.	30,000	200



## 9.3 Service Management Capabilities

### Transport Trail Management Capability

Equivalent NEs	Component	Maximum SDH Trails	Maximum WDM Trails
2000	Manager	90,000	30,000
6000	Manager	90,000	30,000
15000	Manager	220,000	70,000
30000	Manager	500,000	300,000

### Tunnel and service access interface capability

Domain	Category	Indicator (Manager)
NCE (IP Domain)	Number of tunnels	Number of tunnels = $N \times 6$ (with hot-standby) N indicates the maximum number of equivalent NEs.
NCE (IP Domain)	Number of LSPs	<ul style="list-style-type: none"> <li>If only RSVP or SR tunnels are involved, NCE can manage a maximum of 128,000 dynamic tunnels and 256,000 LSPs, assuming that hot standby is enabled for all of these tunnels.</li> <li>If only SR Policies are involved, NCE can manage a maximum of 64,000 dynamic tunnels and 128,000 LSPs, assuming that hot standby is enabled for all of these tunnels.</li> <li>If RSVP tunnels, SR tunnels, and SR Policies are all involved, NCE can manage a maximum of 128,000 dynamic tunnels (including 64,000 SR Policies at most) and 256,000 LSPs.</li> </ul>
NCE (Transport Domain)	Number of tunnels	$N \times 6$ (N indicates the number of equivalent NEs.)
NCE (Transport Domain)	Number of IP service access interfaces	$N \times 20$ (N indicates the number of equivalent NEs.)

Domain	Category	Indicator (Manager)
NCE (IP Domain)	Number of IP service access interfaces	IP service interfaces include access service interfaces and network service interfaces. The total number of IP service interfaces is calculated as follows:  Total number of IP service interfaces = $N \times 20$  N indicates the maximum number of equivalent NEs.

## What-if Analysis Management Capabilities

Indicator	Value
Total number of equivalent IP NEs	6,000 <b>NOTE</b> For details about how to calculate the number of equivalent NEs, see <a href="#">9.4.2 Equivalent NEs in the IP Domain</a> .
Total number of equivalent routes	20,000,000
Total number of IP links	30,000
Total number of flows	100,000
Total number of tunnels	25,000
Period of load data that can be synchronized	30 days
IF definition that can be created (including setting fault points and modifying TE configuration parameters)	50
Simulation analysis time	< 1 hour
Number of users who can concurrently perform simulation analysis	1
Number of users who can concurrently view analysis results	5

## 9.4 Equivalent Coefficients

Equivalent coefficients are the ratios of the resources occupied by physical NEs or ports to the resources occupied by equivalent NEs.

## Definition

- Equivalent NE: a uniform criterion used to describe and calculate the management capabilities of NCE. This criterion is needed because different types of NEs occupy different system resources to support different functions, features, cross-connect capacities, and numbers of boards, ports, and channels. Therefore, different types of NEs and ports must be converted to equivalent NEs based on the number of system resources they occupy. An equivalent NE occupies as many system resources as an STM-1 transport NE.
- Equivalent coefficient: Resources occupied by physical NEs or ports/Resources occupied by equivalent NEs

## Calculation

The number of equivalent NEs that NCE can manage is calculated according to the following rules:

- Basic unit of equivalent NEs: OptiX OSN 1800 I
- The equivalent coefficients of third-party NEs are 1. The equivalent coefficient of OEM devices is the same as that of Huawei devices.
- Number of equivalent NEs = Number of NEs of type 1 x Equivalent coefficient of type 1 + ... + Number of NEs of type  $n$  x Equivalent coefficient of type  $n$

### 9.4.1 Equivalent NEs in the Transport Domain

Number of equivalent NEs in the transport domain = Number of transport NEs of type 1 x Equivalent coefficient of type 1 + ... + Number of transport NEs of type  $n$  x Equivalent coefficient of type  $n$

#### NOTE

For example, if there are 5 OptiX OSN 9500s (equivalent coefficient: 10), 10 OptiX OSN 7500s (equivalent coefficient: 6.5), and 100 OptiX OSN 3500s (equivalent coefficient: 4.5), then: Number of equivalent NEs in the transport domain =  $5 \times 10 + 10 \times 6.5 + 100 \times 4.5 = 565$

**Table 9-13** describes the equivalent coefficients for NEs in the transport domain.

**Table 9-13** Equivalent coefficients for NEs in transport domain

NE Series	NE Type	Equivalent Coefficient
MSTP series	OptiX OSN 50	0.5
	OptiX OSN 80	2
	OptiX OSN 500	1
	OptiX OSN 550	2.5
	OptiX OSN 580	4
	OptiX OSN 1500	2.5
	OptiX OSN 2000	2

NE Series	NE Type	Equivalent Coefficient
	OptiX OSN 2500	3.5
	OptiX OSN 2500 REG	3.5
	OptiX OSN 3500	4.5
	OptiX OSN 3580	4.5
	OptiX OSN 7500	6.5
	OptiX OSN 7500 II	6.5
	OptiX OSN 9500	10
	OptiX OSN 9560	20
	OptiX 10G MADM(Metro 5000)	4
	OptiX 155/622(Metro 2050)	2
	OptiX 155/622H	1
	OptiX 155/622H(Metro 1000)	1
	OptiX 2500+(Metro 3000)	3
	OptiX Metro 100	0.5
	OptiX Metro 1000V3	1
	OptiX Metro 1050	1.5
	OptiX Metro 1100	1.5
	OptiX Metro 200	0.5
	OptiX Metro 3100	3
	OptiX Metro 500	1
	OptiX 2500	3
	OptiX 2500+	3
	SDH Virtual NE	0.2
Metro WDM series	OptiX Metro 6020	1
	OptiX Metro 6040	1
	OptiX Metro 6040 V2	1
	OptiX Metro 6100	1.5
	OptiX Metro 6100V1	1.5
	OptiX Metro 6100V1E	1.5
	OptiX OSN 900A	1

NE Series	NE Type	Equivalent Coefficient
LH WDM series	OptiX BWS 320G (OAS/OCI/OIS)	1.5
	OptiX BWS 320GV3	1.5
	OptiX BWS 1600G Subrack	1.5 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX BWS 1600G OLA Subrack	1.5 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OTU40000	1
NG WDM series	OptiX OSN 1800	1
	OptiX OSN 1800 I E	2
	OptiX OSN 1800 II E	2
	OptiX OSN 1800 II TP Subrack	1 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 1800 V Subrack	4 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 1832	6
	OptiX OSN 1832 X4 E	2
	OptiX OSN 1832 X8	1
	OptiX OSN 1832 X8 E	2
	OptiX OSN 1832 X16 Subrack	4 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 3800	1.5
	OptiX OSN 6800 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 8800 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 8800 T16 Subrack	4 x <i>N</i> <i>N</i> indicates the number of subracks.

NE Series	NE Type	Equivalent Coefficient
	OptiX OSN 8800 T32 Subrack	6 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 8800 T64 Subrack	12 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 U16 Subrack	6 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 U32 Subrack	10 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 U64 Subrack	20 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 M12 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 M24 Subrack	6 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9600 P32 Subrack	10x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 U16 Subrack	6 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 U32 Subrack	10 x <i>N</i> <i>N</i> indicates the number of subracks.

NE Series	NE Type	Equivalent Coefficient
	OptiX OSN 9800 U64 Subrack	20 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 M12 Subrack	2 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 M24 Subrack	6 x <i>N</i> <i>N</i> indicates the number of subracks.
	OptiX OSN 9800 P32 Subrack	10x <i>N</i> <i>N</i> indicates the number of subracks.
	HUAWEI OSN902	1
	OptiX OSN 880	1
	OptiXtrans DC908 Subrack	1 x <i>N</i> <i>N</i> indicates the number of subracks.
	WDM Virtual NE	0.2
RTN series	OptiX RTN 310	0.5
	OptiX RTN 320	1
	OptiX RTN 360	1
	OptiX RTN 380	1
	OptiX RTN 380e	1
	OptiX RTN 380A	1
	OptiX RTN 380AX	1
	OptiX RTN 380H	1
	OptiX RTN 605	0.4
	OptiX RTN 610	0.4
	OptiX RTN 620	0.5
	OptiX RTN 905	0.5
	OptiX RTN 905e	0.5
	OptiX RTN 910	0.5
	OptiX RTN 910A	0.5

NE Series	NE Type	Equivalent Coefficient
	OptiX RTN 950	1
	OptiX RTN 950A	1
	OptiX RTN 980	2.5
	OptiX RTN 980L	2.5
	OptiX RTN 510	0.5
	NEC 5000S	1
	OptiX RTN FlexPort80	1
	PTP 250	1
	PTP 500	1
	PTP 650	1
	PMP 450	1
	X-1200	1
	ePMP 1000	1
PTN series	OptiX PTN 1900	2.5
	OptiX PTN 3900	4.5
	OptiX PTN 3900-8	4
	OptiX PTN 905	0.4
	OptiX PTN 905A	0.4
	OptiX PTN 905B	0.4
	OptiX PTN 906A	0.4
	OptiX PTN 906AI	0.4
	OptiX PTN 906B	0.4
	OptiX PTN 910	0.5
	OptiX PTN 910-F	0.4
	OptiX PTN 912	0.5
	OptiX PTN 950	1
	OptiX PTN 960	1.5
	Layer 2 Virtual NE	1
	Layer 3 Virtual NE	1
	Physical Layer Virtual NE	1



NE Series	NE Type	Equivalent Coefficient
Pre-configuration NE		Equal to a real NE
3rd-Party NE		1

## 9.4.2 Equivalent NEs in the IP Domain

Number of equivalent NEs in the IP domain = Number of IP NEs of type 1 x Equivalent coefficient of type 1 + ... + Number of IP NEs of type  $n$  x Equivalent coefficient of type  $n$

### NOTE

For example, if there are 5 NE5000Es (equivalent coefficient: 10), 200 S5300s (equivalent coefficient: 1.25), and 1000 CX200s (equivalent coefficient: 0.625), then:

Number of equivalent NEs in the IP domain =  $5 \times 10 + 200 \times 1.25 + 1000 \times 0.625 = 925$

Equivalent coefficients of NEs in the IP domain are shown in [Table 9-14](#) describes the equivalent coefficients for NEs in the IP domain.

**Table 9-14** Equivalent coefficients for NEs in the IP domain

NE Series	NE Type	Equivalent Coefficient
Router	NE05/NE08(E)/NE16(E)	0.75
	NE05E-S/NE05E-M	0.5
	NE08E-S/NE08E-M	1.0
	NE20/NE20E	1.25
	NE20E-S4	0.5
	NE20E-S8/S16/S8A/S16A	1.0
	NE20E-M2E/M2F	0.5
	NE40/NE80	5.0
	NE40E	2.5
	NE40E-X1	0.5
	NE40E-X2	1.0
	NE40E-X3/X3A	1.25
	NE40E-4	1.25
	NE40E-X4A(V8)	1.25
NE40E-X8/X8A	2.5	

NE Series	NE Type	Equivalent Coefficient
	NE40E-X8(V8)/X8A(V8)/X8C(V8)	2.5
	NE40E-X8AK(V8)	2.5
	NE40E-8	2.5
	NE40E-X16(V8)/X16A(V8)	5.0
	NE40E-X16/X16A/X16B	5.0
	NE40E-X16C(V8)	5.0
	NE40E-M8A/M16A	1.0
	NE40E-M2E/NE40E-M2F/NE40E-M2H/NE40E-M2K	0.5
	NE40E-F1A	0.5
	NE40E-FW	4.0
	NE80E	5.0
	NE5000E	10.0 x <i>N</i> <i>N</i> indicates the number of chassis.
	AR150	0.125
	AR200	0.125
	AR1200/AR2200/AR3200/AR3600 series	0.25
	AR6120/AR6120-S/AR6120-VW	0.25
	NE16EX	0.25
	R series	1.0
	AR18/19/28/29/46/49 series	0.25
	NE9000/NE9000-20	10.0
	NE9000-8	5.0
	NetEngine 8000 X4/X8	2.5
	NetEngine 8000 F1A	0.5
	NetEngine 8000 M1A/M1D	0.5
	NetEngine 8000 M6/M6K	0.5
	NetEngine 8000 M8/M8K	1.0
	NetEngine 8000 M14/M14K	1.0

NE Series	NE Type	Equivalent Coefficient
	RM9000	1.0
Switch	S2000 series	0.125
	S2300 series	0.625
	S2700 series	0.625
	S3000 series	0.125
	S3300 series	0.75
	S3500 series	0.125
	S3700 series	0.75
	S3900 series	0.125
	S5000 series	0.25
	S5300 series	1.25
	S5500 series	0.25
	S5600 series	0.25
	S5700 series	1.25
	S6300 series	1.25
	S6500 series	0.75
	S6700 series	1.25
	S7800 series	1.25
	S8016 series	1.25
	S8500 series	1.25
	S7703 series	2.0
	S7706 series	3.5
	S7712 series	6.0
	S9300X-4	6.0
	S9300X-8	6.0
	S9300X-12	9.0
	S9303/S9303E series	2.0
S9306/S9306E series	3.5	
S9312/S9312E series	6.0	
S9703	2.0	

NE Series	NE Type	Equivalent Coefficient
	S9706	3.5
	S9712	6.0
	S12700E-4, S12700E-8, S12704, S12708, S12710	6.0
	S12712, S12700E-12	9.0
	E628 series	1.25
	E652 series	1.25
Data center switch	CE16804	6.0
	CE16808	8.0
	CE16816	10.0
	CE12804	6.0
	CE12808	8.0
	CE12812	10.0
	CE9800 series	2.0
	CE8800 series	1.25
	CE7800 series	1.25
	CE6800 series	1.25
	CE5800 series	1.25
PTN6900 series	PTN6900-1/PTN6900-1-M4	0.5
	PTN6900-F1A	0.5
	PTN6900-M8C	0.5
	PTN6900-M2K/M2E/M2F	0.5
	PTN6900-2-M8A/M16A	1.0
	PTN6900-2/PTN6900-2-M8/ PTN6900-2-M14/PTN6900-2- M16	1.0
	PTN6900-3/3A	1.25
	PTN6900-8/8A	2.5
	PTN6900-16/16A	5.0
OptiX PTN series	OptiX PTN 1900	2.5
	OptiX PTN 3900	4.5

NE Series	NE Type	Equivalent Coefficient
	OptiX PTN 3900-8	4
	OptiX PTN 912	0.5
	OptiX PTN 910	0.5
	OptiX PTN 910-F	0.4
	OptiX PTN 910E-F	0.5
	OptiX PTN 916-F	0.5
	OptiX PTN 930	1
	OptiX PTN 950	1
	OptiX PTN 960	1.5
	OptiX PTN 905	0.4
	OptiX PTN 905A	0.4
	OptiX PTN 905B	0.4
	OptiX PTN 905C	0.4
	OptiX PTN 905E	0.4
	OptiX PTN 905G	0.4
	OptiX PTN 906A	0.4
	OptiX PTN 906AI	0.4
	OptiX PTN 906B	0.4
	Layer 2 Virtual NE	1
	Layer 3 Virtual NE	1
	Physical Layer Virtual NE	1
	OptiX PTN 990/990E	2.5
	OptiX PTN 980	2.0
	OptiX PTN 970	2.5
	OptiX PTN 970C	2.5
	OptiX PTN 6900	5
	OptiX PTN 7900-32	5.5
	OptiX PTN 7900-24	5
	OptiX PTN 7900-12	4.5
	OptiX PTN 7900E-32	5.5

NE Series	NE Type	Equivalent Coefficient
	OptiX PTN 7900E-24	5
	OptiX PTN 7900E-12	4.5
ATN series	ATN 910/910I/910B/910C/ 910D	0.5
	ATN 905	0.25
	ATN905(V8)	0.25
	ATN 950	1.0
	ATN 950B	1.0
	ATN 950C	1.0
	ATN 950D	1.0
	ATN 980	1.0
	ATN 980B	1.0
	ATN 990	1.0
ETN series	ETN 500	0.25
	ETN 550-A	1.0
MAN service platform	CX200 series	0.625
	CX300 series	1.25
	CX600-X1	0.5
	CX600-X2	1.0
	CX600-X3	1.25
	CX600-4	1.25
	CX600-X8	2.5
	CX600-8	2.5
	CX600-X16	5.0
	CX600-16	5.0
	CX600-M2E/CX600-M2F/ CX600-M2H/CX600-M2K	0.5
	CX600-F1A	0.5
	CX6620	10.0
	CX6601/CX6602	0.5
CX6608	5.0	

NE Series	NE Type	Equivalent Coefficient
EGW	EGW2100 series	0.25
	EGW2200 series	0.25
	EGW3200 series	0.25
Firewall	Eudemon 300/500/1000	0.5
	Eudemon 100E	0.25
	NGFW	0.75
	Eudemon 200E series	0.25
	Eudemon 200E-G8/-G85/-N	0.75
	Eudemon 200S	0.25
	Eudemon 1000E series	0.75
	Eudemon 1000E-X	0.75
	Eudemon 8040	3.0
	Eudemon 8080	6.0
	Eudemon 8080E	4.0
	Eudemon 8160E	8.0
	Eudemon 8000E-X3	1.5
	Eudemon 8000E-X8	4.0
	Eudemon 8000E-X16	8.0
	Eudemon 6080E	4.0
	NE40E-FW	4.0
	NE80E-FW	8.0
vRouter6000V series	0.75	
USG	USG9110	2.0
	USG9120	4.0
	USG9310	4.0
	USG9320	8.0
	USG9520	1.5
	USG9560	4.0
	USG9580	8.0
	USG6600 series	0.75

NE Series	NE Type	Equivalent Coefficient
	USG6500 series	0.75
	USG6300 series	0.75
	USG5500 series	0.75
	USG5300 series	0.75
	USG5100 series	0.25
	USG3000	0.25
	USG2100 series	0.25
	USG2200 series	0.25
	USG50	0.25
SRG	SRG1200 series	0.25
	SRG20 series	0.25
	SRG2200 series	0.25
	SRG3200 series	0.25
	SRG1300 series	0.25
	SRG2300 series	0.25
	SRG3300 series	0.25
SIG	SIG9810	4.0
	SIG9820	8.0
	SIG9800-X3	1.5
	SIG9800-X8	4.0
	SIG9800-X16	8.0
	SIG Server	4.0
	URL Classify Server	0.25
	RADIUS Proxy	0.25
SeMG9811	SeMG9811-X3	1.5
	SeMG9811-X8	4.0
	SeMG9811-X16	8.0
NE-DPI	NE40E-DPI	4.0
	NE80E-DPI	8.0
	NE40E80E-DPI Server	4.0



NE Series	NE Type	Equivalent Coefficient
	URL Classify Server-DPI	0.25
	RADIUS Proxy-DPI	0.25
SVN	SVN3000	0.25
	SVN2200	0.25
	SVN5300	0.75
	SVN5500	0.75
ASG	ASG2100	0.25
	ASG2200	0.25
	ASG2600	0.75
	ASG2800	0.75
NIP	NIP6600	0.75
CE-FWA	CE-FWA	0.75
CE-IPSA	CE-IPSA	0.75
OP-Bypass	OP-Bypass	0.25
iCache	iCache9200 RSS	1.0
	iCache9200 DSS	1.0
	iCache9200 MSS	1.0
	iCache9200 CSS-HTTP	1.0
	iCache9200 CSS-BT	1.0
	iCache9200 CSS-EM	1.0
	iCache9200 CSS-WEB	1.0
	iCache9200 CSS-PPS	1.0
	iCache9200 CSS-PPL	1.0
	iCache9200 CSS-QQL	1.0
Broadband access	MA5200E/F series	1.5
	MA5200G series	10.0
	ME60 series	10.0
	BGW9916	5.0
Voice gateway	VG1040/1041 series	0.25
VNE1000	VNE1000 series	1

NE Series	NE Type	Equivalent Coefficient
VNE9000	VNE9000 series	1
VSIG9800	VSIG9800 series	1
ICMP device	ICMP device	1
Third-party NE	SNMP Third-party NE	1
	Cisco ASR 9001	0.5
	Cisco ASR 9006	1.25
	Cisco ASR 9922	7
	Nokia 7750 SR-a4	0.5
	Nokia 7750 SR-7	1.5
	Nokia 7750 SR-12	3
	Nokia 7750 SR-12e	3
	Juniper MX480	2.5
	UBIQUOSS E7124	0.5
DASAN M3000	0.5	

### 9.4.3 Equivalent NEs in the Access Domain

Number of equivalent NEs in the access domain = Number of FTTx OLT equivalent NEs + Number of FTTx MDU equivalent NEs + Number of MSAN equivalent NEs + Number of DSLAM equivalent NEs + Number of other equivalent NEs

 **NOTE**

Access capacity is measured by lines. In [Table 9-15](#), each port is a line.

- Number of FTTx OLT equivalent NEs = Number of ONTs x Equivalent coefficient of ONTs + Number of P2P ports x Equivalent coefficient of P2P ports
- Number of FTTx MDU equivalent NEs = Number of ports of type 1 x Equivalent coefficient of type 1 + ... + Number of ports of type *n* x Equivalent coefficient of type *n*
- Number of MSAN equivalent NEs = Number of ports of type\_1 x Equivalent coefficient of type\_1 + ... + Number of ports of type *n* x Equivalent coefficient of type *n*
- Number of DSLAM equivalent NEs = Number of ports of type 1 x Equivalent coefficient of type 1 + ... + Number of ports of type\_ *n* x Equivalent coefficient of type\_ *n*
- Number of other equivalent NEs = Number of NEs of type 1 x Equivalent coefficient of type 1 + ... + Number of NEs of type *n* x Equivalent coefficient of type *n*

[Table 9-15](#) describes the equivalent coefficients for NEs in the access domain.

**Table 9-15** Equivalent coefficients for NEs in the access domain

NE Series	NE Type	Equivalent Coefficient
FTTx OLT (calculated based on the numbers of ONTs, and P2P ports)	ONT in the P2MP scenario	1/80
	P2P port	1/64
FTTx MDU (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	POTS/ISDN BRA/ISDN PRA port	1/160
	CNU port	1/128
	G.fast port	1/128
	Serial port	1/64
MSAN (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
	POTS/ISDN BRA/ISDN PRA port	1/160
DSLAM (calculated based on the number of user ports)	xDSL port	1/128
	E1 port	1/128
	ETH port	1/128
RPS (calculated based on the number of chassis)	RPS frame	1/3
EDFA (calculated based on the number of NEs)	EDFA	1/3
CCU (calculated based on the number of CCUs)	CCU	1
SMU11B (calculated based on the number of SMU11Bs)	SMU11B	1
Other NEs (calculated based on NE types)	BITS	1

## 9.5 Equivalent Routes

The route equivalent coefficient is calculated based on the size of the memory occupied by the route data structure and the ratio of the preferred route to the non-preferred route in the typical networking.

The formula for calculating the number of equivalent routes is as follows:

$$\text{Number of equivalent routes} = \sum_{\text{Item in \{ProtocolType\}}} \text{Number of preferred routes} \times \text{Equivalent coefficient}$$

Protocol type = {Direct, Static, OSPF, IS-IS, BGP, VPN, FIB}

For the equivalent coefficient of each protocol route, see [Equivalent coefficients of protocol routes](#).

For example, if there are 10,000 direct routes, 20,000 static routes, 100,000 OSPF routes, 30,000 IS-IS routes, 20,000 BGP routes, 150,000 VPN routes, and 50,000 FIB routes, then the number of equivalent routes is calculated as follows based on the equivalent coefficients of protocol routes listed in [Table 9-16](#):

$$\text{Number of equivalent routes} = 10,000 \times 1 + 20,000 \times 1 + 100,000 \times 1.5 + 30,000 \times 1.5 + 20,000 \times 1.6 + 150,000 \times 1.6 + 50,000 \times 1 = 547,000$$

**Table 9-16** Equivalent coefficients of protocol routes

Protocol Type	Equivalent Coefficient
Direct	1
Static	1
OSPF	1.5
IS-IS	1.5
BGP	1.6
VPN	1.6
FIB	1

On a network, there are different node roles such as PEs, CEs, and UPEs. Calculate the total number of equivalent routes on the network as follows:

1. Query the total number of protocol routes on a node of each role.
2. Calculate the number of equivalent routes of the node based on the formula.
3. Multiply the number of equivalent routes by the number of nodes of a role to obtain the total number of equivalent routes of the role.
4. Sum up the numbers of equivalent routes of nodes of all roles.

Finally, compare the estimated number of equivalent routes with the maximum number of equivalent routes (10 million) supported.

If there are 500 PEs, 1000 CEs, and 2000 UPEs on a network and the numbers of equivalent routes of a PE, CE, and UPE are A, B, and C respectively, the total number of equivalent routes on the network is estimated based on the formula as follows:  $500 \times A + 1000 \times B + 2000 \times C$ .

# 10 Version Requirements

---

## NOTE

- The **New Version** column lists the NE versions newly supported by the current NCE version.
- The **Compatible Version** column lists the NE versions supported by earlier NCE versions. Unless otherwise specified, the current NCE version also supports these NE versions.

[10.1 MSTP Series](#)

[10.2 WDM Series](#)

[10.3 RTN Series](#)

[10.4 PTN Series](#)

[10.5 NE/ATN/CX/Multi-service gateways Series](#)

[10.6 R/AR Series](#)

[10.7 RM9000 Series](#)

[10.8 Switch Series](#)

[10.9 Security Series](#)

[10.10 iCache Series](#)

[10.11 FTTx Series](#)

[10.12 MSAN Series](#)

[10.13 DSLAM Series](#)

[10.14 BITS/iSite/EDFA Series](#)

## 10.1 MSTP Series

The following table lists the MSTP series NE supported.

**Table 10-1** MSTP series

NE	New Version	Compatible Version
OptiX Metro 100	N/A	5.42.05.10 (V100R005C00), 5.42.03.20, 5.42.03.10, 5.42.02.10, 5.42.01.30, 5.42.01.20, 5.42.01.10
OptiX Metro 1000V3	N/A	5.37.07.30 (V300R007C02), 5.37.07.20 (V300R007C01), 5.37.07.10 (V300R007C00), 5.37.06.10 (V300R006), 5.37.05.10 (V300R005), 5.37.04.10 (V300R004), 5.37.03.10 (V300R003), 5.37.02.30, 5.37.02.20, 5.37.02.10, 5.37.01.10
OptiX Metro 500	N/A	5.24.05.10, 5.24.04.30, 5.24.04.20, 5.24.04.10, 5.24.03.10, 5.24.02.20, 5.17.01.20, 5.17.01.10

**Table 10-2** OSN series

NE	New Version	Compatible Version
OptiX OSN 1500	N/A	5.36.34.80 (V200R015C30), 5.36.34.60 (V200R015C20), 5.36.34.30 (V200R015C10), 5.36.34.10 (V200R015C00), 5.36.33.70 (V200R013C30), 5.36.33.50 (V200R013C20), 5.36.33.30 (V200R013C10), 5.36.33.10 (V200R013C00), 5.36.32.50 (V200R012C01), 5.36.32.10 (V200R012C00), 5.36.31.70 (V200R011C03), 5.36.31.60 (V200R011C02), 5.36.31.50 (V200R011C01), 5.36.31.30 (V200R011C00), 5.36.30.10 (V100R009C03), 5.36.20.50 (V100R010C03), 5.36.20.40 (V100R010C02), 5.36.20.10 (V100R010C00), 5.36.19.40 (V100R009C02), 5.36.19.10 (V100R009C01), 5.36.18.40 (V100R008C02),



NE	New Version	Compatible Version
		5.36.18.10 (V100R008C01), 5.36.17.10, 5.36.16.10, 5.36.15.10-5.36.15.99, 5.36.14.30-5.36.14.49, 5.36.14.10, 5.36.13.40, 5.36.12.40, 5.36.12.10, 5.36.11.10
OptiX OSN 2000	N/A	5.50.03.10 (V100R003), 5.50.02.20 (V100R002), 5.50.02.10, 5.50.01.10
OptiX OSN 2500	N/A	5.36.20.50 (V100R010C03), 5.36.20.40 (V100R010C02), 5.36.20.10 (V100R010C00), 5.36.19.40 (V100R009C02), 5.36.19.10 (V100R009C01), 5.36.18.40 (V100R008C02), 5.36.18.10 (V100R008C01), 5.36.17.10, 5.36.16.10, 5.36.15.10-5.36.15.99, 5.36.14.30-5.36.14.49, 5.36.14.10, 5.36.13.40, 5.36.12.40, 5.36.12.10, 5.27.12.10, 5.27.01.10

NE	New Version	Compatible Version
OptiX OSN 2500REG	N/A	5.43.13.10, 5.36.18.40, 5.36.13.40

NE	New Version	Compatible Version
OptiX OSN 3500	N/A	5.21.34.80 (V200R015C30), 5.21.34.60 (V200R015C20), 5.21.34.30 (V200R015C10), 5.21.34.10 (V200R015C00), 5.21.33.70 (V200R013C30), 5.21.33.50 (V200R013C20), 5.21.33.30 (V200R013C10), 5.21.33.10 (V200R013C00), 5.21.32.50 (V200R012C01), 5.21.32.10 (V200R012C00), 5.21.31.70 (V200R011C03), 5.21.31.60 (V200R011C02), 5.21.31.50 (V200R011C01), 5.21.31.30 (V200R011C00), 5.21.31.10 (V100R009C05), 5.21.30.10 (V100R009C03), 5.21.20.50 (V100R010C03), 5.21.20.40 (V100R010C02), 5.21.20.10 (V100R010C00), 5.21.19.40 (V100R009C02), 5.21.19.10 (V100R009C01), 5.21.18.44,

NE	New Version	Compatible Version
		5.21.18.40 (V100R008C02), 5.21.18.10 (V100R008C01), 5.21.17.10, 5.21.16.10, 5.21.15.10-5.21.15.99, 5.21.14.30-5.21.14.59, 5.21.14.10, 5.21.13.40, 5.21.12.40, 5.21.12.10, 5.21.01.10
OptiX OSN 3580	N/A	5.21.34.80 (V200R015C30), 5.21.34.60 (V200R015C20), 5.21.34.30 (V200R015C10), 5.21.34.10 (V200R015C00), 5.21.33.70 (V200R013C30), 5.21.33.50 (V200R013C20), 5.21.33.30 (V200R013C10), 5.21.33.10 (V200R013C00)
OptiX OSN 50	N/A	5.119.05.10 (V100R005C00)

NE	New Version	Compatible Version
OptiX OSN 500	N/A	5.62.08.60 (V100R008C50), 5.62.08.40 (V100R008C30), 5.62.08.30 (V100R008C20), 5.62.08.20 (V100R008C10), 5.62.08.10 (V100R008C00), 5.62.07.40 (V100R007C30), 5.62.07.30 (V100R007C20), 5.62.07.20 (V100R007C10), 5.62.07.10 (V100R007C00), 5.62.06.20 (V100R006C01), 5.62.06.10 (V100R006C00), 5.62.05.30 (V100R005C02), 5.62.05.10 (V100R005C00), 5.62.03.10 (V100R003C00), 5.62.02.10 (V100R002), 5.62.01.10 (V100R001)

NE	New Version	Compatible Version
OptiX OSN 550	N/A	5.81.08.60 (V100R008C50), 5.81.08.40 (V100R008C30), 5.81.08.30 (V100R008C20), 5.81.08.20 (V100R008C10), 5.81.08.10 (V100R008C00), 5.81.07.40 (V100R007C30), 5.81.07.30 (V100R007C20), 5.81.07.20 (V100R007C10), 5.81.07.10 (V100R007C00), 5.81.06.20 (V100R006C01), 5.81.06.10 (V100R006C00), 5.81.05.30 (V100R005C02), 5.81.05.20 (V100R005C01), 5.81.05.10 (V100R005C00), 5.81.03.10 (V100R003C00)

NE	New Version	Compatible Version
OptiX OSN 580	N/A	5.125.08.60 (V100R008C50), 5.125.08.40 (V100R008C30), 5.125.08.30 (V100R008C20), 5.125.08.20 (V100R008C10), 5.125.08.10 (V100R008C00), 5.125.07.40 (V100R007C30), 5.125.07.30 (V100R007C20), 5.125.07.20 (V100R007C10)

NE	New Version	Compatible Version
OptiX OSN 7500	N/A	5.21.34.80 (V200R015C30), 5.21.34.60 (V200R015C20), 5.21.34.30 (V200R015C10), 5.21.34.10 (V200R015C00), 5.21.33.70 (V200R013C30), 5.21.33.50 (V200R013C20), 5.21.33.30 (V200R013C10), 5.21.33.10 (V200R013C00), 5.21.32.50 (V200R012C01), 5.21.32.10 (V200R012C00), 5.21.31.70 (V200R011C03), 5.21.31.60 (V200R011C02), 5.21.31.50 (V200R011C01), 5.21.31.30 (V200R011C00), 5.21.31.10 (V100R009C05), 5.21.20.50 (V100R010C03), 5.21.20.40 (V100R010C02), 5.21.20.10 (V100R010C00), 5.21.19.40 (V100R009C02), 5.21.19.10 (V100R009C01), 5.21.18.40 (V100R008C02), 5.21.18.10 (V100R008C01),



NE	New Version	Compatible Version
		5.21.17.10, 5.21.16.10, 5.21.15.10-5.21.15.99, 5.21.14.30-5.21.14.49, 5.21.14.10, 5.21.13.40
OptiX OSN 7500 II	N/A	5.21.34.80 (V200R015C30), 5.21.34.60 (V200R015C20), 5.21.34.30 (V200R015C10), 5.21.34.10 (V200R015C00), 5.21.33.70 (V200R013C30), 5.21.33.50 (V200R013C20), 5.21.33.30 (V200R013C10), 5.21.33.10 (V200R013C00), 5.21.32.50 (V200R012C01), 5.21.32.10 (V200R012C00), 5.21.31.70 (V200R011C03), 5.21.31.60 (V200R011C02), 5.21.31.50 (V200R011C01)
OptiX OSN 80	N/A	5.120.03.10 (V100R003C00)

NE	New Version	Compatible Version
OptiX OSN 9500	N/A	5.15.06.50 (V100R006C05SPC200), 5.15.06.30 (V100R006C03), 5.15.06.10 (V100R006C00), 5.15.05.10, 5.15.04.10, 5.15.03.30, 5.15.03.26, 5.15.03.20, 5.15.02.20, 5.15.02.11, 5.15.02.10, 5.15.01.30, 5.15.01.20, 5.15.01.10
OptiX OSN 9560	N/A	5.51.08.10 (V100R007C00), 5.51.07.30-5.51.07.59 (V100R006C01), 5.51.07.10 (V100R006C00), 5.51.06.10 (V100R005C00), 5.51.05.20 (V100R002C00)

**Table 10-3** SDH series

NE	New Version	Compatible Version
OptiX 10G MADM(Metro5000)	N/A	5.10.06.40, 5.10.06.30, 5.10.06.10, 5.10.05.20, 5.10.05.10, 5.10.04.40, 5.10.04.35, 5.10.04.30, 5.10.04.10, 5.10.03.10, 5.10.02.10, 5.10.01.20, 5.10.01.10, 5.10.01.01
OptiX 155/622 (Metro 2050)	N/A	4.01.18.10, 4.01.17.04, 4.01.17.03, 4.01.17.02, 4.01.17.01, 4.01.16.22, 4.01.16.21, 4.01.16.20

NE	New Version	Compatible Version
OptiX 155/622H	N/A	4.02.06.60, 4.02.06.53, 4.02.06.50, 4.02.06.41, 4.02.06.40, 4.02.06.31, 4.02.06.30, 4.02.06.20, 4.02.06.10, 4.02.06.07, 4.02.06.06, 4.02.06.04, 4.02.06.03, 4.02.05.06, 4.02.05.05, 4.02.05.04
OptiX 155/622H(Metro 1000)	N/A	4.02.06.60, 4.02.06.53, 4.02.06.50, 4.02.06.41, 4.02.06.40, 4.02.06.31, 4.02.06.30, 4.02.06.20, 4.02.06.10, 4.02.06.07, 4.02.06.06, 4.02.06.04, 4.02.06.03, 4.02.05.06, 4.02.05.05, 4.02.05.04
OptiX 2500	N/A	4.01.18.10, 4.01.17.04

NE	New Version	Compatible Version
OptiX 2500+	N/A	4.05.10.10, 4.05.09.10, 4.05.08.10, 4.05.07.10, 4.05.06.41, 4.05.06.40, 4.05.06.30, 4.05.06.15, 4.05.06.10, 4.05.05.10, 4.05.04.16, 4.05.04.15, 4.05.03.40, 4.05.03.36, 4.05.03.33, 4.05.03.20, 4.05.03.10, 4.05.03.02
OptiX 2500+(Metro 3000)	N/A	4.05.10.10, 4.05.09.10, 4.05.08.10, 4.05.07.10, 4.05.06.41, 4.05.06.40, 4.05.06.30, 4.05.06.15, 4.05.06.10, 4.05.05.10, 4.05.04.16, 4.05.04.15, 4.05.03.40, 4.05.03.36, 4.05.03.33, 4.05.03.20, 4.05.03.10, 4.05.03.02

 **NOTE**

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product. Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the NCE, a.bb.cc.2x is supported by version A of the NCE.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the NCE, a.bb.cc.xx is supported by version A of the NCE.

## 10.2 WDM Series

The following table lists the WDM series NE supported.

**Table 10-4** NG WDM series

NE	New Version	Compatible Version
HUAWEI OSN902	N/A	5.169.19.18 (V100R019C00), 5.169.1.30 (V100R001C10), 5.169.1.10 (V100R001C00), 5.169.02.16 (V100R003C00), 5.169.02.12 (V100R002C10), 5.169.02.10 (V100R002C00)
OptiX OSN 1800 I E	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10)

NE	New Version	Compatible Version
OptiX OSN 1800 I/II	5.141.19.95 (F3SCC V100R019C11SPC300)	5.67.19.83 (V100R019C10), 5.67.03.88~5.67.03.89 (F1SCC), 5.67.03.86~5.67.03.87 (F1SCC), 5.67.03.50 (V100R003C05), 5.67.03.40 (V100R003C03), 5.67.03.30 (V100R003C02), 5.67.03.20~5.67.03.90 (V100R005C00), 5.67.03.20~5.67.03.90 (F1SCC) (V100R006C00), 5.67.03.20~5.67.03.90 (F1SCC) (V100R005C20), 5.67.03.20 (V100R003C01), 5.67.03.10 (V100R003C00 ), 5.67.02.10 (V100R002C00 ), 5.67.01.20, 5.67.01.10 (V100R001), 5.153.19.13 (V100R009C00), 5.153.09.11 (V100R009C00 F1SCC), 5.153.08.12 (V100R008C10 F1SCC), 5.153.08.11 (V100R008C00 F1SCC), 5.153.07.31 (F1SCC) (V100R007C10), 5.153.07.11 (F1SCC) (V100R007C00), 5.141.19.83 (V100R019C10), 5.141.19.13 (V100R009C00),

NE	New Version	Compatible Version
		5.141.09.11 (V100R009C00 F3SCC), 5.141.08.30 (V100R008C10 F3SCC), 5.141.08.11 (V100R008C00 F3SCC), 5.141.07.31 (F3SCC) (V100R007C10), 5.141.07.11 (F3SCC) (V100R007C00), 5.141.06.31 (F3SCC) (V100R006C20), 5.141.06.21 (F3SCC) (V100R006C10), 5.141.06.11 (F3SCC) (V100R006C00), 5.141.05.11 (F3SCC) (V100R005C20)
OptiX OSN 1800 II E	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.30 (V100R007C10)
OptiX OSN 1800 II TP	5.67.19.95 (B1SCC V100R019C11SPC300)	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00)



NE	New Version	Compatible Version
OptiX OSN 1800 II(Packet)	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.31 (V100R007C10), 5.67.07.11 (V100R007C00), 5.67.06.31 (V100R006C20), 5.67.06.21 (V100R006C10), 5.67.06.11 (V100R006C00), 5.67.05.30 (V100R005C20), 5.67.05.20 (V100R005C10), 5.67.05.11 (V100R005C00), 5.67.03.91 (V100R003C05)

NE	New Version	Compatible Version
OptiX OSN 1800 V	5.67.19.95 (F5XCH Z8SCC V100R019C11SPC300)	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.31 (V100R007C10), 5.67.07.11 (V100R007C00), 5.67.06.31 (V100R006C20), 5.67.06.21 (V100R006C10), 5.67.06.11 (V100R006C00), 5.67.05.30 (V100R005C20), 5.67.05.20 (V100R005C10), 5.67.05.11 (V100R005C00), 5.67.03.60 (V100R003C05)

NE	New Version	Compatible Version
OptiX OSN 1832	N/A	5.51.19.83 (V100R019C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00)

NE	New Version	Compatible Version
OptiX OSN 1832 X16	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.31 (V100R007C10), 5.67.07.11 (V100R007C00), 5.67.06.31 (V100R006C20), 5.67.06.21 (V100R006C10), 5.67.06.11 (V100R006C00), 5.67.05.30 (V100R005C20), 5.67.05.20 (V100R005C10), 5.67.05.11 (V100R005C00), 5.67.03.60 (V100R003C05)
OptiX OSN 1832 X4 E	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10)

NE	New Version	Compatible Version
OptiX OSN 1832 X8	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.31 (V100R007C10), 5.67.07.11 (V100R007C00), 5.67.06.31 (V100R006C20), 5.67.06.21 (V100R006C10), 5.67.06.11 (V100R006C00), 5.67.05.30 (V100R005C20), 5.67.05.20 (V100R005C10), 5.67.05.11 (V100R005C00), 5.67.03.91 (V100R003C05)
OptiX OSN 1832 X8 E	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00), 5.67.09.11 (V100R009C00), 5.67.08.30 (V100R008C10), 5.67.08.11 (V100R008C00), 5.67.07.30 (V100R007C10)

NE	New Version	Compatible Version
OptiX OSN 3800	N/A	5.52.05.20 (V100R004C04), 5.52.04.30 (V100R004C03), 5.52.04.20 (V100R004C02), 5.52.04.10, 5.52.03.20, 5.52.02.10, 5.52.01.10, 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00), 5.51.07.60 (V100R006C03), 5.51.07.30 (V100R006C01),

NE	New Version	Compatible Version
		5.51.07.10 (V100R006C00), 5.51.06.10 (V100R005C00)

NE	New Version	Compatible Version
OptiX OSN 6800	N/A	5.51.15.82 (V100R013C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00), 5.51.07.60 (V100R006C03), 5.51.07.30 (V100R006C01), 5.51.07.10 (V100R006C00), 5.51.06.10 (V100R005C00), 5.51.05.20 (V100R004C04), 5.51.04.30 (V100R004C03), 5.51.04.20 (V100R004C02),



NE	New Version	Compatible Version
		5.51.04.10, 5.51.03.20, 5.51.02.10, 5.51.01.10
OptiX OSN 880	N/A	5.67.19.83 (V100R019C10), 5.67.19.13 (V100R009C00)
OptiX OSN 8800	N/A	5.51.15.82 (V100R013C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00)

NE	New Version	Compatible Version
OptiX OSN 8800 T16	N/A	5.51.15.82 (V100R013C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00), 5.51.07.60 (V100R006C03), 5.51.07.30 (V100R006C01), 5.51.07.10 (V100R006C00)

NE	New Version	Compatible Version
OptiX OSN 8800 T32	N/A	5.51.15.82 (V100R013C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00), 5.51.07.60 (V100R006C03), 5.51.07.30 (V100R006C01), 5.51.07.10 (V100R006C00), 5.51.06.10 (V100R005C00), 5.51.05.21 (V100R002C02), 5.51.05.20 (V100R002C00), 5.51.04.30 (V100R001C02),

NE	New Version	Compatible Version
		5.51.04.20 (V100R001C01)
OptiX OSN 8800 T64	N/A	5.51.15.82 (V100R013C10), 5.51.15.32 (V100R013C10), 5.51.15.10 (V100R013C00), 5.51.13.30 (V100R012C10), 5.51.13.10 (V100R012C00), 5.51.12.30 (V100R011C10), 5.51.12.10 (V100R011C00), 5.51.11.30 (V100R010C10), 5.51.11.10 (V100R010C00), 5.51.10.30 (V100R009C10), 5.51.10.10 (V100R009C00), 5.51.09.30 (V100R008C10), 5.51.09.10 (V100R008C00), 5.51.08.30 (V100R007C02), 5.51.08.10 (V100R007C00), 5.51.07.60 (V100R006C03), 5.51.07.30 (V100R006C01), 5.51.07.10 (V100R006C00), 5.51.06.10 (V100R005C00), 5.51.05.21 (V100R002C02)

NE	New Version	Compatible Version
OptiX OSN 9600	N/A	5.51.19.60 (V100R019C10 52SCC), 5.51.15.82 (V100R007C00 52SCC), 5.51.15.10 (V100R006C10), 5.51.13.30 (V100R006C00), 5.51.13.10 (V100R005C10), 5.51.12.17 (V100R005C00), 5.51.12.11 (V100R003C10), 5.51.11.31 (V100R003C00), 5.51.11.13 (V100R002C10), 5.51.10.13 (V100R001C30), 5.51.09.33 (V100R001C20), 5.51.09.17 (V100R001C01), 5.51.08.15 (V100R001C00), 5.174.19.60 (V100R019C10 51SCU), 5.174.06.82 (V100R007C00 51SCU), 5.174.06.60 (V100R007C00)
OptiX OSN 9600 M05	N/A	5.172.19.60 (V100R019C10)
OptiX OSN 9600 M12	N/A	5.172.19.60 (V100R019C10), 5.172.06.82 (V100R007C00)

NE	New Version	Compatible Version
OptiX OSN 9600 M24	N/A	5.172.06.60 (V100R007C00 UTS), 5.172.06.30 (V100R006C10), 5.172.06.10 (V100R006C00), 5.172.19.60 (V100R019C10)
OptiX OSN 9600 P32	N/A	5.200.06.68 (V100R007C00), 5.200.06.30 (V100R006C10), 5.200.19.60 (V100R019C10)
OptiX OSN 9600 U16	N/A	5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30)

NE	New Version	Compatible Version
OptiX OSN 9600 U32	N/A	5.171.19.60 (V100R019C10 UTS), 5.171.06.60 (V100R007C00 UTS), 5.171.06.30 (V100R006C10 UTS), 5.171.06.10 (V100R006C00 UTS), 5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30), 5.111.01.60 (V100R001C20), 5.111.01.30 (V100R001C01), 5.111.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX OSN 9600 U64	N/A	5.171.19.60 (V100R019C10 UTS), 5.171.06.60 (V100R007C00 UTS), 5.171.06.30 (V100R006C10 UTS), 5.171.06.10 (V100R006C00 UTS), 5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30), 5.111.01.60 (V100R001C20), 5.111.01.30 (V100R001C01), 5.111.01.10 (V100R001C00)



NE	New Version	Compatible Version
OptiX OSN 9800	5.174.19.75 (V100R019C11SPC300)	5.51.19.60 (V100R019C10 52SCC), 5.51.15.82 (V100R007C00 52SCC), 5.51.15.10 (V100R006C10), 5.51.13.30 (V100R006C00), 5.51.13.10 (V100R005C10), 5.51.12.17 (V100R005C00), 5.51.12.11 (V100R003C10), 5.51.11.31 (V100R003C00), 5.51.11.13 (V100R002C10), 5.51.10.13 (V100R001C30), 5.51.09.33 (V100R001C20), 5.51.09.17 (V100R001C01), 5.51.08.15 (V100R001C00), 5.51.06.60 (V100R007C00 52SCC), 5.174.06.82 (V100R007C00 51SCU), 5.174.06.60 (V100R007C00 51SCU), 5.174.19.60 (V100R019C10 51SCU)
OptiX OSN 9800 M05	N/A	5.172.19.60 (V100R019C10)
OptiX OSN 9800 M12	5.172.19.75 (V100R019C11SPC300)	5.172.19.60 (V100R019C10), 5.172.06.82 (V100R007C00)

NE	New Version	Compatible Version
OptiX OSN 9800 M24	5.172.19.75 (V100R019C11SPC300)	5.172.19.60 (V100R019C10), 5.172.06.60 (V100R007C00 UTS), 5.172.06.30 (V100R006C10), 5.172.06.10 (V100R006C00)
OptiX OSN 9800 P32	N/A	5.200.19.60 (V100R019C10), 5.200.06.60 (V100R007C00), 5.200.06.30 (V100R006C10)
OptiX OSN 9800 U16	N/A	5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30)

NE	New Version	Compatible Version
OptiX OSN 9800 U32	5.171.19.75 (V100R019C11SPC300)	5.171.19.60 (V100R019C10 UTS), 5.171.06.60 (V100R007C00 UTS), 5.171.06.30 (V100R006C10 UTS), 5.171.06.10 (V100R006C00 UTS), 5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30), 5.111.01.60 (V100R001C20), 5.111.01.30 (V100R001C01), 5.111.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX OSN 9800 U64	5.171.19.75 (V100R019C11SPC300)	5.171.19.60 (V100R019C10 UTS), 5.171.06.60 (V100R007C00 UTS), 5.171.06.30 (V100R006C10 UTS), 5.171.06.10 (V100R006C00 UTS), 5.111.19.60 (V100R019C10 VRP), 5.111.06.60 (V100R007C00 VRP), 5.111.06.30 (V100R006C10 VRP), 5.111.06.10 (V100R006C00 VRP), 5.111.05.30 (V100R005C10), 5.111.05.10 (V100R005C00), 5.111.03.50 (V100R003C10), 5.111.03.30 (V100R003C10), 5.111.03.10 (V100R003C00), 5.111.02.30 (V100R002C10), 5.111.01.80 (V100R001C30), 5.111.01.60 (V100R001C20), 5.111.01.30 (V100R001C01), 5.111.01.10 (V100R001C00)
OptiXtrans E6608	N/A	5.67.19.85 (V100R019C10)
OptiXtrans E6616	N/A	5.67.19.85 (V100R019C10)
OptiXtrans E9605	N/A	5.172.19.66 (V100R019C10)

**Table 10-5** LH WDM and Metro WDM series

NE	New Version	Compatible Version
AC-T	N/A	V100R001C00
OptiX BWS 1600G	N/A	5.08.07.30 (V100R007C03), 5.08.07.20 (V100R007C02), 5.08.07.10 (V100R007C01), 5.08.06.40, 5.08.06.20, 5.08.06.10 (V100R006), 5.08.05.10 (V100R005), 5.08.04.10, 5.08.03.70-5.08.03.99 (V100R003GA), 5.08.03.70-5.08.03.99 (V100R003GA'), 5.08.03.11, 5.08.03.10, 5.08.02.23, 5.08.02.22, 5.08.02.21, 5.08.02.20, 5.08.01.30, 5.08.01.20
OptiX BWS 1600G OLA	N/A	5.08.07.30 (V100R007C03), 5.08.07.20 (V100R007C02), 5.08.07.10 (V100R007C01), 5.08.06.40, 5.08.06.10, 5.08.05.10, 5.08.04.10
OptiX BWS 320G (OAS/OCI/OIS)	N/A	4.08.04.20, 4.08.04.10, 4.08.04.05, 4.08.04.04

NE	New Version	Compatible Version
OptiX BWS 320GV3	N/A	5.08.03.10, 5.08.02.20, 5.08.02.10, 5.08.01.30
OptiX Metro 6020	N/A	5.04.01.03
OptiX Metro 6040	N/A	5.18.01.20, 5.18.01.10
OptiX Metro 6040V2	N/A	5.39.04.10 (V100R008C01), 5.39.03.61, 5.39.03.33 (V100R007C03), 5.39.03.20 (V100R007C02), 5.39.03.10 (V100R007C01), 5.39.02.20 (V100R006C02), 5.39.02.10 (V100R006), 5.39.01.42, 5.39.01.40, 5.39.01.30, 5.26.01.30, 5.26.01.20, 5.26.01.10
OptiX Metro 6100	N/A	4.09.02.05, 4.09.02.03
OptiX Metro 6100V1	N/A	5.08.03.10, 5.08.02.22, 5.08.02.21, 5.08.02.20, 5.08.02.10, 5.08.01.40

NE	New Version	Compatible Version
OptiX Metro 6100V1E	N/A	5.39.05.10 (V100R008C04), 5.39.04.10 (V100R008C01), 5.39.03.61, 5.39.03.33 (V100R007C03), 5.39.03.20 (V100R007C02), 5.39.03.10 (V100R007C01), 5.39.02.20 (V100R006C02), 5.39.02.10 (V100R006), 5.39.01.42, 5.39.01.40, 5.39.01.20, 5.39.01.10
OptiX OSN 900A	N/A	5.53.01.10
OptiX OTU40000	N/A	V2.0

 **NOTE**

- Except for North America and Marine cable devices, NCE can manage all types of WDM devices supported by U2000.
- Different from OptiX OSN 8800 T32 and other devices, OptiX OSN 8800 is a platform-based device.
- Different from OptiX OSN 9600 U32 and other devices, OptiX OSN 9600 is a platform-based device.
- Different from OptiX OSN 9800 U32 and other devices, OptiX OSN 9800 is a platform-based device.
- The OptiX BWS 1600G OLA is an independent power supply subrack. It is supported by the OptiX BWS 1600G backbone DWDM optical transmission system V100R004 and later versions.
- Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product. Mapping principle:
  1. If the mapping table provides only the information that a.bb.cc.20 is supported by a version of the NCE, a.bb.cc.2x is supported by the version of the NCE.
  2. If the mapping table provides only the information that a.bb.cc is supported by a version of the NCE, a.bb.cc.xx is supported by the version of the NCE.

## 10.3 RTN Series

The following table lists the RTN series NE supported.

**Table 10-6** RTN series

NE	New Version	Compatible Version
OptiX RTN 310	N/A	5.92.19.27 (V100R019C10), 5.92.19.10 (V100R019C00), 5.92.09.20 (V100R009C10), 5.92.09.10 (V100R009C00), 5.92.08.20 (V100R008C10), 5.92.08.10 (V100R008C00), 5.92.07.20 (V100R007C10), 5.92.07.10 (V100R007C00), 5.92.06.10 (V100R006C00), 5.92.05.10 (V100R005C00), 5.92.03.10 (V100R003C00), 5.92.01.20 (V100R001C01), 5.92.01.10 (V100R001C00)



NE	New Version	Compatible Version
OptiX RTN 320	N/A	5.204.19.27(DMD4D) (V100R019C10), 5.204.19.10(DMD4D) (V100R019C00), 5.204.09.20(DMD4D) (V100R009C10), 5.151.19.27 (V100R019C10), 5.151.19.10 (V100R019C00), 5.151.09.20 (V100R009C10), 5.151.09.10 (V100R009C00), 5.151.08.20 (V100R008C10), 5.151.08.10 (V100R008C00), 5.151.07.20 (V100R007C10), 5.151.07.10 (V100R007C00), 5.151.06.10 (V100R006C00), 5.151.05.10 (V100R005C00)

NE	New Version	Compatible Version
OptiX RTN 360	N/A	5.138.19.27 (V100R019C10), 5.138.19.10 (V100R019C00), 5.138.09.20 (V100R009C10), 5.138.09.10 (V100R009C00), 5.138.08.20 (V100R008C10), 5.138.08.10 (V100R008C00), 5.138.07.20 (V100R007C10), 5.138.07.10 (V100R007C00), 5.138.06.10 (V100R006C00), 5.138.05.10 (V100R005C00), 5.138.03.10 (V100R003C00), 5.138.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX RTN 380	N/A	5.115.19.27 (V100R019C10), 5.115.19.10 (V100R019C00), 5.115.09.20 (V100R009C10), 5.115.09.10 (V100R009C00), 5.115.08.20 (V100R008C10), 5.115.08.10 (V100R008C00), 5.115.07.20 (V100R007C10), 5.115.07.10 (V100R007C00), 5.115.06.10 (V100R006C00), 5.115.05.10 (V100R005C00), 5.115.03.10 (V100R003C00), 5.115.02.10 (V100R002C00), 5.115.01.20 (V100R001C10), 5.115.01.10 (V100R001C00)
OptiX RTN 380A	N/A	5.203.19.27 (V100R019C10), 5.203.19.10 (V100R019C00), 5.203.09.20 (V100R009C10), 5.203.09.10 (V100R009C00)

NE	New Version	Compatible Version
OptiX RTN 380AX	N/A	5.212.19.27(MXXI4B) (V100R019C10), 5.212.19.10(MXXI4B) (V100R019C00), 5.206.19.27 (V100R019C10), 5.206.19.10 (V100R019C00), 5.206.09.20 (V100R009C10)
OptiX RTN 380H	N/A	5.190.19.27(MXXI5) (V100R019C10), 5.190.19.10(MXXI5) (V100R019C00), 5.190.09.20(MXXI5) (V100R009C10), 5.190.09.10(MXXI5) (V100R009C00), 5.190.08.20(MXXI5) (V100R008C10), 5.190.08.10(MXXI5) (V100R008C00), 5.160.19.27 (V100R019C10), 5.160.19.10 (V100R019C00), 5.160.09.20 (V100R009C10), 5.160.09.10 (V100R009C00), 5.160.08.20 (V100R008C10), 5.160.08.10 (V100R008C00), 5.160.07.20 (V100R007C10), 5.160.07.10 (V100R007C00), 5.160.06.10 (V100R006C00)

NE	New Version	Compatible Version
OptiX RTN 380e	N/A	5.180.19.10 (V100R019C00), 5.180.09.20 (V100R009C10), 5.180.09.10 (V100R009C00), 5.180.08.20 (V100R008C10), 5.180.08.10 (V100R008C00), 5.180.07.20 (V100R007C10)
OptiX RTN 510	N/A	5.194.19.27 (V100R019C10), 5.194.19.10 (V100R019C00), 5.194.02.20 (V100R002C10), 5.194.02.10 (V100R002C00), 5.194.01.20 (V100R001C10)
OptiX RTN 605	N/A	5.60.05.10 (V100R005), 5.60.03.30 (V100R003C02), 5.60.03.10 (V100R003), 5.60.01.10 (V100R001)
OptiX RTN 610	N/A	5.54.03.10 (V100R003), 5.54.02.10 (V100R002C00), 5.54.01.20 (V100R001C01), 5.54.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX RTN 620	N/A	5.54.05.30 (V100R005C02), 5.54.05.20 (V100R005C01), 5.54.05.10 (V100R005C00), 5.54.03.10 (V100R003), 5.54.02.10 (V100R002C00), 5.54.01.20 (V100R001C01), 5.54.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX RTN 905	N/A	5.95.19.27 (V100R019C10), 5.95.19.10 (V100R019C00), 5.95.11.20 (V100R011C10), 5.95.11.10 (V100R011C00), 5.95.10.20 (V100R010C10), 5.95.10.10 (V100R010C00), 5.95.09.20 (V100R009C10), 5.95.09.10 (V100R009C00), 5.95.08.20 (V100R008C10), 5.95.08.10 (V100R008C00), 5.95.07.20 (V100R007C10), 5.95.07.10 (V100R007C00), 5.95.06.20 (V100R006C10), 5.95.06.10 (V100R006C00), 5.95.05.20 (V100R005C01), 5.95.05.10 (V100R005C00)

NE	New Version	Compatible Version
OptiX RTN 905e	N/A	5.183.19.10 (V100R019C00), 5.183.11.20 (V100R011C10), 5.183.11.10 (V100R011C00), 5.183.10.20 (V100R010C10), 5.183.10.10 (V100R010C00), 5.183.09.20 (V100R009C10)
OptiX RTN 910	N/A	5.76.06.10 (V100R006C00), 5.76.05.20 (V100R005C01), 5.76.05.10 (V100R005C00), 5.76.03.40 (V100R003C03), 5.76.03.30 (V100R003C02), 5.76.03.20 (V100R003C01), 5.76.03.10 (V100R003C00), 5.76.02.30 (V100R002C02), 5.76.02.20 (V100R002C01), 5.76.02.10 (V100R002C00), 5.76.01.40 (V100R001C03), 5.76.01.30 (V100R001C02), 5.76.01.20 (V100R001C01), 5.76.01.10 (V100R001C00)



NE	New Version	Compatible Version
OptiX RTN 910A	N/A	5.207.19.27(CSHRF) (V100R019C10), 5.207.19.10 (CSHRF) (V100R019C00), 5.152.19.27 (V100R019C10), 5.152.19.10 (V100R019C00), 5.152.11.20 (V100R011C10), 5.152.11.10 (V100R011C00), 5.152.10.20 (V100R010C10), 5.152.10.10 (V100R010C00), 5.152.09.20 (V100R009C10), 5.152.09.10 (V100R009C00), 5.152.08.20 (V100R008C10), 5.152.08.10 (V100R008C00)

NE	New Version	Compatible Version
OptiX RTN 950	N/A	5.76.19.27 (V100R019C10), 5.76.19.10 (V100R019C00), 5.76.11.20 (V100R011C10), 5.76.11.10 (V100R011C00), 5.76.10.20 (V100R010C10), 5.76.10.10 (V100R010C00), 5.76.09.20 (V100R009C10), 5.76.09.10 (V100R009C00), 5.76.08.20 (V100R008C10), 5.76.08.10 (V100R008C00), 5.76.07.20 (V100R007C10), 5.76.07.10 (V100R007C00), 5.76.06.20 (V100R006C10), 5.76.06.10 (V100R006C00), 5.76.05.20 (V100R005C01), 5.76.05.10 (V100R005C00), 5.76.03.40 (V100R003C03), 5.76.03.30 (V100R003C02), 5.76.03.20 (V100R003C01), 5.76.03.10 (V100R003C00), 5.76.02.30 (V100R002C02), 5.76.02.20 (V100R002C01),

NE	New Version	Compatible Version
		5.76.02.10 (V100R002C00), 5.76.01.40 (V100R001C03), 5.76.01.30 (V100R001C02), 5.76.01.20 (V100R001C01), 5.76.01.10 (V100R001C00), 5.196.19.27(CSHUF) (V100R019C10), 5.196.19.10(CSHUF) (V100R019C00), 5.196.11.20(CSHUF) (V100R011C10), 5.196.11.10(CSHUF) (V100R011C00)

NE	New Version	Compatible Version
OptiX RTN 950A	N/A	5.195.19.27(CSHOF) (V100R019C10), 5.195.19.10(CSHOF) (V100R019C00), 5.195.11.20(CSHOF) (V100R011C10), 5.114.19.27 (V100R019C10), 5.114.19.10 (V100R019C00), 5.114.11.20 (V100R011C10), 5.114.11.10 (V100R011C00), 5.114.10.20 (V100R010C10), 5.114.10.10 (V100R010C00), 5.114.09.20 (V100R009C10), 5.114.09.10 (V100R009C00), 5.114.08.20 (V100R008C10), 5.114.08.10 (V100R008C00), 5.114.07.20 (V100R007C10), 5.114.07.10 (V100R007C00), 5.114.06.20 (V100R006C10), 5.114.06.10 (V100R006C00), 5.114.05.20 (V100R005C01)

NE	New Version	Compatible Version
OptiX RTN 980	N/A	5.83.19.10 (V100R019C00), 5.83.11.20 (V100R011C10), 5.83.11.10 (V100R011C00), 5.83.10.20 (V100R010C10), 5.83.10.10 (V100R010C00), 5.83.09.20 (V100R009C10), 5.83.09.10 (V100R009C00), 5.83.08.20 (V100R008C10), 5.83.08.10 (V100R008C00), 5.83.07.20 (V100R007C10), 5.83.07.10 (V100R007C00), 5.83.06.20 (V100R006C10), 5.83.06.10 (V100R006C00), 5.83.05.20 (V100R005C01), 5.83.05.10 (V100R005C00), 5.83.03.40 (V100R003C03), 5.83.03.30 (V100R003C02), 5.83.03.10 (V100R003C00), 5.178.19.27(CSHNU) (V100R019C10), 5.178.19.10(CSHNU) (V100R019C00), 5.178.11.20(CSHNU) (V100R011C10), 5.178.11.10(CSHNU) (V100R011C00),

NE	New Version	Compatible Version
		5.178.10.20(CSHNU) (V100R010C10), 5.178.10.10(CSHNU) (V100R010C00), 5.178.09.20(CSHNU) (V100R009C10)

NE	New Version	Compatible Version
OptiX RTN 980L	N/A	5.179.19.27(CSHLU) (V100R019C10), 5.179.19.10(CSHLU) (V100R019C00), 5.179.11.20(CSHLU) (V100R011C10), 5.179.11.10(CSHLU) (V100R011C00), 5.179.10.20(CSHLU) (V100R010C10), 5.179.10.10(CSHLU) (V100R010C00), 5.179.09.20(CSHLU) (V100R009C10), 5.140.19.27 (V100R019C10), 5.140.19.10 (V100R019C00), 5.140.11.20 (V100R011C10), 5.140.11.10 (V100R011C00), 5.140.10.20 (V100R010C10), 5.140.10.10 (V100R010C00), 5.140.09.20 (V100R009C10), 5.140.09.10 (V100R009C00), 5.140.08.20 (V100R008C10), 5.140.08.10 (V100R008C00), 5.140.07.20 (V100R007C10), 5.140.07.10 (V100R007C00)

 **NOTE**

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product. Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the NCE, a.bb.cc.2x is supported by version A of the NCE.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the NCE, a.bb.cc.xx is supported by version A of the NCE.

## 10.4 PTN Series

The PTN series NEs managed by NCE vary according to domains. For details, see "Version Requirements" in NCE (Transport Domain) Product Description or NCE (IP Domain) Product Description.

NCE (IP Domain) Manager supports only PTN 6900 series products. To manage other PTN products, deploy IP+T components.

The following table lists the PTN series NE supported.



**Table 10-7** PTN series

NE	New Version	Compatible Version
OptiX PTN 1900	N/A	5.58.08.20 (V100R008C10), 5.58.07.30 (V100R007C10), 5.58.07.10 (V100R007C00), 5.58.06.30 (V100R006C10), 5.58.05.30 (V100R005C01), 5.58.05.10 (V100R005C00), 5.58.03.30 (V100R003C02), 5.58.03.20 (V100R003C01), 5.58.02.90 (V100R002C02SPC600), 5.58.02.60 (V100R002C03), 5.58.02.50 (V100R002C02), 5.58.02.30 (V100R002C01), 5.58.02.10 (V100R002C00), 5.58.01.50 (V100R001C03), 5.58.01.30 (V100R001C02), 5.58.01.10 (V100R001C01)

NE	New Version	Compatible Version
OptiX PTN 3900	N/A	5.59.08.20 (V100R008C10), 5.59.07.30 (V100R007C10), 5.59.07.10 (V100R007C00), 5.59.06.30 (V100R006C10), 5.59.05.30 (V100R005C01), 5.59.05.10 (V100R005C00), 5.59.03.30 (V100R003C02), 5.59.03.20 (V100R003C01), 5.59.02.90 (V100R002C02SPC600), 5.59.02.70 (V100R002C05), 5.59.02.60 (V100R002C03), 5.59.02.50 (V100R002C02), 5.59.02.30 (V100R002C01), 5.59.02.10 (V100R002C00), 5.59.01.50 (V100R001C03), 5.59.01.30 (V100R001C02), 5.59.01.10 (V100R001C01)

NE	New Version	Compatible Version
OptiX PTN 3900-8	N/A	5.78.08.20 (V100R008C10), 5.78.07.30 (V100R007C10), 5.78.07.10 (V100R007C00), 5.78.06.30 (V100R006C10), 5.78.05.30 (V100R005C01), 5.78.05.10 (V100R005C00), 5.78.03.30 (V100R003C02), 5.78.03.20 (V100R003C01), 5.78.02.90 (V100R002C02SPC600), 5.78.02.70 (V100R002C05), 5.78.02.60 (V100R002C03), 5.78.02.50 (V100R002C02)
OptiX PTN 905	N/A	5.88.2.80 (V100R002C05)
OptiX PTN 905A	N/A	5.123.08.20 (V100R008C10), 5.123.07.30 (V100R007C10), 5.123.07.10 (V100R007C00), 5.123.06.30 (V100R006C10), 5.123.05.30 (V100R005C01)

NE	New Version	Compatible Version
OptiX PTN 905B	N/A	5.124.08.20 (V100R008C10), 5.124.07.30 (V100R007C10), 5.124.07.10 (V100R007C00), 5.124.06.30 (V100R006C10), 5.124.05.30 (V100R005C01)
OptiX PTN 905D	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.166.10.10 (V100R010C00)
OptiX PTN 905E	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.163.10.10 (V100R010C00), 8.163.09.10 (V100R009C00)
OptiX PTN 905G	N/A	8.166.09.10 (V100R009C00)
OptiX PTN 906A	N/A	5.145.08.20 (V100R008C10), 5.145.07.30 (V100R007C10), 5.145.07.10 (V100R007C00), 5.145.06.30 (V100R006C10)
OptiX PTN 906AI	N/A	5.159.08.20 (V100R008C10), 5.159.07.30 (V100R007C10), 5.159.07.10 (V100R007C00)

NE	New Version	Compatible Version
OptiX PTN 906B	N/A	5.146.08.20 (V100R008C10), 5.146.07.30 (V100R007C10)
OptiX PTN 910	N/A	5.64.08.20 (V100R008C10), 5.64.07.30 (V100R007C10), 5.64.07.10 (V100R007C00), 5.64.06.30 (V100R006C10), 5.64.05.30 (V100R005C01), 5.64.05.10 (V100R005C00), 5.64.03.30 (V100R003C02), 5.64.03.20 (V100R003C01), 5.64.02.90 (V100R002C01SPC600), 5.64.02.80 (V100R002C01SPC800), 5.64.02.70 (V100R002C05), 5.64.02.60 (V100R002C03), 5.64.02.50 (V100R002C01), 5.64.02.10 (V100R002C00), 5.64.01.50 (V100R001C01), 5.64.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX PTN 910-F	N/A	5.91.08.20 (V100R008C10), 5.91.07.30 (V100R007C10), 5.91.07.10 (V100R007C00), 5.91.06.30 (V100R006C10), 5.91.05.30 (V100R005C01), 5.91.05.10 (V100R005C00), 5.91.03.30 (V100R003C02)
OptiX PTN 910E-F	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.176.10.20 (V100R010C00), 8.176.09.20 (V100R009C10)
OptiX PTN 912	N/A	5.63.01.50 (V100R001C02), 5.63.01.10 (V100R001C01)
OptiX PTN 916-F	N/A	V100R012C00
OptiX PTN 930	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.182.10.20 (V100R010C00)

NE	New Version	Compatible Version
OptiX PTN 950	N/A	5.65.08.20 (V100R008C10), 5.65.07.30 (V100R007C10), 5.65.07.10 (V100R007C00), 5.65.06.30 (V100R006C10), 5.65.05.30 (V100R005C01), 5.65.05.10 (V100R005C00), 5.65.03.30 (V100R003C02), 5.65.03.20 (V100R003C01), 5.65.02.90 (V100R002C01SPC600), 5.65.02.80 (V100R002C01SPC800), 5.65.02.70 (V100R002C05), 5.65.02.60 (V100R002C03), 5.65.02.50 (V100R002C01), 5.65.02.10 (V100R002C00), 5.65.01.50 (V100R001C01), 5.65.01.10 (V100R001C00)

NE	New Version	Compatible Version
OptiX PTN 960	N/A	5.94.08.20 (V100R008C10), 5.94.07.30 (V100R007C10), 5.94.07.10 (V100R007C00), 5.94.06.30 (V100R006C10), 5.94.05.30 (V100R005C01), 5.94.05.10 (V100R005C00), 5.94.03.40 (V100R003C03)
OptiX PTN 960(160G)	N/A	V100R011C00SPC100, V100R011C00, V100R010C00SPC600
OptiX PTN 970	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.182.10.20 (V100R010C00), 8.182.09.20 (V100R009C10), 8.182.09.10 (V100R009C00), 8.182.08.20 (V100R008C10)
OptiX PTN 970C	N/A	V100R012C00
OptiX PTN 980	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00



NE	New Version	Compatible Version
OptiX PTN 990	N/A	V100R012C00SPC300, V100R011C00SPC300, V100R011C00, V100R010C00SPC600, 8.150.10.20 (V100R010C00), 8.150.09.20 (V100R009C10), 8.150.08.20 (V100R008C10SPC300/500), 8.150.08.20 (V100R008C10), 8.150.08.10 (V100R008C00), 8.150.07.20 (V100R007C10)
OptiX PTN 990E	N/A	V100R012C00SPC300

**Table 10-8** PTN6900 series

NE	New Version	Compatible Version
OptiX PTN 6900-1-M4/PTN 6900-2-M8/PTN 6900-2-M16	V800R011C10	V800R011C00, V800R010C10
OptiX PTN 6900-1/2/M2E/M2F	V800R011C10	V800R011C00, V800R010C10
OptiX PTN 6900-1/PTN 6900-2/PTN 6900-3/PTN 6900-8/PTN 6900-16	N/A	V600R009C50
OptiX PTN 6900-2-M8A/M16A	V800R011C10	V800R011C00, V800R010C10
OptiX PTN 6900-3/8/16/3A/8A/16A	V800R011C10	V800R011C00, V800R010C10
OptiX PTN 6900-F1A-14H24Q	V800R011C10	V800R011C00

NE	New Version	Compatible Version
PTN 6900-1 PTN 6900-2 PTN 6900-3 PTN 6900-8 PTN 6900-16	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC600, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00
PTN 6900-1 PTN 6900-3 PTN 6900-8 PTN 6900-16	N/A	V6R3C02
PTN 6900-2-M14	V800R012C00	N/A
PTN 6900-2-M8C	V800R011C10	N/A
PTN6900-1-M4 PTN6900-2-M8 PTN6900-2-M16	N/A	V8R6C10, V8R6C00, V8R5C01
PTN6900-1-M4 PTN6900-2-M8 PTN6900-2-M16 PTN 6900-3 PTN 6900-3A PTN 6900-8 PTN 6900-16 PTN 6900-8A PTN 6900-16A	N/A	V8R7C00
PTN6900-1-M4 PTN6900-2-M8 PTN6900-2-M16 PTN 6900-3 PTN 6900-3A PTN 6900-8 PTN 6900-16 PTN 6900-8A PTN 6900-16A PTN6900- M2E PTN6900-M2F	N/A	V8R8C00, V8R7C10

NE	New Version	Compatible Version
PTN6900-1-M4 PTN6900-2-M8 PTN6900-2-M16 PTN 6900-3 PTN 6900-3A PTN 6900-8 PTN 6900-16 PTN 6900-8A PTN 6900-16A PTN6900- M2E PTN6900-M2F PTN6900-2-M8A PTN6900-2-M16A	N/A	V8R9C10, V8R9C00, V8R8C11, V8R8C10, V8R10C10, V8R10C00
PTN6900-1-M4 PTN6900-2-M8 PTN6900-2-M16 PTN 6900-3 PTN 6900-3A PTN 6900-8 PTN 6900-16 PTN 6900-8A PTN 6900-16A PTN6900- M2E PTN6900-M2F PTN6900-M2K PTN6900-2-M8A PTN6900-2-M16A PTN6900-F1A-14H24Q PTN6900-M2K-B	N/A	V8R11C10, V8R11C00
PTN6900-F1A-14H24Q	V800R012C00	N/A
PTN6900-M2K	V800R012C00, V800R011C10, V800R011C00	N/A

**Table 10-9** PTN7900 series

NE	New Version	Compatible Version
OptiX PTN 7900-12	V100R012C00, V100R011C00SPC100, 8.148.11.10 (V100R011C00), 8.148.10.20 (V100R010C00SPC600), 8.148.10.10 (V100R010C00)	V100R011C00, V100R010C00SPC600, 8.148.10.20 (V100R010C00), 8.148.09.20 (V100R009C10), 8.148.08.20 (V100R008C10), 8.148.08.10 (V100R008C00), 8.148.07.20 (V100R007C10), 8.148.07.10 (V100R007C00)
OptiX PTN 7900-24	V100R012C00, V100R011C00SPC100, 8.135.11.10 (V100R011C00), 8.135.10.20 (V100R010C00SPC600), 8.135.10.10 (V100R010C00)	V100R011C00, V100R010C00SPC600, 8.135.10.20 (V100R010C00), 8.135.09.20 (V100R009C10), 8.135.08.20 (V100R008C10), 8.135.08.10 (V100R008C00), 8.135.07.20 (V100R007C10), 8.135.07.10 (V100R007C00), 8.135.06.30 (V100R006C20), 8.135.06.20 (V100R006C10)

NE	New Version	Compatible Version
OptiX PTN 7900-32	V100R012C00, V100R011C00SPC100, 8.128.11.10 (V100R011C00), 8.128.10.20 (V100R010C00SPC600), 8.128.10.10 (V100R010C00)	V100R011C00, V100R010C00SPC600, 8.128.10.20 (V100R010C00), 8.128.09.20 (V100R009C10), 8.128.08.20 (V100R008C10), 8.128.08.10 (V100R008C00), 8.128.07.20 (V100R007C10), 8.128.07.10 (V100R007C00), 8.128.06.30 (V100R006C20), 8.128.06.20 (V100R006C10), 8.128.06.10 (V100R006C00)
OptiX PTN 7900E-12	V100R012C00, V100R011C00SPC100, 8.148.11.10 (V100R011C00), 8.148.10.20 (V100R010C00SPC600), 8.148.10.10 (V100R010C00)	V100R011C00, V100R010C00SPC600, 8.148.10.20 (V100R010C00)
OptiX PTN 7900E-24	V100R012C00, V100R011C00SPC100, 8.135.11.10 (V100R011C00), 8.135.10.20 (V100R010C00SPC600), 8.135.10.10 (V100R010C00)	V100R011C00, V100R010C00SPC600, 8.135.10.20 (V100R010C00)

NE	New Version	Compatible Version
OptiX PTN 7900E-32	V100R012C00, V100R011C00SPC100, 8.128.11.10 (V100R011C00), 8.128.10.20 (V100R010C00SPC600), 8.128.10.10 (V100R010C00), 8.128.09.20 (V100R009C10)	V100R011C00, V100R010C00SPC600, 8.128.10.20 (V100R010C00), 8.128.09.20 (V100R009C10)

 **NOTE**

Rules for defining commercial versions of NE software: a.bb.cc.dd. "a" indicates the NE platform version. Currently, 4, 5 and 8 are supported. "bb" indicates the product name. "cc" indicates the R version of the product. To be specific, 01 represents R001, 02 represents R002, and so on. "dd" indicates the C version of the product. Mapping principle:

1. If the mapping table provides only the information that a.bb.cc.20 is supported by version A of the NCE, a.bb.cc.2x is supported by version A of the NCE.
2. If the mapping table provides only the information that a.bb.cc is supported by version A of the NCE, a.bb.cc.xx is supported by version A of the NCE.

## 10.5 NE/ATN/CX/Multi-service gateways Series

Manageable NE/ATN/CX/Multi-service gateways series NE is listed as follows:

**Table 10-10** NE series

NE	New Version	Compatible Version
CH-NE40E-X8/X16 CH-NE40E-X8A/X16A CH-NE40E-X3 CH-NE40E-X3A	N/A	V8R10C10SPC800
CX600-X8 CX600-X8A CX600-X16 CX600-X16A NE40E-X8 NE40E-X8A NE40E-X16 NE40E-X16A	N/A	V8R6C30
NE05E-S2 NE05E-SG NE05E-SH NE05E-SI	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10

NE	New Version	Compatible Version
NE05E-SE NE05E-SF	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10
NE05E-SJ NE05E-SK NE05E-SL NE05E-SM	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10
NE05E-SN	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00
NE05E-SQ NE05E-SR	N/A	V3R3C10, V3R3C00, V3R2C10, V3R2C00, V3R1C10
NE05E-SQ NE05E-SR NE05E-S2	N/A	V3R5C10, V3R5C00
NE05E/NE08E	N/A	V300R005C10, V300R005C00, V300R003C10
NE08E-S6	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10

NE	New Version	Compatible Version
NE08E-S6E	N/A	V3R3C00, V3R2C10, V3R2C00, V3R1C10
NE08E-S6E NE08E-S9	N/A	V3R5C10, V3R5C00, V3R3C10
NE16/NE08	N/A	V1R7
NE16E/NE08E/NE05	N/A	V3R2, V1R7
NE16EX	N/A	V2R5C10
NE16EX-6 NE16EX	N/A	V2R5C30, V2R5C20
NE20-2/4/8	N/A	V2R5, V2R3
NE20E-8	N/A	V2R5, V2R3
NE20E-S16A	N/A	V800R011C10, V800R011C00
NE20E-S2/S4/S8/S16	N/A	V800R011C10, V800R011C00, V800R010C10
NE20E-S2E NE20E-S2F NE20E-S4 NE20E-S8 NE20E-S16	N/A	V8R8C00, V8R7C10, V8R7C00
NE20E-S2E NE20E-S2F NE20E-S4 NE20E-S8 NE20E-S16 NE20E-S8A NE20E-S16A	N/A	V8R9C10, V8R9C00, V8R8C11, V8R8C10, V8R10C10, V8R10C00
NE20E-S2E NE20E-S2F NE20E-S4 NE20E-S8 NE20E-S16 NE20E-S8A NE20E-S16A NE20E-S16B	N/A	V8R11C10, V8R11C00



NE	New Version	Compatible Version
NE20E-S4 NE20E-S8	N/A	V8R5C00
NE20E-S4 NE20E-S8 NE20E-S16	N/A	V8R6C10, V8R5C01
NE20E-S8A	N/A	V800R011C10, V800R011C00
NE20E-X6	N/A	V6R9C20, V6R9C10, V6R9C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00
NE40	N/A	V3R5, V3R2, V1R2
NE40E-4/8/NE80E	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7, V6R6, V6R5, V6R3, V6R2, V6R1, V600R009C50, V3R6, V3R3, V3R2, V3R1
NE40E-F1A-14H24Q	N/A	V800R011C10, V800R011C00

NE	New Version	Compatible Version
NE40E-M16A	N/A	V800R011C00
NE40E-M2	N/A	V800R011C10, V800R011C00, V800R010C10
NE40E-M2E NE40E-M2F CX600-M2E CX600-M2F NE40E-X1-M4 NE40E-X2-M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2-M8 CX600-X2-M16	N/A	V8R7C10
NE40E-M2E NE40E-M2F CX600-M2E CX600-M2F NE40E-X1-M4 NE40E-X2-M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2-M8 CX600-X2-M16 CX600-X3 CX600-X3A CX600-X8 CX600-X8A CX600-X16 CX600-X16A NE40E-X3 NE40E-X3A NE40E-X8 NE40E-X8A NE40E-X16 NE40E-X16A CX600-X3-DO CX600-X8-DO	N/A	V8R8C00, V8R7C00
NE40E-M2E NE40E-M2F CX600-M2E CX600-M2F NE40E-X1-M4 NE40E-X2-M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2-M8 CX600-X2-M16 CX600-X3A-DO CX600-X8A-DO CX600-X16-DO CX600-X16A-DO NE40E-X2-M8A NE40E-X2-M16A CX600-X2-M8A CX600-X2-M16A	N/A	V8R8C11, V8R8C10

NE	New Version	Compatible Version
NE40E-M2E NE40E-M2F NE40E-M2H CX600-M2E CX600-M2F CX600-M2H NE40E-X1-M4 NE40E-X2- M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2- M8 CX600-X2-M16 CX600-X3A-DO CX600- X8A-DO CX600-X16-DO CX600-X16A-DO NE40E- X2-M8A NE40E-X2-M16A CX600-X2-M8A CX600- X2-M16A NE40E-X3 NE40E-X3A NE40E-X8 NE40E-X8A NE40E-X16 NE40E-X16A	N/A	V8R9C10, V8R9C00, V8R10C00
NE40E-M2E NE40E-M2F NE40E-M2H NE40E-M2K CX600-M2E CX600-M2F CX600-M2H CX600-M2K NE40E-X1-M4 NE40E-X2- M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2- M8 CX600-X2-M16 CX600-X3A-DO CX600- X8A-DO CX600-X16-DO CX600-X16A-DO NE40E- X2-M8A NE40E-X2-M16A CX600-X2-M8A CX600- X2-M16A NE40E-M8A NE40E-M16A CX600- F1A-14H24Q NE40E- F1A-14H24Q CX600- M2K-B NE40E-M2K-B NE40E-X3 NE40E-X3A NE40E-X8 NE40E-X8A NE40E-X16 NE40E-X16A	N/A	V8R11C10, V8R11C00

NE	New Version	Compatible Version
NE40E-M2E NE40E-M2F NE40E-M2H NE40E-M2K CX600-M2E CX600-M2F CX600-M2H CX600-M2K NE40E-X1-M4 NE40E-X2-M8 NE40E-X2-M16 CX600-X1-M4 CX600-X2-M8 CX600-X2-M16 CX600-X3A-DO CX600-X8A-DO CX600-X16-DO CX600-X16A-DO NE40E-X2-M8A NE40E-X2-M16A CX600-X2-M8A CX600-X2-M16A NE40E-M8A NE40E-M16A NE40E-X3 NE40E-X3A NE40E-X8 NE40E-X8A NE40E-X16 NE40E-X16A	N/A	V8R10C10
NE40E-M8A	N/A	V800R011C00
NE40E-X1-M4 NE40E-X2-M8 CX600-X1-M4 CX600-X2-M8 CX600-M8-DO CX600-M4-DO CX600-X2-M16 CX600-M16-DO NE40E-X2-M16 NE40E-X8 CX600-X8 NE40E-X16 CX600-X16 NE40E-X8A CX600-X8A NE40E-X16A CX600-X16A	N/A	V8R6C10
NE40E-X1-M4 NE40E-X2-M8 CX600-X1-M4 CX600-X2-M8 CX600-X2-M8-DO	N/A	V8R5C00
NE40E-X1-M4 NE40E-X2-M8 CX600-X1-M4 CX600-X2-M8 CX600-X2-M8-DO CX600-X1-M4-DO CX600-X2-M16 CX600-X2-M16-DO NE40E-X2-M16	N/A	V8R5C01

NE	New Version	Compatible Version
NE40E-X1-M4 NE40E-X2-M8 CX600-X1-M4 CX600-X2-M8 CX600-X2-M8-DO CX600-X1-M4-DO CX600-X2-M16 CX600-X2-M16-DO NE40E-X2-M16 NE40E-X8 CX600-X8 NE40E-X16 CX600-X16	N/A	V8R6C00
NE40E-X1/X2	N/A	V800R011C10, V800R011C00, V800R010C10, V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC501, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00&C01, V6R2C05, V6R2C03
NE40E-X16B	N/A	V800R011C10, V800R011C00, V800R010C10
NE40E-X16B(V8)	N/A	V8R9C10, V8R11C10, V8R11C00, V8R10C10, V8R10C00
NE40E-X16C	N/A	V800R011C10
NE40E-X2-M14	N/A	V800R012C00

NE	New Version	Compatible Version
NE40E-X3/X8/X16	N/A	V800R011C10, V800R011C00, V800R010C10
NE40E-X3/X8/X16 NE40E-X16A	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00&C01, V6R2C02, V6R2C01, V6R2C00, V6R1C01, V6R1C00
NE40E-X3A	N/A	V800R011C10, V800R011C00
NE40E-X4A(V8)	N/A	V800R012C10
NE40E-X8	N/A	V600R009C20
NE40E-X8A(V8)	N/A	V800R012C10
NE40E-X8A/X16A	N/A	V800R011C10, V800R011C00, V800R010C10
NE40E-X8AK(V8)	N/A	V800R012C10
NE40E-X8C	N/A	V800R011C10

NE	New Version	Compatible Version
NE5000E	N/A	V800R011C10, V800R011C00, V800R010C10, V3R7C00, V3R5, V2R3, V2R2
NE5000E-16 NE5000E-X16	N/A	V8R3C00, V8R2C01, V8R2C00
NE5000E-16 NE5000E-X16 NE5000E-X16A	N/A	V8R6C10, V8R6C00, V8R5C01, V8R5C00
NE5000E-16 NE5000E-X16 NE5000E-X16A NE5000E-X16B	N/A	V8R9C10, V8R9C00, V8R8C10, V8R8C00, V8R7C10, V8R7C00, V8R11C10SPC200, V8R11C10, V8R11C00, V8R10C10, V8R10C00
NE5000E-Multi	N/A	V800R011C10, V800R011C00, V800R010C10, V3R7C00, V3R6C02, V3R5
NE5000E-Multi-S(V8)	N/A	V800R012C10
NE5000E-S	N/A	V800R011C10
NE80	N/A	V3R5, V3R2, V1R2

NE	New Version	Compatible Version
NE9000	N/A	V8R9C10, V8R9C00, V8R8C10, V800R011C10, V800R011C00, V800R010C10
NE9000 NE9000-8	N/A	V8R10C10, V8R10C00
NE9000 NE9000-8 NE9000-20	N/A	V8R11C10
NE9000 NE9000-8 NE9000-8-LS NE9000-20-LS NE9000-20	N/A	V8R11C00
NE9000-8-ADMIN NE9000-20-ADMIN	N/A	V8R11C00
NetEngine 8000 F1A	N/A	V800R012C00
NetEngine 8000 M14	N/A	V800R012C00
NetEngine 8000 M14K	N/A	V800R012C10
NetEngine 8000 M1A	N/A	V800R012C00
NetEngine 8000 M1D	N/A	V800R012C10
NetEngine 8000 M6	N/A	V800R012C00
NetEngine 8000 M6K	N/A	V800R012C10
NetEngine 8000 M8	N/A	V800R012C00, V800R011C10
NetEngine 8000 M8K	N/A	V800R012C10
NetEngine 8000 X4	N/A	V800R012C00
NetEngine 8000 X8	N/A	V800R012C00

**Table 10-11** ATN series

NE	New Version	Compatible Version
ATN 905 ATN 905A ATN 905A-P	N/A	V2R2C01



NE	New Version	Compatible Version
ATN 905 ATN 905A ATN 905A-P ATN905A-V ATN905A-V AC	N/A	V2R3C10, V2R3C00
ATN 905 ATN 905A ATN 905A-P ATN905A-V ATN905A-V AC ATN905-V AC ATN905 DC	N/A	V2R3C10 V2R3C20
ATN-905-AC(V8) ATN-905-DC(V8)	N/A	V3R5C10, V3R5C00, V3R3C10
ATN905	N/A	V300R003C10
ATN905 AC ATN905A AC ATN905A-P AC ATN905A-V AC ATN905-V AC ATN905 DC ATN905A-C ATN905A-D ATN905E	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C00, V2R5C10
ATN905 AC ATN905A AC ATN905A-P AC ATN905A-V AC ATN905-V AC ATN905 DC ATN905A-C ATN905A-D ATN905E ATN905-BM	N/A	V2R6C10
ATN905-F	N/A	V300R005C10, V300R005C00
ATN905-G(V8)	N/A	V300R006C10
ATN905A ATN905A-P ATN905A-V ATN905-V ATN905C	N/A	V2R5C00
ATN910	N/A	V2R1C02, V2R1C01, V2R1C00
ATN910 ATN910I	N/A	V2R2C00
ATN910 ATN910I ATN 910I-D	N/A	V2R5C00
ATN910 ATN910I ATN 910I-P	N/A	V2R3C00, V2R2C01

NE	New Version	Compatible Version
ATN910 ATN910I ATN910I-P ATN910I-D DC ATN910I-D AC ATN910I-B DC ATN910I-E DC	N/A	V2R3C20, V2R3C10, V2R3C10
ATN910 ATN910I ATN910I AC ATN910I DC ATN910I-C AC ATN910I-TC DC ATN910I-P AC ATN910I-D DC ATN910I-D AC ATN910I-B DC ATN910I-E DC	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00
ATN910B	N/A	V300R005C10, V300R005C00, V300R003C10, V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10, V2R5C00, V2R3C10 V2R3C20, V2R3C10, V2R3C00
ATN910B(V8) ATN910B-D AC(V8) ATN910B-D DC(V8) ATN910B-E AC(V8) ATN910B-E DC(V8) ATN910B-F AC(V8) ATN910B-F DC(V8)	N/A	V3R5C10, V3R5C00, V3R3C10, V3R3C00
ATN910C	N/A	V300R003C10
ATN910C-A	N/A	V300R005C10, V300R005C00
ATN910C-A ATN910C-B ATN910C-D	N/A	V3R3C10, V3R3C00, V3R2C10, V3R2C00, V3R1C10

NE	New Version	Compatible Version
ATN910C-A ATN910C-B ATN910C-D ATN910C-F	N/A	V3R5C00
ATN910C-A ATN910C-B ATN910C-D ATN910C-F ATN910C-H ATN910C-S	N/A	V3R5C10
ATN910C-B	N/A	V300R005C10, V300R005C00
ATN910C-D	N/A	V300R005C10, V300R005C00
ATN910C-F	N/A	V300R005C10, V300R005C00
ATN910C-G	N/A	V300R006C00
ATN910C-H	N/A	V300R005C10
ATN910C-S	N/A	V300R005C10
ATN910D	N/A	V300R006C10
ATN910D-A	N/A	V300R006C10
ATN910I AC ATN910I DC ATN910I-C AC ATN910I- TC DC ATN910I-P ATN910I-D DC ATN910I- D AC ATN910I-B DC ATN910I-E DC	N/A	V2R5C10
ATN950	N/A	V2R6C20SPC800, V2R5C00, V2R3C10, V2R3C10, V2R3C00, V2R2C01, V2R2C00, V2R1C02, V2R1C01, V2R1C00

NE	New Version	Compatible Version
ATN950B	N/A	V300R005C10, V300R005C00, V300R003C10, V2R6C20SPC800, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10, V2R5C00, V2R3C10 V2R3C20, V2R3C10, V2R3C00, V2R2C01, V2R2C00, V2R1C02
ATN950B(160G)	N/A	V3R5C10, V3R5C00, V3R3C10
ATN950B(V8)	N/A	V3R5C10, V3R5C00, V3R3C10, V3R3C00
ATN950C	N/A	V3R5C10, V3R5C00, V3R3C10, V3R3C00, V3R2C10, V3R2C00, V3R1C10, V300R005C10, V300R005C00, V300R003C10
ATN950D	N/A	V300R006C00

NE	New Version	Compatible Version
ATN980/ATN990	N/A	V6R6C00, V6R5C00, V6R3C00&C01, V6R2C05, V6R2C03
ATN980B	N/A	V3R5C10, V3R5C00, V3R3C10, V3R3C00, V3R2C10, V3R2C00, V3R1C10, V3R1C00, V300R005C10, V300R005C00, V300R003C10
ATN980C	N/A	V3R5C10, V300R005C10

**Table 10-12** ETN series

NE	New Version	Compatible Version
ETN500-A ETN500-B ETN500-C ETN550-A	N/A	V2R6C20SPC800, V2R6C20SPC600, V2R6C20SPC600, V2R6C20, V2R6C10, V2R6C00, V2R5C10
ETN500-D	N/A	V300R003C10
ETN500-F	N/A	V3R5C10, V3R5C00, V3R3C10, V300R005C10, V300R005C00

**Table 10-13** CX series

NE	New Version	Compatible Version
CX200	N/A	V1R5, V1R2
CX200C	N/A	V1R5
CX300	N/A	V1R5, V1R2
CX600-4/8/16	N/A	V6R9, V3R6, V2R2, V2R1, V1R1
CX600-F1A-14H24Q	N/A	V800R011C10, V800R011C00
CX600-M2	N/A	V800R011C10, V800R011C00, V800R010C10
CX600-X1-M4	N/A	V800R011C10, V800R011C00

NE	New Version	Compatible Version
CX600-X1/X2	N/A	V800R011C10, V800R011C00, V800R010C10, V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00&C01, V6R2C05, V6R2C03
CX600-X2-M16/M16A	N/A	V800R011C10, V800R011C00
CX600-X2-M16B	N/A	V800R011C10, V800R011C00
CX600-X2-M8/M8A	N/A	V800R011C10, V800R011C00
CX600-X3-DO/X8-DO/ X16-DO	N/A	V800R011C10, V800R011C00, V800R010C10
CX600-X3/X8/X16	N/A	V800R011C10, V800R011C00, V800R010C10

NE	New Version	Compatible Version
CX600-X3/X8/X16 CX600-X3-DO/X8-DO/X16-DO CX600-4/8/16	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00&C01, V6R2C05, V6R2C02, V6R2C00, V6R1C01, V6R1C00
CX600-X3A-DO/X8A-DO/X16A-DO	N/A	V800R011C10, V800R011C00
CX600-X3A/X8A/X16A	N/A	V800R011C10, V800R011C00
CX6600	N/A	V800R011C10, V800R011C00, V800R010C10
CX6601-14H24Q	N/A	V800R011C00
CX6602	N/A	V800R011C00, V800R010C10
CX6602 CX6602-B	N/A	V8R11C10, V8R11C00
CX6602-A	N/A	V8R10C10
CX6608	N/A	V800R011C00



NE	New Version	Compatible Version
CX6608 CX6620	N/A	V8R11C10, V8R11C00, V8R10C10, V8R10C00
CX6620	N/A	V800R011C00

**Table 10-14** Multi-service gateways series

NE	New Version	Compatible Version
BGW9916	N/A	V1R2C50, V1R2C30, V1R2C20, V1R2C10, V1R2C00, V1R1C10, V1R1C00, V100R002C50SPC200
MA5200F	N/A	V1R7
MA5200G	N/A	V3R3, V3R2, V2R3
ME60	N/A	V600R009C50
ME60-4 ME60-8 ME60-16	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V1R6C05
ME60-8 ME60-16	N/A	V1R6, V1R5, V1R3, V1R2
ME60-X16/X16A	N/A	V800R011C10, V800R011C00
ME60-X16A ME60-X8A ME60-X16 ME60-X8 ME60-X3	N/A	V8R10C10SPC800

NE	New Version	Compatible Version
ME60-X16A ME60-X8A ME60-X16 ME60-X8 ME60-X3 ME60-X2-M8 ME60-X2-M16 ME60-X2-M8A ME60-X2-M16A	N/A	V8R9C10, V8R9C00, V8R8C11, V8R8C10, V8R11C10, V8R11C00, V8R10C10, V8R10C00
ME60-X3	N/A	V800R011C10, V800R011C00
ME60-X3/X8/X16	N/A	V6R9C20SPCa00, V6R9C20SPC900, V6R9C20SPC500, V6R9C20, V6R9C10, V6R9C00, V6R8C20, V6R8C10, V6R8C00, V6R7C00, V6R6C00, V6R5C00, V6R3C05 V6R5C00, V6R3C00&C01, V6R2C02, V6R2C00
ME60-X8/X8A	N/A	V800R011C10, V800R011C00
S8016	N/A	V5R3

**Table 10-15** VNE series

NE	New Version	Compatible Version
VNE 9000	N/A	V1R6C00, V1R5C10, V1R5C00, V1R3C00, V1R19C00
VNE 9000(vBRAS-CP)	N/A	V1R6C00, V1R5C10, V1R5C00, V1R19C00
VNE1000	N/A	V1R2C00, V1R1C00
VNE9000(vBRAS-CP)	N/A	V100R005C10
VSIG9800	N/A	V3R8C10, V1R3C00
vRGW	N/A	V1R1C00

## 10.6 R/AR Series

The following table lists the R/AR series NE supported.

**Table 10-16** R/AR series

NE	New Version	Compatible Version
AR 18-18	N/A	Version 1.74 Release 0108
AR1000V	N/A	V2R8C20
AR1000V AR2204-51GE-R AR2504-D-H	N/A	V2R8C30/V2R8C50
AR101GW-Lc-S AR109AR109W AR109GW-L	N/A	V2R8C30/V2R8C50
AR1200	V200R009C00	N/A

NE	New Version	Compatible Version
AR121-S AR156W AR151G-C AR151-S AR151W-P-S AR151G-U-S AR151 AR157 AR156 AR158E AR157VW AR158EVW AR151G-HSPA+7 AR157G-HSPA+7 AR151W-P AR157W	N/A	V2R5C30, V2R5C20, V2R5C10

NE	New Version	Compatible Version
AR121-S AR156W AR151G-C AR151-S AR151W-P-S AR151G-U-S AR151 AR157 AR156 AR158E AR157VW AR158EVW AR151G-HSPA+7 AR157G-HSPA+7 AR151W-P AR157W AR161-S AR161 AR161G-L AR169 AR169-P-M9 AR169G-L AR121 AR121-S(SOC) AR129 AR161F-S	N/A	V2R6C10
AR121W AR129W AR121W-S AR121GW-L AR129GW-L AR129	N/A	V2R7C00

NE	New Version	Compatible Version
AR1220-D AR2201-48FE AR2202-48FE AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S AR2220L AR2230L AR2204	N/A	V2R3C00
AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S	N/A	V2R2C01, V2R2C00
AR1220 AR2220 AR2240 AR3260 AR1220V	N/A	V2R1C00
AR1220 AR2220 AR2240 AR3260 AR1220V AR1220W AR1220VW	N/A	V2R1C01
AR1220C	N/A	V2R7C00

NE	New Version	Compatible Version
AR1220L-S AR1220F AR2201-48FE-S AR2204-S AR2240-S AR1220-D AR2201-48FE AR2202-48FE AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S AR1220E AR1220EV AR1220EVW AR1220E-S AR2220E AR3260-S AR3670(SRU-x5) AR1220F-S	N/A	V2R6C10

NE	New Version	Compatible Version
AR1220L-S AR1220F AR2201-48FE-S AR2204-S AR2240-S AR1220-D AR2201-48FE AR2202-48FE AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S AR1220E AR1220EV AR1220EVW AR1220E-S AR2220E AR3260-S AR3670(SRU-x5) AR1220F-S AR2204-27GE AR2204-27GE-P AR2204-51GE-P AR2204E AR2240C AR2504-H AR3260	N/A	V2R9C00, V2R7C00



NE	New Version	Compatible Version
AR1220L-S AR1220F AR2201-48FE-S AR2204-S AR2240-S AR1220-D AR2201-48FE AR2202-48FE AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S AR2220L AR2230L AR2204	N/A	V2R5C30, V2R5C20, V2R5C10, V2R5C00
AR129CGVW-L	N/A	V2R10C00SPC200
AR129CGVW-L AR101-S AR101W-S	N/A	V2R8C20
AR150	V200R009C00	N/A
AR151 AR157	N/A	V2R2C01, V2R2C00
AR151 AR157 AR156 AR158E	N/A	V2R2C02

NE	New Version	Compatible Version
AR151 AR157 AR156 AR158E AR157VW AR158EVW AR151G-HSPA+7 AR157G-HSPA+7 AR151W-P AR157W	N/A	V2R3C00
AR151G-C AR151-S AR151W-P-S AR151G-U-S AR151 AR157 AR156 AR158E AR157VW AR158EVW AR151G-HSPA+7 AR157G-HSPA+7 AR151W-P AR157W	N/A	V2R5C00

NE	New Version	Compatible Version
AR1610 AR161EGW-L AR169JFVW-4B4S AR502EGRz-Lc AR1504-24S AR1504-24T AR1504-16S8T AR1504-8S16T AR168F-4P AR129CV AR550C-2C6GE-2D AR550E AR161FG-Lc AR502EGRz-L AR503EDGW-Lo AR502EG-L-PD AR161FV-1P AR169W-P-M9 AR169RW-P-M9 AR531GZ-U-D AR161FGW-La AR515GW-LM9-D AR161G-U AR161W AR169W AR502G-L-D-H AR502GR-L-D-H AR161FW AR509G-L-D-H AR151-S2 AR169 AR502G	N/A	V2R9C00

NE	New Version	Compatible Version
AR161FG-L AR161FGW-L AR161F-S AR168F AR169F AR531-2C-H AR531-F2C-H AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW	N/A	V2R5C10
AR161FV-1P AR169W-P-M9 AR169RW-P-M9 AR531GZ-U-D AR161FGW-La AR515GW-LM9-D AR161G-U AR161W AR169W AR502G-L-D-H AR502GR-L-D-H AR161FW AR509G-L-D-H AR151-S2 AR169 AR502G	N/A	V2R7C00

NE	New Version	Compatible Version
AR162F AR169FVW AR161FW-P-M5 AR169FGVW-L AR161FG-L AR161FGW-L AR161F-S AR168F AR169F AR531-2C-H AR531-F2C-H AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW	N/A	V2R5C20
AR168F AR169F AR531-2C-H AR531-F2C-H AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW	N/A	V2R5C00

NE	New Version	Compatible Version
AR18-12	N/A	Bootrom Version is 5.27 VRP (R) software, Version 1.74 Release 0108 8040V200R007B06D467, VRP 1.74
AR18-21	N/A	VRP 3.4 R1711P04
AR19-10	N/A	Version 5.20, Release 1618P10 Extended BootROM Version: 1.19
AR19-10w	N/A	VRP Software, Version 5.20, Release 1618P10
AR19-13I	N/A	Version 5.20, Release 1618P10 Extended BootROM Version: 1.19
AR19-13IW	N/A	VRP Software, Version 5.20, Release 1618P10
AR19-15I	N/A	Version 5.20, Release 1618P10 Extended BootROM Version: 1.19
AR19-15IW	N/A	VRP Software, Version 5.20, Release 1618P10
AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S	N/A	V2R2C00

NE	New Version	Compatible Version
AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7	N/A	V2R2C02, V2R2C01
AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW	N/A	V2R3C00
AR2201-48FE AR2202-48FE AR1220 AR1220V AR2220 AR2240 AR3260 AR1220-S AR1220VW AR1220W AR1220W-S	N/A	V2R2C02
AR2504-H AR2204-51GE AR2204E-D AR2504E-H	N/A	V2R8C20

NE	New Version	Compatible Version
AR28	VRP3.40 Release 0109P10, VRP3.40 R0201	N/A
AR28-09	N/A	Version 3.40, Release 0201P26
AR28-30	N/A	Version 3.40, Release 0201P26, Version 3.40, Feature 0308
AR28-31	N/A	VRP340-R0201P23, 8040V300R003B04D040S P69 (COMWAREV300R002B6 2D014) VRP 3.40, Release 0201P26
AR28-80	N/A	VRP (R) software, Version 1.74 Release 0108 8040V200R007B06D467, VRP 1.74 Bootrom Version is 7.03
AR29	VRP5.20 R2104[11], VRP5.20 R1618	N/A
AR29-01	N/A	Version 5.20, Release 1618
AR29-41	N/A	Version 5.20, Release 1618
AR46	VRP3.40 RT-0015	N/A
AR46-20	N/A	Version 3.40, Release 0201P26
AR46-40	N/A	8040V300R003B04D040S P69 (COMWAREV300R002B6 2D014) VRP Version 3.40, Release 0201P26



NE	New Version	Compatible Version
AR46-80	N/A	Version 3.40, Feature 0305, 8040V300R003B04D040S P69 (COMWAREV300R002B6 2D014) VRP Version 3.40, Release 0201P26
AR49-45	N/A	V300R003
AR49-65	N/A	V300R003
AR509G-Lc AR502EGRc-Lc AR502CG-L AR161FGW-Lc AR161G-Lc AR201V AR503EDGW-Lc3 AR502EGRb-L AR169CVW-4B4S AR169CVW AR169EGW-L AR169EW AR161EW AR161EW-M1	N/A	V2R8C30/V2R8C50

NE	New Version	Compatible Version
AR511GW-LAV2M3 AR511GW-L-B3 AR511GW-LM7 AR513W-V3M8 AR169FGW-L AR161F AR162F AR169FVW AR161FW-P-M5 AR169FGVW-L AR161FG-L AR161FGW-L AR161F-S AR168F AR169F AR531-2C-H AR531-F2C-H AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW AR511GW-LAV2M3 AR511GW-L-B3 AR511GW-LM7 AR513W-V3M8	N/A	V2R5C30

NE	New Version	Compatible Version
AR511GW-LAV2M3 AR511GW-L-B3 AR511GW-LM7 AR513W-V3M8 AR169FGW-L AR161F AR162F AR169FVW AR161FW-P-M5 AR169FGVW-L AR161FG-L AR161FGW-L AR161F-S AR168F AR169F AR531-2C-H AR531-F2C-H AR201 AR206 AR207 AR207V AR207V-P AR208E AR201-S AR207-S AR207G-HSPA+7 AR201VW-P AR207VW AR511GW-LAV2M3 AR511GW-L-B3 AR511GW-LM7 AR513W-V3M8 AR503GW-LM6 AR509G-L AR161FW AR169BF AR169FV-8S AR169FVW-8S	N/A	V2R6C10

NE	New Version	Compatible Version
AR531G-U-D-H AR531GPe-U-H AR531GR-U-H AR550-8FE-D-H AR550-24FE-D-H AR502G AR531GP-H AR531GB-U-D-H	N/A	V2R5C70
AR550C-4GE AR550C-2C6GE AR509CG-Lt AR503EDGW-Lc AR532 AR502EG-L AR502EGW-L AR161FW AR111-S AR531-2C-H AR531-F2C-H AR531G-U-D-H AR531GPe-U-H AR531GR-U-H AR515GW-LM9-D AR511CGW-LAV2M3 AR503GW-LcM7 AR509CG-Lc	N/A	V2R9C00, V2R8C20
AR611W	V300R019C10	N/A
AR611W-LTE4CN	V300R019C10	N/A
AR6120	N/A	V3R19C00SPC200
AR6120-S	V300R019C10	N/A
AR6121	V300R019C10	N/A
AR6140-16G4XG	AR V300R019C10	N/A
AR6140-9G-2AC	AR V300R019C00	N/A
AR6140-S	AR V300R019C00	N/A
AR617VW	V300R019C10	N/A

NE	New Version	Compatible Version
AR617VW-LTE4EA	V300R019C10	N/A
AR6280	AR V300R019C00	N/A
AR6300	AR V300R019C00	N/A
AR6300-S	AR V300R019C00	N/A
AR651C	AR V300R019C00	N/A
AR651U-A4-LTE4EA	AR V300R019C10	N/A
AR651U-A4-LTE6EA	AR V300R019C10	N/A
AR651-LTE6EA	AR V300R019C10	N/A
AR651F-Lite	AR V300R019C10	N/A
AR651W	AR V300R019C10	N/A
AR657	V300R019C10	N/A
R1600	N/A	V200R007, V100R001
R2500	N/A	V100R001
R2600	N/A	V200R007
SRG1320V SRG1320VW SRG2320 SRG3340 SRG3360	N/A	V2R3C00, V2R2C02
SRG1340-9G	V300R019C10	N/A
SRG2320D SRG2304 SRG1320 SRG1320W SRG1320V SRG1320VW SRG2320 SRG3340 SRG3360	N/A	V2R5C10, V2R5C00
SRG2320EI SRG1320E SRG2340E	N/A	V2R8C30/V2R8C50

NE	New Version	Compatible Version
SRG2320E SRG2320D SRG2304 SRG1320 SRG1320W SRG1320V SRG1320VW SRG2320 SRG3340 SRG3360	N/A	V2R5C30, V2R5C20
SRG33X0	V300R019C10	N/A

## 10.7 RM9000 Series

The following table lists the RM9000 series NE supported.

**Table 10-17** RM9000 series

NE	New Version	Compatible Version
RM9000	N/A	V300R002C02

## 10.8 Switch Series

The following table lists the switch NEs supported.

**Table 10-18** S series

NE	New Version	Compatible Version
2403TP-PWR-EA	N/A	VRP Software, Version 3.10, Release 2107P07 VRP Lanswitch Platform Software Version COMWAREV300R002B16 D019SP21 Quidway S2403TP-PWR-EA Software Version V200R001B60D010SP06

NE	New Version	Compatible Version
5628C-HI-AC	N/A	VRP Software, Version 5.20, Release 2102P01 VRP Platform Software Version COMWAREV500R002B38 D009 Quidway S5628C- HI-AC Software Version V200R001B02D015SP02
E628 E628-X	N/A	V2R9C00, V2R8C00
E652 E652-X	N/A	V2R9C00, V2R8C00
Quidway S12700	N/A	V200R0011C10, V200R0011C00
Quidway S2300	N/A	V200R0013C00, V200R0012C00
Quidway S2700	N/A	V200R0013C00, V200R0012C00
Quidway S5300	N/A	V200R0012C00
Quidway S5700	N/A	V200R0012C00
Quidway S6300	N/A	V200R0013C00, V200R0012C00
Quidway S6700	N/A	V200R0013C00, V200R0012C00
Quidway S7700	N/A	V200R0013C00, V200R0011C10, V200R0011C00
Quidway S9300/S9300E	N/A	V200R0013C00, V200R0012C00, V200R0011C10, V200R0011C00
Quidway S9700	N/A	V200R0013C00, V200R0011C10, V200R0011C10, V200R0011C00

NE	New Version	Compatible Version
S12700E-12	N/A	V200R019C00SPC210
S12700E-4	N/A	V200R019C00SPC210
S12700E-8	N/A	V200R019C00SPC210
S12704	N/A	V2R10C00
S12708 S12712	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R10C00
S12710	N/A	V2R10C00
S1730S-S24P4S-A	N/A	V200R019C00SPC210
S1730S-S24T4S-A	N/A	V200R019C00SPC210
S1730S-S48T4S-A	N/A	V200R019C00SPC210
S2016TP-EA	N/A	Version 3.10, Release 2107P07
S2016TP-MI	N/A	VRP310-R2107P01, VRP Software, Version 3.10, Release 2107P03V200R001B60D0 10SP01 (COMWAREV300R002B1 6D019SP19)



NE	New Version	Compatible Version
S2016TP-PWR-EA	N/A	Version 3.10, Release 2107P07 Bootrom Version is 518 VRP Lanswitch Platform Software Version COMWAREV300R002B16 D019SP21 Quidway S2016TP-PWR-EA Software Version V200R001B60D010SP06 Quidway S2016TP-PWR- EA Product Version S2016TP-PWR- EA-2107P07 Web Network Manager Version WNMV300R001B08D040
S2309TP-EI S2318TP-EI S2326TP-EI S2352P-EI S2309TP-PWR-EI S2326TP-PWR-EI	N/A	V1R5
S2309TP-SI S2309TP-EI S2318TP-SI S2318TP-EI S2326TP-SI S2326TP-EI S2352P-EI	N/A	V1R2
S2309TP-SI S2309TP-EI S2318TP-SI S2318TP-EI S2326TP-SI S2326TP-EI S2352P-EI S2309TP- PWR-EI S2326TP-PWR-EI	N/A	V1R6C03, V1R6, V1R3
S2309TP-SI S2309TP-EI S2318TP-SI S2318TP-EI S2326TP-SI S2326TP-EI S2352P-EI S2309TP- PWR-EI S2326TP-PWR-EI S2328P-EI-AC	N/A	V1R6C05
S2309TP-SI S2318TP-SI S2326TP-SI	N/A	V1R5

NE	New Version	Compatible Version
S2320-12TP-EI-AC S2320-12TP-EI-DC S2320-12TP-PWR-EI-AC S2320-52TP-EI-AC S2320-52TP-PWR-EI-AC S2320-28TP-EI-AC S2320-28TP-EI-DC S2320-28TP-PWR-EI-AC S2320-28P-PWR-EI-ACF	N/A	V2R12C00
S2320-12TP-EI-AC S2350-28TP-EI-DC S2320-12TP-EI-DC S2320-12TP-PWR-EI-AC S2320-28P-PWR-EI-ACF S2320-52TP-EI-AC S2320-52TP-PWR-EI-AC S2320-28TP-PWR-EI-AC S2320-28TP-EI-AC S2320-28TP-EI-DC	N/A	V2R11C10
S2350-28TP-EI-AC S2350-28TP-PWR-EI-AC S2350-20TP-PWR-EI-AC	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3C00, V2R11C10, V2R11C00, V2R10C00
S2350-28TP-EI-DC	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R11C00, V2R10C00

NE	New Version	Compatible Version
S2403H-EI	N/A	VRP (R) Software, Version 3.10, RELEASE 0018 VRP (tm) Lanswitch Platform Software Version V100R003B23D002SP08 Quidway S2403H-EI Software Version V300R001B01D020 Bootrom Version is 150
S2700-18TP-EI-AC S2700-18TP-SI-AC S2700-26TP-EI-AC S2700-26TP-PWR-EI S2700-26TP-SI-AC S2700-52P-EI-AC S2700-9TP-EI -AC S2700-9TP-PWR-EI S2700-9TP-SI-AC S2700-26TP-EI-DC S2700-9TP-EI -DC	N/A	V1R5
S2700-18TP-EI-AC S2700-18TP-SI-AC S2700-26TP-EI-AC S2700-26TP-PWR-EI S2700-26TP-SI-AC S2700-52P-EI-AC S2700-9TP-EI -AC S2700-9TP-PWR-EI S2700-9TP-SI-AC S2700-26TP-EI-DC S2700-9TP-EI -DC S2710-52P-SI-AC S2710-52P-PWR-SI S2700-52P-PWR-EI	N/A	V1R6
S2720-12TP-EI-AC S2720-12TP-PWR-EI-AC S2720-52TP-EI-AC S2720-52TP-PWR-EI-AC S2720-28TP-PWR-EI-ACL S2720-28TP-PWR-EI-AC S2720-28TP-EI-V2-AC S2751-28TP-PWR-EI-AC S2750-28TP-EI-AC S2750-28TP-PWR-EI-AC S2750-20TP-PWR-EI-AC	N/A	V2R12C00, V2R11C10

NE	New Version	Compatible Version
S2751-28TP-PWR-EI-AC S2750-28TP-EI-AC S2750-28TP-PWR-EI-AC S2750-20TP-PWR-EI-AC	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R11C00, V2R10C00
S2751-28TP-PWR-EI-AC S2750-28TP-EI-AC S2750-28TP-PWR-EI-AC S2750-20TP-PWR-EI-AC	N/A	V2R3
S3000	N/A	VRP3.10 R0040[02]
S3026S-SI	N/A	VRP (R) Software, Version 3.10, RELEASE 0020 (VRP Version V100R003B23D002SP02 )S3026S-SI Software Version V100R001B02D005SP02S 3026S-SI Product Version S3026S-SI-0020
S3050C	N/A	Version 3.10, Release 0033
S3318TP-EI-MC S3328TP-EI S3328TP- EI-24S S3328TP-EI-MC S3328TP-PWR-EI S3328TP-SI S3352P-EI S3352P-EI-24S S3352P- EI-48S S3352P-PWR-EI S3352P-SI S3352P-SI-48S	N/A	V1R6C03
S3318TP-EI-MC S3328TP-EI S3328TP- EI-24S S3328TP-EI-MC S3328TP-PWR-EI S3328TP-SI S3352P-EI S3352P-EI-24S S3352P- EI-48S S3352P-PWR-EI S3352P-SI S3352P-SI-48S S3300-52P-EI	N/A	V1R6C05

NE	New Version	Compatible Version
S3318TP-EI-MC S3328TP-EI(-24S)(-MC) S3328TP-PWR-EI S3328TP-SI S3352P- EI(-24S)(-48S) S3352P- PWR-EI S3352P-SI(-48S)	N/A	V1R5
S3318TP-EI-MC S3328TP-EI(-24S)(-MC) S3328TP-PWR-EI S3328TP-SI S3352P- EI(-24S)(-48S) S3352P- PWR-EI S3352P-SI(-48S) S3326C-HI	N/A	V1R6
S3328TP-SI S3328TP- EI(-24S) S3352P-SI S3352P-EI(-24S)(-48S)	N/A	V1R2
S3328TP-SI S3328TP- EI(-24S) S3352P-SI S3352P-EI(-24S)(-48S) S3328TP-PWR-EI S3352P-PWR-EI	N/A	V1R3
S3528F-EA	N/A	VRP Software, Version 5.20, Release 5303
S3528G	N/A	Version 3.10
S3528P	N/A	Version 3.10, Release 0025P03 Version 3.10, Feature 1532L01
S3528P-EA	N/A	VRP Software, Version 5.20, Release 5303
S3552F-EA	N/A	VRP3.1
S3552F-HI	N/A	S3552-VRP310-R0030

NE	New Version	Compatible Version
S3552P-EA	N/A	VRP Software, Version 5.20, Release 5303 VRP Platform Software Version COMWAREV500R002B36 D009 S3552P-EA Software Version V500R003B04D008SP02 Bootrom Version is 142
S3700-26C-HI	N/A	V2R3, V2R2, V2R1
S3700-28TP-EI-24S-AC S3700-28TP-EI-AC S3700-28TP-EI-MC-AC S3700-28TP-PWR-EI S3700-28TP-SI-AC S3700-52P-EI-24S-AC S3700-52P-EI-48S-AC S3700-52P-EI-AC S3700-52P-PWR-EI S3700-52P-SI-AC S3700-28TP-EI-DC S3700-28TP-SI-DC S3700-52P-EI-24S-DC S3700-52P-EI-48S-DC S3700-52P-EI-DC	N/A	V1R5
S3700-28TP-EI-24S-AC S3700-28TP-EI-AC S3700-28TP-EI-MC-AC S3700-28TP-PWR-EI S3700-28TP-SI-AC S3700-52P-EI-24S-AC S3700-52P-EI-48S-AC S3700-52P-EI-AC S3700-52P-PWR-EI S3700-52P-SI-AC S3700-28TP-EI-DC S3700-28TP-SI-DC S3700-52P-EI-24S-DC S3700-52P-EI-48S-DC S3700-52P-EI-DC S3700-26C-HI S3700-52P-PWR-SI S3700-28TP-PWR-SI	N/A	V1R6

NE	New Version	Compatible Version
S3900	N/A	VRP3.10 R1602[01]
S3928P-EI	N/A	Version 3.10, Release 1602P11, Version 3.10, Release 1602P10, S3900EI-VRP310- R1602P06
S3928P-SI	N/A	Version 3.10, Release 1602P10
S3952P	N/A	S3900EI-VRP310— R1602P06
S3952P-EI	N/A	VRP Version COMWAREV300R002B16 D019SP21 Software Version V100R002B60D052SP01- EI
S3952P-PWR-EI	N/A	Version 3.10, Release 1602P10
S3952P-SI	N/A	Version 3.10, Release 1602P10
S5124P-EI	N/A	Version 3.10, Release 2201 VRP3.10 R2200
S5148P-EI	N/A	Version 3.10, Release 2201
S5300-28P-LI-BAT S5300-28P-LI-4AH S5300-28P-LI-24S-BAT S5300-28P-LI-24S-4AH S5300-52X-LI-48CS-AC S5300-52X-LI-48CS-DC	N/A	V2R3C02
S5300-28P-LI-BAT S5300-28P-LI-4AH S5300-28P-LI-24S-BAT S5300-28P-LI-24S-4AH S5300-52X-LI-48CS-AC S5300-52X-LI-48CS-DC S5300-52X-LI-AC S5300-52X-LI-DC	N/A	V2R6C00, V2R5C00

NE	New Version	Compatible Version
S5300-28P-LI-BAT S5300-28P-LI-4AH S5300-28P-LI-24S-BAT S5300-28P-LI-24S-4AH S5300-52X-LI-48CS-AC S5300-52X-LI-48CS-DC S5300-52X-LI-AC S5300-52X-LI-DC S5320-36C-EI-28S-AC S5320-36C-EI-28S-DC S5320-56C-EI-48S-AC S5320-56C-EI-48S-DC S5320-36C-EI-AC S5320-36C-EI-DC S5320-36PC-EI-AC S5320-36PC-EI-DC S5320-56C-EI-AC S5320-56C-EI-DC S5320-56PC-EI-AC S5320-56PC-EI-DC S5320-36C-PWR-EI-AC S5320-36C-PWR-EI-DC S5320-56C-PWR-EI-AC S5320-32X-EI-24S-AC S5320-32X-EI-24S-DC S5320-50X-EI-46S-AC S5320-50X-EI-46S-DC S5320-32X-EI-AC S5320-32X-EI-DC S5320-32P-EI-AC S5320-32P-EI-DC S5320-52X-EI-AC S5320-52X-EI-DC S5320-52P-EI-AC S5320-52P-EI-DC S5320-50X-EI-AC S5320-50X-EI-DC	N/A	V2R9C00, V2R8C00, V2R7C00



NE	New Version	Compatible Version
S5300-28TP-PWR-LI-AC S5300-10P-PWR-LI-AC S5320-28X-SI-DC S5320-52X-SI-DC S5320-52X-PWR-SI-ACF S5321-28X-SI-AC S5321-28X-SI-DC S5321-52P-SI-AC S5321-52X-SI-AC S5321-52X-SI-DC S5320-28P-SI-AC S5320-28X-SI-AC S5320-52P-SI-AC S5320-52X-SI-AC S5320-28X-PWR-SI-AC S5320-52X-PWR-SI-AC	N/A	V2R9C00
S5300-28TP-PWR-LI-AC S5300-10P-PWR-LI-AC S5320-52X-PWR-SI-ACF	N/A	V2R8C10
S5320-56C-HI-AC S5320-56C-HI-DC S5320-32C-HI-24S-DC S5320-32C-HI-24S-AC S5328-HI S5328-HI-24S S5328C-EI S5328C-EI-24S S5328C-PWR-EI S5352C- PWR-EI S5328C-SI S5352C-SI S5324TP-SI- AC S5324TP-SI-DC S5348TP-SI-AC S5348TP- SI-DC S5324TP-PWR-SI S5348TP-PWR-SI S5328C-PWR-SI S5352C- PWR-SI S5306TP-LI-AC S5300-28P-LI-AC S5300-28P-LI-DC S5300-52P-LI-AC S5300-52P-LI-DC S5300-10P-LI-AC S5310-28C-EI S5310-52C-EI S5300-28X-LI-DC S5300-28X-LI-AC S5300-28X-LI-24S-DC S5300-28X-LI-24S-AC	N/A	V2R9C00

NE	New Version	Compatible Version
S5320-56C-HI-AC S5320-56C-HI-DC S5320-32C-HI-24S-DC S5320-32C-HI-24S-AC S5328-HI S5328-HI-24S S5328C-EI S5328C-EI-24S S5328C-PWR-EI S5352C-PWR-EI S5328C-SI S5352C-SI S5324TP-SI-AC S5324TP-SI-DC S5348TP-SI-AC S5348TP-SI-DC S5324TP-PWR-SI S5348TP-PWR-SI S5328C-PWR-SI S5352C-PWR-SI S5306TP-LI-AC S5300-28P-LI-AC S5300-28P-LI-DC S5300-52P-LI-AC S5300-52P-LI-DC S5300-10P-LI-AC S5310-28C-EI S5310-52C-EI S5300-28X-LI-DC S5300-28X-LI-AC S5300-28X-LI-24S-DC S5300-28X-LI-24S-AC S5300-28P-LI-BAT S5300-28P-LI-4AH S5300-28P-LI-24S-BAT S5300-28P-LI-24S-4AH S5300-52X-LI-48CS-AC S5300-52X-LI-48CS-DC S5300-52X-LI-AC S5300-52X-LI-DC S5320-36C-EI-28S-AC S5320-36C-EI-28S-DC S5320-56C-EI-48S-AC S5320-56C-EI-48S-DC S5320-36C-EI-AC S5320-36C-EI-DC S5320-36PC-EI-AC S5320-36PC-EI-DC S5320-56C-EI-AC S5320-56C-EI-DC S5320-56PC-EI-AC S5320-56PC-EI-DC S5320-36C-PWR-EI-AC S5320-36C-PWR-EI-DC S5320-56C-PWR-EI-AC S5320-32X-EI-24S-AC	N/A	V2R12C00, V2R11C10, V2R11C00, V2R10C00

NE	New Version	Compatible Version
S5320-32X-EI-24S-DC S5320-50X-EI-46S-AC S5320-50X-EI-46S-DC S5320-32X-EI-AC S5320-32X-EI-DC S5320-32P-EI-AC S5320-32P-EI-DC S5320-52X-EI-AC S5320-52X-EI-DC S5320-52P-EI-AC S5320-52P-EI-DC S5320-50X-EI-AC S5320-50X-EI-DC S5300-28TP-PWR-LI-AC S5300-10P-PWR-LI-AC S5320-28X-SI-DC S5320-52X-SI-DC S5320-52X-PWR-SI-ACF S5321-28X-SI-AC S5321-28X-SI-DC S5321-52P-SI-AC S5321-52X-SI-AC S5321-52X-SI-DC S5320-28P-SI-AC S5320-28X-SI-AC S5320-52P-SI-AC S5320-52X-SI-AC S5320-28X-PWR-SI-AC S5320-52X-PWR-SI-AC S5320-12TP-LI-AC S5320-12TP-PWR-LI-AC S5320-28P-LI-AC S5320-28X-LI-AC S5320-28X-LI-DC S5320-28P-PWR-LI-AC S5320-28X-PWR-LI-AC S5320-52P-LI-AC S5320-52X-LI-AC S5320-52X-LI-DC S5320-52P-PWR-LI-AC S5320-52X-PWR-LI-AC S5321-28X-SI-24S-AC S5321-28X-SI-24S-DC S5320-28X-LI-24S-AC S5320-28X-LI-24S-DC S5321-28X-SI-24S-AC S5321-28X-SI-24S-DC S5320-28X-LI-24S-AC S5320-28X-LI-24S-DC S5320-28X-PWR-SI-DC		

NE	New Version	Compatible Version
S5320-52X-PWR-SI-DC S5320-28P-SI-DC S5320-52P-SI-DC S5320-12TP-LI-DC S5320-28X-PWR-SI S5320-52X-PWR-SI S5320-28P-SI S628X-E S628X-PWR-E S652-E S652X-E S652-PWR-E S652X-PWR-E S628- PWR-E S628-E		
S5320-56C-PWR-EI-ACF	N/A	V2R11C00, V2R10C00
S5320-56C-PWR-EI-ACF S5320-12X-PWR-LI-AC S5320-28TP-LI-AC S5320-12P-LI-BAT S5320-28X-SI-24S-AC S5320-28X-SI-24S-DC S5330-68C-SI-AC S5330-68C-SI	N/A	V2R11C10
S5320-56C-PWR-EI-ACF S5320-12X-PWR-LI-AC S5320-28TP-LI-AC S5320-12P-LI-BAT S5320-28X-SI-24S-AC S5320-28X-SI-24S-DC S5330-68C-SI-AC S5330-68C-SI S5320-28X-SI-24S-AC S5320-28X-SI-24S-DC S5330-48C-SI-AC S5330-56C-PWH-SI-AC S5330-56C-PWH-SI	N/A	V2R12C00
S5321-28X-SI-AC S5321-28X-SI-DC S5321-52P-SI-AC S5321-52X-SI-AC S5321-52X-SI-DC S5320-28P-SI-AC S5320-28X-SI-AC S5320-52P-SI-AC S5320-52X-SI-AC S5320-28X-PWR-SI-AC S5320-52X-PWR-SI-AC	N/A	V2R8C00

NE	New Version	Compatible Version
S5324TP-SI S5328C-SI S5328C-EI(-24S) S5348TP-SI S5352C-SI S5352C-EI S5324TP- PWR-SI S5328C-PWR-SI S5328C-PWR-EI S5348TP-PWR-SI S5352C-PWR-SI S5352C- PWR-EI	N/A	V1R5, V1R3
S5324TP-SI S5328C-SI S5328C-EI(-24S) S5348TP-SI S5352C-SI S5352C-EI S5324TP- PWR-SI S5328C-PWR-SI S5328C-PWR-EI S5348TP-PWR-SI S5352C-PWR-SI S5352C- PWR-EI S5328C-HI S5328C-HI-24S S5306TP- LI	N/A	V1R6
S5328-HI S5328-HI-24S S5328C-EI S5328C-EI-24S S5328C-PWR-EI S5352C- PWR-EI S5328C-SI S5352C-SI S5324TP-SI- AC S5324TP-SI-DC S5348TP-SI-AC S5348TP- SI-DC S5324TP-PWR-SI S5348TP-PWR-SI S5328C-PWR-SI S5352C- PWR-SI S5306TP-LI-AC S3326C-HI S5300-28P-LI- AC S5300-28P-LI-DC S5300-52P-LI-AC S5300-52P-LI-DC	N/A	V2R1

NE	New Version	Compatible Version
S5328-HI S5328-HI-24S S5328C-EI S5328C-EI-24S S5328C-PWR-EI S5352C- PWR-EI S5328C-SI S5352C-SI S5324TP-SI- AC S5324TP-SI-DC S5348TP-SI-AC S5348TP- SI-DC S5324TP-PWR-SI S5348TP-PWR-SI S5328C-PWR-SI S5352C- PWR-SI S5306TP-LI-AC S5300-28P-LI-AC S5300-28P-LI-DC S5300-52P-LI-AC S5300-52P-LI-DC S5300-10P-LI-AC S5310-28C-EI S5310-52C-EI	N/A	V2R2
S5328-HI S5328-HI-24S S5328C-EI S5328C-EI-24S S5328C-PWR-EI S5352C- PWR-EI S5328C-SI S5352C-SI S5324TP-SI- AC S5324TP-SI-DC S5348TP-SI-AC S5348TP- SI-DC S5324TP-PWR-SI S5348TP-PWR-SI S5328C-PWR-SI S5352C- PWR-SI S5306TP-LI-AC S5300-28P-LI-AC S5300-28P-LI-DC S5300-52P-LI-AC S5300-52P-LI-DC S5300-10P-LI-AC S5310-28C-EI S5310-52C-EI S5300-28X-LI-DC S5300-28X-LI-AC S5300-28X-LI-24S-DC S5300-28X-LI-24S-AC	N/A	V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3
S5328C-EI(-24) S5352C- EI	N/A	V1R2
S5330-60C-HI-48S S5330-36C-HI-24S S5320-52X-LI-48S-AC S5320-52X-LI-48S-DC S5320-52X-SI-48S	N/A	V2R13C00
S5331-H24P4XC	N/A	V200R019C00SPC210

NE	New Version	Compatible Version
S5331-H24T4XC	N/A	V200R019C00SPC210
S5331-H48P4XC	N/A	V200R019C00SPC210
S5331-H48T4XC	N/A	V200R019C00SPC210
S5332-H24S6Q	N/A	V200R019C00SPC210
S5332-H48S6Q	N/A	V200R019C00SPC210
S5335-L12P4S-A	N/A	V200R019C00SPC210
S5335-L12T4S-A	N/A	V200R019C00SPC210
S5335-L24P4X-A	N/A	V200R019C00SPC210
S5335-L24T4X-A	N/A	V200R019C00SPC210
S5335-L32ST4X-A	N/A	V200R019C00SPC210
S5335-L48T4X-A	N/A	V200R019C10
S5335-S24P4X	N/A	V200R019C00SPC210
S5335-S24T4X	N/A	V200R019C00SPC210
S5335-S32ST4X	N/A	V200R019C00SPC210
S5335-S48P4X	N/A	V200R019C00SPC210
S5335-S48S4X	N/A	V200R019C00SPC210
S5335-S48T4X	N/A	V200R019C00SPC210
S5352C-EI	N/A	V200R001C00
S5624F	N/A	Versio 3.10, Release 1602P10 3.10, Feature 1532L01, VRP310-R1602P06
S5624P	N/A	Version 3.10, Release 1602P10 VRP V3.10 R1510P15 3.10 Feature 1532L01
S5624P-PWR	N/A	VRP Software, Version 3.10, Release 1602P10 S5624P-PWR Software Version V100R002B60D052SP01 VRP Version COMWAREV300R002B16 D019SP21

NE	New Version	Compatible Version
S5648P	N/A	Version 3.10, Release 1602P10
S5700-24TP-PWR-SI S5700-24TP-SI-AC S5700-28C-EI S5700-28C-EI-24S S5700-28C-PWR-EI S5700-28C-SI S5700-48TP-PWR-SI S5700-48TP-SI-AC S5700-52C-EI S5700-52C-PWR-EI S5700-52C-SI S5700-24TP-SI-DC S5700-48TP-SI-DC	N/A	V1R6, V1R5
S5700-24TP-PWR-SI S5700-24TP-SI-AC S5700-28C-EI S5700-28C-EI-24S S5700-28C-PWR-EI S5700-28C-SI S5700-48TP-PWR-SI S5700-48TP-SI-AC S5700-52C-EI S5700-52C-PWR-EI S5700-52C-SI S5700-24TP-SI-DC S5700-48TP-SI-DC S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-28C-EI S5710-52C-EI S5700-28C-HI S5700-28C-HI-24S S5700-6TP-LI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI	N/A	V2R1



NE	New Version	Compatible Version
S5700-28C-EI S5700-28C-EI-24S S5700-52C-EI S5700-28C-PWR-EI S5700-52C-PWR-EI S5700-28C-SI S5700-52C-SI S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-HI S5700-28C-HI-24S S5710-28C-EI S5710-52C-EI S5700-6TP-LI-AC S5700-28P-LI S5700-52P- LI S5700-28P-PWR-LI S5700-52P-PWR-LI S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-108C-PWR-HI S5700-10P-LI-AC S5700-10P-PWR-LI-AC S5700-26X-SI-12S-AC S5710-28C-PWR-EI S5710-52C-PWR-EI S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5710-108C-HI-AC S5710-108C-PWR-HI-AC S5710-28C-PWR-EI-AC S5710-52C-PWR-EI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI	N/A	V2R2

NE	New Version	Compatible Version
S5700-28C-EI S5700-28C-EI-24S S5700-52C-EI S5700-28C-PWR-EI S5700-52C-PWR-EI S5700-28C-SI S5700-52C-SI S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-HI S5700-28C-HI-24S S5710-28C-EI S5710-52C-EI S5700-6TP-LI-AC S5700-28P-LI S5700-52P- LI S5700-28P-PWR-LI S5700-52P-PWR-LI S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-108C-PWR-HI S5700-10P-LI-AC S5700-10P-PWR-LI-AC S5700-26X-SI-12S-AC S5710-28C-PWR-EI S5710-52C-PWR-EI S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5710-108C-HI-AC S5710-108C-PWR-HI-AC S5710-28C-PWR-EI-AC S5710-52C-PWR-EI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC	N/A	V2R3

NE	New Version	Compatible Version
S5700-28C-EI S5700-28C-EI-24S S5700-52C-EI S5700-28C-PWR-EI S5700-52C-PWR-EI S5700-28C-SI S5700-52C-SI S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-HI S5700-28C-HI-24S S5710-28C-EI S5710-52C-EI S5700-6TP-LI-AC S5700-28P-LI S5700-52P- LI S5700-28P-PWR-LI S5700-52P-PWR-LI S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-108C-PWR-HI S5700-10P-LI-AC S5700-10P-PWR-LI-AC S5700-26X-SI-12S-AC S5710-28C-PWR-EI S5710-52C-PWR-EI S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5710-108C-HI-AC S5710-108C-PWR-HI-AC S5710-28C-PWR-EI-AC S5710-52C-PWR-EI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT	N/A	V2R5C00

NE	New Version	Compatible Version
S5700-28P-LI-24S-4AH S5700-28X-LI-24CS-AC S5700-28X-LI-24CS-DC		
S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-28X-LI-24CS-AC S5700-28X-LI-24CS-DC	N/A	V2R3C02

NE	New Version	Compatible Version
S5700-28TP-LI-AC S5700-28TP-PWR-LI-AC S5701-28TP-PWR-LI-AC S5720-36C-EI-28S-AC S5720-56C-EI-48S-AC S5720-36C-EI-AC S5720-36PC-EI-AC S5720-56C-EI-AC S5720-56PC-EI-AC S5720-36C-PWR-EI-AC S5720-56C-PWR-EI-AC S5720-56C-PWR-EI-AC1 S5720-32X-EI-24S-AC S5720-50X-EI-46S-AC S5720-32X-EI-AC S5720-32P-EI-AC S5720-52X-EI-AC S5720-52P-EI-AC S5720-50X-EI-AC S5720-56C-HI-AC S5720-56C-PWR-HI-AC S5720-32C-HI-24S-AC S5700-28C-EI S5700-28C-EI-24S S5700-52C-EI S5700-28C-PWR-EI S5700-52C-PWR-EI S5700-28C-SI S5700-52C-SI S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-HI S5700-28C-HI-24S S5710-28C-EI S5710-52C-EI S5700-6TP-LI-AC S5700-28P-LI S5700-52P- LI S5700-28P-PWR-LI S5700-52P-PWR-LI S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-108C-PWR-HI S5700-10P-LI-AC S5700-10P-PWR-LI-AC S5700-26X-SI-12S-AC S5710-28C-PWR-EI	N/A	V2R7C00

NE	New Version	Compatible Version
S5710-52C-PWR-EI S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5710-108C-HI-AC S5710-108C-PWR-HI-AC S5710-28C-PWR-EI-AC S5710-52C-PWR-EI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-28X-LI-24CS-AC S5700-28X-LI-24CS-DC		

NE	New Version	Compatible Version
S5720-12X-LI- ACS5720-12X-PWR-LI- ACS5720-30C-LI- ACS5720-54C-LI- ACS5720-30C-PWR-LI- ACS5720-54C-PWR-LI- ACS5720-28X-PWR-LI- ACFS5720-52X-PWR-LI- ACFS5720-28X-SI-12S- ACS5721-28X-SI-24S- ACS5730-36C-HI S5730-44C-HI S5730-36C-PWH-HI S5730-44C-PWH-HI S5730-60C-HI S5730-68C-HI S5730-60C-PWH-HI S5730-68C-PWH- HIS5720I-12X-SI- ACS5720I-12X-PWH-SI- DCS5720I-28X-SI- ACS5720I-28X-PWH-SI- ACS5730-36C- HIS5730-44C- HIS5730-36C-PWH- HIS5730-44C-PWH- HIS5730-60C- HIS5730-68C- HIS5730-60C-PWH- HIS5730-68C-PWH- HIS5730-56C-PWH-SI- ACS5730-56C-PWH-SI	N/A	V2R12C00

NE	New Version	Compatible Version
S5720-14X-PWH-SI-AC S5720-28X-PWR-SI-DC S5720-52X-PWR-SI-DC S5720-28X-SI-DC S5720-52X-SI-DC S5720S-28X-SI-DC S5720S-52X-SI-DC S5720S-28P-SI-AC S5720S-28X-SI-AC S5720S-52P-SI-AC S5720S-52X-SI-AC S5720-28P-SI-AC S5720-28X-SI-AC S5720-52P-SI-AC S5720-28X-PWH-LI-AC S5720-52X-SI-AC S5720-28X-PWR-SI-AC S5720-52X-PWR-SI-AC S5720-52X-PWR-SI-ACF S5710-28X-LI-AC S5710-52X-LI-AC S5700S-28X-LI-AC S5700S-52X-LI-AC S5700S-28P-PWR-LI-AC S5700-10P-LI-AC S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-10P-PWR-LI-AC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC S5700-28X-LI-AC S5700-28X-LI-DC S5701-28X-LI-AC S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5701-28X-LI-24S-AC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-52X-LI-48CS-AC S5700-28TP-LI-AC S5700-28TP-PWR-LI-AC S5701-28TP-PWR-LI-AC	N/A	V2R11C00



NE	New Version	Compatible Version
S5700S-28P-LI-AC S5700S-52P-LI-AC		

NE	New Version	Compatible Version
S5720-14X-PWH-SI-AC S5720-28X-PWR-SI-DC S5720-52X-PWR-SI-DC S5720-28X-SI-DC S5720-52X-SI-DC S5720S-28X-SI-DC S5720S-52X-SI-DC S5720S-28P-SI-AC S5720S-28X-SI-AC S5720S-52P-SI-AC S5720S-52X-SI-AC S5720-28P-SI-AC S5720-28X-SI-AC S5720-52P-SI-AC S5720-52X-SI-AC S5720-28X-PWR-SI-AC S5720-52X-PWR-SI-AC S5720-52X-PWR-SI-ACF S5710-28X-LI-AC S5710-52X-LI-AC S5700S-28X-LI-AC S5700S-52X-LI-AC S5700S-28P-PWR-LI-AC S5700-10P-LI-AC S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-10P-PWR-LI-AC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC S5700-28X-LI-AC S5700-28X-LI-DC S5701-28X-LI-AC S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5701-28X-LI-24S-AC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-52X-LI-48CS-AC S5700-28TP-LI-AC S5700-28TP-PWR-LI-AC S5701-28TP-PWR-LI-AC	N/A	V2R9C00, V2R12C00, V2R11C10

NE	New Version	Compatible Version
S5700S-28P-LI-AC S5700S-52P-LI-AC		

NE	New Version	Compatible Version
S5720-14X-PWH-SI-AC S5720-28X-PWR-SI-DC S5720-52X-PWR-SI-DC S5720-28X-SI-DC S5720-52X-SI-DC S5720S-28X-SI-DC S5720S-52X-SI-DC S5720S-28P-SI-AC S5720S-28X-SI-AC S5720S-52P-SI-AC S5720S-52X-SI-AC S5720-28P-SI-AC S5720-28X-SI-AC S5720-52P-SI-AC S5720-52X-SI-AC S5720-28X-PWR-SI-AC S5720-52X-PWR-SI-AC S5720-52X-PWR-SI-ACF S5710-28X-LI-AC S5710-52X-LI-AC S5700S-28X-LI-AC S5700S-52X-LI-AC S5700S-28P-PWR-LI-AC S5700-10P-LI-AC S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-10P-PWR-LI-AC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC S5700-28X-LI-AC S5700-28X-LI-DC S5701-28X-LI-AC S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5701-28X-LI-24S-AC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-52X-LI-48CS-AC S5700-28TP-LI-AC S5700-28TP-PWR-LI-AC S5701-28TP-PWR-LI-AC S5700S-28P-LI-AC	N/A	V2R10C00

NE	New Version	Compatible Version
S5700S-52P-LI-AC Huawei-S5700-8P-G S5720-12TP-LI-AC S5720S-12TP-LI-AC S5720-12TP-PWR-LI-AC S5720S-12TP-PWR-LI-AC S5720-28P-LI-AC S5720S-28P-LI-AC S5720-28X-LI-AC S5720-28X-LI-DC S5720S-28X-LI-AC S5720-28P-PWR-LI-AC S5720-28X-PWR-LI-AC S5720S-28X-PWR-LI-AC S5720-52P-LI-AC S5720S-52P-LI-AC S5720S-52X-LI-AC S5720-52X-LI-AC S5720-52X-LI-DC S5720-52P-PWR-LI-AC S5720S-52P-PWR-LI-AC S5720S-52X-PWR-LI-AC S5720-52X-PWR-LI-AC S5720-28X-SI-24S-AC S5720-28X-SI-24S-DC S5720-28X-LI-24S-AC S5720S-28X-LI-24S-AC S5720-28X-LI-24S-DC S5720-28TP-PWR-LI-ACL S5720S-28TP-PWR-LI-ACL S5720-28TP-PWR-LI-AC S5720-28X-SI-24S-AC S5720-28X-SI-24S-DC S5720-28X-LI-24S-AC S5720S-28X-LI-24S-AC S5720-28X-LI-24S-DC S5720-28TP-PWR-LI-ACL S5720S-28TP-PWR-LI-ACL S5720-28TP-PWR-LI-AC S5720-28TP-LI-AC S5720-16X-PWH-LI-AC		

NE	New Version	Compatible Version
S5720-32X-EI-DC S5720-50X-EI-DC S5720-32X-EI-24S-DC S5720-50X-EI-46S-DC S5720-36C-EI-DC S5720-56C-EI-DC S5720-36C-PWR-EI-DC S5720-56C-PWR-EI-DC S5720-36C-EI-28S-DC S5720-56C-EI-48S-DC S5720-56C-PWR-HI-AC1 S5720-28X-PWH-LI-AC S5720-56C-HI-AC S5720-56C-PWR-HI-AC S5720-32C-HI-24S-AC S5720-36C-EI-28S-AC S5720-56C-EI-48S-AC S5720-36C-EI-AC S5720-36PC-EI-AC S5720-56C-EI-AC S5720-56PC-EI-AC S5720-36C-PWR-EI-AC S5720-56C-PWR-EI-AC S5720-56C-PWR-EI-AC1 S5720-32X-EI-24S-AC S5720-50X-EI-46S-AC S5720-32X-EI-AC S5720-32P-EI-AC S5720-52X-EI-AC S5720-52P-EI-AC S5720-50X-EI-AC	N/A	V2R12C00, V2R11C10

NE	New Version	Compatible Version
S5720-32X-EI-DC S5720-50X-EI-DC S5720-32X-EI-24S-DC S5720-50X-EI-46S-DC S5720-36C-EI-DC S5720-56C-EI-DC S5720-36C-PWR-EI-DC S5720-56C-PWR-EI-DC S5720-36C-EI-28S-DC S5720-56C-EI-48S-DC S5720-56C-PWR-HI-AC1 S5720-56C-HI-AC S5720-56C-PWR-HI-AC S5720-32C-HI-24S-AC S5720-36C-EI-28S-AC S5720-56C-EI-48S-AC S5720-36C-EI-AC S5720-36PC-EI-AC S5720-56C-EI-AC S5720-56PC-EI-AC S5720-36C-PWR-EI-AC S5720-56C-PWR-EI-AC S5720-56C-PWR-EI-AC1 S5720-32X-EI-24S-AC S5720-50X-EI-46S-AC S5720-32X-EI-AC S5720-32P-EI-AC S5720-52X-EI-AC S5720-52P-EI-AC S5720-50X-EI-AC	N/A	V2R9C00, V2R11C00
S5720-36PC-EI-AC	N/A	V200R010C00
S5720-52X-PWR-LI-ACF S5721-28X-SI-24S-AC S5730-68C-PWR-SI-AC S5730-68C-PWR-SI S5730-48C-SI-AC S5730-48C-PWR-SI-AC S5730-68C-SI-AC	N/A	V2R11C10

NE	New Version	Compatible Version
S5720-56C-HI-AC S5720-56C-PWR-HI-AC S5720-32C-HI-24S-AC S5700-28C-EI S5700-28C-EI-24S S5700-52C-EI S5700-28C-PWR-EI S5700-52C-PWR-EI S5700-28C-SI S5700-52C-SI S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-HI S5700-28C-HI-24S S5710-28C-EI S5710-52C-EI S5700-6TP-LI-AC S5700-28P-LI S5700-52P- LI S5700-28P-PWR-LI S5700-52P-PWR-LI S5700S-28P-LI-AC S5700S-52P-LI-AC S5710-108C-PWR-HI S5700-10P-LI-AC S5700-10P-PWR-LI-AC S5700-26X-SI-12S-AC S5710-28C-PWR-EI S5710-52C-PWR-EI S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5710-108C-HI-AC S5710-108C-PWR-HI-AC S5710-28C-PWR-EI-AC S5710-52C-PWR-EI-AC S5700-28C-PWR-SI S5700-52C-PWR-SI S5710-28C-PWR-LI S5710-52C-PWR-LI S5710-28C-LI S5710-52C-LI S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC	N/A	V2R6C00



NE	New Version	Compatible Version
S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-28X-LI-24CS-AC S5700-28X-LI-24CS-DC		

NE	New Version	Compatible Version
S5720S-28P-SI-AC S5720S-28X-SI-AC S5720S-52P-SI-AC S5720S-52X-SI-AC S5720-28P-SI-AC S5720-28X-SI-AC S5720-52P-SI-AC S5720-52X-SI-AC S5720-28X-PWR-SI-AC S5720-52X-PWR-SI-AC S5720-52X-PWR-SI-ACF S5710-28X-LI-AC S5710-52X-LI-AC S5700S-28X-LI-AC S5700S-52X-LI-AC S5700S-28P-PWR-LI-AC S5720-56C-HI-AC S5720-56C-PWR-HI-AC S5720-32C-HI-24S-AC S5720-36C-EI-28S-AC S5720-56C-EI-48S-AC S5720-36C-EI-AC S5720-36PC-EI-AC S5720-56C-EI-AC S5720-56PC-EI-AC S5720-36C-PWR-EI-AC S5720-56C-PWR-EI-AC S5720-56C-PWR-EI-AC1 S5720-32X-EI-24S-AC S5720-50X-EI-46S-AC S5720-32X-EI-AC S5720-32P-EI-AC S5720-52X-EI-AC S5720-52P-EI-AC S5720-50X-EI-AC S5700-10P-LI-AC S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-10P-PWR-LI-AC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC S5700-28X-LI-AC S5700-28X-LI-DC S5701-28X-LI-AC S5700-28X-LI-24S-DC S5700-28X-LI-24S-AC S5701-28X-LI-24S-AC S5700-52X-LI-AC	N/A	V2R8C00

NE	New Version	Compatible Version
S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5700-28P-LI-BAT S5700-28P-LI-4AH S5700-28P-LI-24S-BAT S5700-28P-LI-24S-4AH S5700-52X-LI-48CS-AC S5700-28TP-LI-AC S5700-28TP-PWR-LI-AC S5701-28TP-PWR-LI-AC S5700S-28P-LI-AC S5700S-52P-LI-AC		
S5730-60C-HI-48S S5730-68C-HI-48S S5730-36C-HI-24S S5730-44C-HI-24S S5720-52X-SI-48S S5720-52X-LI-48S-AC	N/A	V2R13C00
S5731-H24P4XC	N/A	V200R019C00SPC210
S5731-H24P4XC-K	N/A	V200R019C10
S5731-H24T4XC	N/A	V200R019C00SPC210
S5731-H24T4XC-K	N/A	V200R019C10
S5731-H48P4XC	N/A	V200R019C00SPC210
S5731-H48P4XC-K	N/A	V200R019C10
S5731-H48T4XC	N/A	V200R019C00SPC210
S5731-S24P4X	N/A	V200R019C00SPC210
S5731-S24T4X	N/A	V200R019C00SPC210
S5731-S48P4X	N/A	V200R019C00SPC210
S5731-S48T4X	N/A	V200R019C00SPC210
S5731S-H24T4S-A	N/A	V200R019C00
S5731S-H24T4XC-A	N/A	V200R019C00SPC210
S5731S-H48T4S-A	N/A	V200R019C00
S5731S-H48T4XC-A	N/A	V200R019C00SPC210
S5731S-S24P4X-A	N/A	V200R019C00SPC210
S5731S-S24T4X-A	N/A	V200R019C00SPC210
S5731S-S48P4X-A	N/A	V200R019C00SPC210

NE	New Version	Compatible Version
S5731S-S48T4X-A	N/A	V200R019C00SPC210
S5732-H24S6Q	N/A	V200R019C00SPC210
S5732-H24S6Q-K	N/A	V200R019C10
S5732-H24UM2CC	N/A	V200R019C20
S5732-H48S6Q	N/A	V200R019C00SPC210
S5732-H48S6Q-K	N/A	V200R019C10
S5732-H48UM2CC	N/A	V200R019C20
S5735-L12P4S-A	N/A	V200R019C00SPC210
S5735-L12T4S-A	N/A	V200R019C00SPC210
S5735-L24P4S-A	N/A	V200R019C00SPC210
S5735-L24P4X-A	N/A	V200R019C00SPC210
S5735-L24T4S-A	N/A	V200R019C00SPC210
S5735-L24T4X-A	N/A	V200R019C00SPC210
S5735-L32ST4X-A	N/A	V200R019C00SPC210
S5735-L48P4X-A	N/A	V200R019C00SPC210
S5735-L48T4S-A	N/A	V200R019C00SPC210
S5735-L48T4X-A	N/A	V200R019C00SPC210
S5735-S24P4X	N/A	V200R019C00SPC210
S5735-S24T4X	N/A	V200R019C00SPC210
S5735-S32ST4X	N/A	V200R019C00SPC210
S5735-S48P4X	N/A	V200R019C00SPC210
S5735-S48S4X	N/A	V200R019C00SPC210
S5735-S48T4X	N/A	V200R019C00SPC210
S5735-S4T2X-IA150G1	N/A	V200R019C00SPC210
S5735-S8P2X-IA200G1	N/A	V200R019C00SPC210
S5735-S8P2X-IA200H1	N/A	V200R019C00SPC210
S5735S-H24T4S-A	N/A	V200R019C00SPC210
S5735S-H48T4S-A	N/A	V200R019C00SPC210
S5735S-L12P4S-A	N/A	V200R019C00SPC210
S5735S-L12T4S-A	N/A	V200R019C00SPC210

NE	New Version	Compatible Version
S5735S-L24FT4S-A	N/A	V200R019C00SPC210
S5735S-L24P4S-A	N/A	V200R019C00SPC210
S5735S-L24P4S-MA	N/A	V200R019C00SPC210
S5735S-L24P4X-A	N/A	V200R019C00SPC210
S5735S-L24T4S-A	N/A	V200R019C00SPC210
S5735S-L24T4S-MA	N/A	V200R019C00SPC210
S5735S-L24T4X-A	N/A	V200R019C00SPC210
S5735S-L32ST4X-A	N/A	V200R019C00SPC210
S5735S-L48FT4S-A	N/A	V200R019C00SPC210
S5735S-L48P4S-A	N/A	V200R019C00SPC210
S5735S-L48P4X-A	N/A	V200R019C00SPC210
S5735S-L48T4S-A	N/A	V200R019C00SPC210
S5735S-L48T4X-A	N/A	V200R019C00SPC210
S5735S-S24T4S-A	N/A	V200R019C00SPC210
S5735S-S32ST4X-A	N/A	V200R019C00SPC210
S5735S-S48T4S-A	N/A	V200R019C00SPC210
S6320-26Q-EI-24S-AC S6320-26Q-EI-24S-DC S6320-30C-EI-24S-AC S6320-30C-EI-24S-DC S6320-54C-EI-48S-AC S6320-54C-EI-48S-DC	N/A	V2R9C00
S6320-30C-EI-24S-AC S6320-30C-EI-24S-DC S6320-54C-EI-48S-AC S6320-54C-EI-48S-DC	N/A	V2R8C00

NE	New Version	Compatible Version
S6320-50L-HI-48S S6320-30L-HI-24S S6321-26Q-SI-24S-AC S6320-26Q-SI-24S-AC S6320-32X-SI-32S-AC S6320-32C-SI-AC S6320-32C-SI-DC S6320-56C-PWH-SI-AC S6320-56C-PWH-SI S6320-48Q-SI-48S-AC S6320-52X-PWH-SI-ACF S6320-32C-PWH-SI-AC S6320-32C-PWH-SI	N/A	V2R12C00
S6320-54C-EI-48S S6320-26Q-EI-24S-AC S6320-26Q-EI-24S-DC S6320-30C-EI-24S-AC S6320-30C-EI-24S-DC S6320-54C-EI-48S-AC S6320-54C-EI-48S-DC	N/A	V2R12C00, V2R10C00
S6324-EI S6348-EI	N/A	V2R7C00, V2R6C00, V2R5C00, V2R3C00, V2R2C00, V2R1C00, V1R6
S6330-H24X6C	N/A	V200R019C00SPC210
S6330-H48X6C	N/A	V200R019C00SPC210
S6500	N/A	VRP3.10 R2039[03]
S6502 S6503 S6506 S6506R	N/A	V200R005
S6700-24-EI S6700-48-EI	N/A	V2R7C00, V2R6C00, V2R5C00, V2R3, V2R2, V2R1, V1R6

NE	New Version	Compatible Version
S6720-26Q-LI-24S-AC S6720S-26Q-LI-24S-AC S6720S-26Q-SI-24S-AC S6720-26Q-SI-24S-AC S6720-16X-LI-16S-AC S6720S-16X-LI-16S-AC S6720-32X-LI-32S-AC S6720-50L-HI-48S S6720-30L-HI-24S S6720S-32X-LI-32S-AC S6720-32X-SI-32S-AC S6720-32C-SI-AC S6720-32C-SI-DC S6720-32C-PWH-SI-AC S6720-32C-PWH-SI	N/A	V2R12C00
S6720-26Q-LI-24S-AC S6720S-26Q-LI-24S-AC S6720S-26Q-SI-24S-AC S6720-26Q-SI-24S-AC S6720-16X-LI-16S-AC S6720S-16X-LI-16S-AC S6720-32X-LI-32S-AC S6720S-32X-LI-32S-AC S6720-32X-SI-32S-AC S6720-32C-SI-AC S6720-32C-SI-DC S6720-32C-PWH-SI-AC S6720-32C-PWH-SI S6720S-26Q-EI-24S-AC S6720S-26Q-EI-24S-DC S6720-30C-EI-24S-DC S6720-54C-EI-48S-DC S6720-30C-EI-24S-AC S6720-54C-EI-48S-AC	N/A	V2R12C00, V2R11C10, V2R11C00
S6720-30C-EI-24S-AC S6720-54C-EI-48S-AC	N/A	V2R8C00
S6720-50L-HI-48S S6720-30L-HI-24S	N/A	V2R12C00
S6720-56C-PWH-SI-AC S6720-56C-PWH-SI S6720-48Q-SI-48S-AC S6720S-48Q-SI-48S-AC S6720-52X-PWH-SI-ACF S6720-52X-PWH-SI	N/A	V2R11C10

NE	New Version	Compatible Version
S6720S-26Q-EI-24S-AC S6720S-26Q-EI-24S-DC S6720-30C-EI-24S-DC S6720-54C-EI-48S-DC S6720-30C-EI-24S-AC S6720-54C-EI-48S-AC	N/A	V2R9C00, V2R10C00
S6730-H24X6C	N/A	V200R019C00SPC210
S6730-H24X6C-K	N/A	V200R019C10
S6730-H48X6C	N/A	V200R019C00SPC210
S6730-H48X6C-K	N/A	V200R019C10
S6730-S24X6Q	N/A	V200R019C00SPC210
S6730S-S24X6Q-A	N/A	V200R019C00SPC210
S7703 S7706 S7712	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3, V2R2, V2R12C00, V2R10C00, V2R1, V1R6, V1R3
S7710	N/A	V2R10C00
S7810	N/A	Version 5.20, Release 6305
S8502	N/A	VRP310-R1640P01
S8505	N/A	V3.10 R1640P01, S8500-VRP310-R1648, S8500-VRP310-R1632P08 S8500-VRP310-R1632P07
S8508	N/A	Version 3.10, Release 1651, VRP V3.10 R1632P07 VRP V3.10 R1278P07, V100R006B01D028SP03



NE	New Version	Compatible Version
S8512	N/A	Version 3.10, Release 1648, VRP310-R1640P01
S9300X-12	N/A	V200R019C00SPC210
S9300X-4	N/A	V200R019C00SPC210
S9300X-8	N/A	V200R019C00SPC210
S9303 S9306 S9312	N/A	V2R9C00, V2R8C10, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3C00, V2R2C00, V2R1C00, V2R12C00, V2R10C00, V1R6, V1R3, V1R2, V1R1
S9303E S9306E S9312E	N/A	V2R9C00, V2R8C10, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3C00, V2R2C00, V2R1C00, V2R12C00, V2R10C00
S9310 S9310X	N/A	V2R10C00

NE	New Version	Compatible Version
S9703 S9306 S9712	N/A	V2R9C00, V2R8C00, V2R7C00, V2R6C00, V2R5C00, V2R3, V2R2, V2R12C00, V2R10C00, V2R1

**Table 10-19** CX200D series

NE	New Version	Compatible Version
CX200D CX200D-EA CX200D-MC CX200D-EA- MC	N/A	V2R3, V2R2

**Table 10-20** CE series

NE	New Version	Compatible Version
CE12800	N/A	V200R019C00
CE16804	N/A	V200R005C20
CE16808	N/A	V200R005C20
CE16816	N/A	V200R005C20
CE5800	N/A	V200R019C00
CE5800/CE6800/CE7800/ CE8800/CE12800	N/A	V200R005C00, V200R003C00
CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812	N/A	V1R3C00

NE	New Version	Compatible Version
CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S	N/A	V1R5C00
CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q-HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI	N/A	V1R5C10
CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE12804 CE12808 CE12812	N/A	V1R2C00
CE5850-48T4S2Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE12804 CE12808 CE12812	N/A	V1R1C00
CE5881-48T6CQ	N/A	V200R020C00
CE6800	N/A	V200R019C00

NE	New Version	Compatible Version
CE6820-48S6CQ	N/A	V200R005C20
CE6863-48S6CQ	N/A	V200R005C20
CE6863-48S6CQ-K	N/A	V200R019C10
CE6865-48S8CQ-SI	N/A	V200R005C20
CE6881-48S6CQ	N/A	V200R005C20
CE6881-48S6CQ-K	N/A	V200R019C10
CE6881-48T6CQ	N/A	V200R020C00
CE6881-48T6CQ-K	N/A	V200R020C00
CE6881E-48S6CQ	N/A	V200R019C10
CE7800	N/A	V200R019C00
CE8800	N/A	V200R019C00
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI	N/A	V1R6C00

NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q-HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6865-48S8CQ-EI CE8850-64CQ-EI CE6875-48S4CQ-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M CE6880-48S4Q2CQ-EI CE6880-24S4Q2CQ-EI CE6880-48T4Q2CQ-EI CE8850-32CQ-EI CE6860-48S18CQ-EI CE12804E CE12808E CE12812E CE12816E CE6870-48T6CQ-EI CE6856-48S6Q-HI CE6856-48T6Q-HI CE8861-4C-EI CE8868-4C-EI CE5880-48T6Q-EI CE6857-48S6CQ-EI	N/A	V2R5C10, V2R19C00

NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6865-48S8CQ-EI CE8850-64CQ-EI CE6875-48S4CQ-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M CE6880-48S4Q2CQ-EI CE6880-24S4Q2CQ-EI CE6880-48T4Q2CQ-EI CE8850-32CQ-EI CE6860-48S18CQ-EI CE12804E CE12808E CE12812E CE12816E CE6870-48T6CQ-EI CE6856-48S6Q-HI CE6856-48T6Q-HI	N/A	V2R5C00

NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M	N/A	V2R2C01

NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M CE6880-48S4Q2CQ-EI CE6880-24S4Q2CQ-EI CE6880-48T4Q2CQ-EI	N/A	V2R2C10



NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M CE6880-48S4Q2CQ-EI CE6880-24S4Q2CQ-EI CE6880-48T4Q2CQ-EI CE8850-32CQ-EI CE6860-48S18CQ-EI	N/A	V2R2C20

NE	New Version	Compatible Version
CE8800 CE5850-48T4S2Q-EI CE5810-24T4S-EI CE5810-48T4S-EI CE6810-48S4Q-EI CE6850-48T4Q-EI CE6850-48S4Q-EI CE7850-32Q-EI CE12804 CE12808 CE12812 CE6850-48S6Q-HI CE6850U-48S6Q-HI CE12804S CE12808S CE5855-48T4S2Q-EI CE5855-24T4S2Q-EI CE5810-48T4S-HI CE6850-48T6Q-HI CE6810-32T16S4Q-LI CE6850U-48S6Q- HIU2000 CE6850U-24S2Q-HI CE6810-24S2Q-HI CE6810-24S2Q-LI CE6855-48T6Q-HI CE6855-48S6Q-HI CE6870-48S6CQ-EI CE6870-24S6CQ-EI CE7855-32Q-EI CE6860-48S8CQ-EI CE12816M CE6880-48S4Q2CQ-EI CE6880-24S4Q2CQ-EI CE6880-48T4Q2CQ-EI CE8850-32CQ-EI CE6860-48S18CQ-EI CE12804E CE12808E CE12812E CE12816E CE6870-48T6CQ-EI CE6856-48S6Q-HI CE6856-48T6Q-HI	N/A	V2R2C50

NE	New Version	Compatible Version
CE8800CE5850-48T4S2Q -EICE5810-24T4S- EICE5810-48T4S- EICE6810-48S4Q- EICE6850-48T4Q- EICE6850-48S4Q- EICE7850-32Q- EICE12804CE12808CE128 12CE6850-48S6Q- HICE6850U-48S6Q- HICE12804SCE12808SCE 5855-48T4S2Q- EICE5855-24T4S2Q- EICE5810-48T4S- HICE6850-48T6Q- HICE6810-32T16S4Q- LICE6850U-48S6Q- HIU2000CE6850U-24S2Q- -HICE6810-24S2Q- HICE6810-24S2Q- LICE6855-48T6Q- HICE6855-48S6Q- HICE6870-48S6CQ- EICE6870-24S6CQ- EICE7855-32Q-EI	N/A	V2R1C00
CE9860-4C-EI	N/A	V200R020C00

## 10.9 Security Series

The following table lists the security series NEs supported.

**Table 10-21** Eudemon series

NE	New Version	Compatible Version
1U:E200E-CE200E- FE200E-F-DE200E- X3E200E-X5E200E- X5DC2U:E200E-X6E200E- X6DC3U:E200E-X7	N/A	V3R1C00

NE	New Version	Compatible Version
3U:E8000E- X3USG95208U:E8000E- X8USG956016U:E8000E- X16USG9580	N/A	V5R2C10/V5R1C50, V5R2C00/V5R1C30, V5R1C20, V5R1C10, V5R1C00, V3R1C00, V2R1C01, V2R1C00
3U:E8000E- X3USG95208U:E8000E- X8USG956016U:E8000E- X16USG9580USG9000VE 8000E-V	N/A	V5R3C00/V5R1C80
3U:SeMG9811- X38U:SeMG9811- X816U:SeMG9811-X16	N/A	V300R001C01, V300R001C00
E1000E-G3-AC E1000E- G3-DC E1000E-G5-AC E1000E-G5-DC E1000E- G8-AC E1000E-G8-DC E1000E-G12-AC E1000E- G12-DC E1000E-G16-AC E1000E-G16-DC	N/A	V600R006
E100E	N/A	V2R7C01
E200	N/A	V2R1C03, V2R1C01
E200E-B	N/A	V1R2C00
E200E-B E200E-BW E200E-X2 E200E-X2W E200E-X2NEW E200E- X2WNEW	N/A	V3R1C00, V1R5C00
E200E-C E200E-F E200E- F-D	N/A	V1R2C00
E200E-CE200E-FE200E-F- DE200E-X3E200E- X5E200E-X5DC2U:E200E- X6E200E-X6DC3U:E200E- X7	N/A	V1R5C00
E200E-G8-AC E200E-G8- DC	N/A	V600R006

NE	New Version	Compatible Version
E200S	N/A	V2R7C01
E300 E500 E1000	N/A	V2R6C02
E8040 E8080	N/A	V3R1C06, V3R1C05
E8080E E8160E	N/A	V2R1C01
E8080E E8160E USG9310 USG9320	N/A	V5R1C00, V2R1C00, V1R3C00, V1R2C00, V1R1C05, V1R1C01
Eudemon 1000E-N	N/A	V500R003C00
Eudemon 200E-N	N/A	V500R003C00
Eudemon 8080E	N/A	V500R003C00
Eudemon1000E-G15-AC	N/A	V600R007C00
Eudemon1000E-G15-DC	N/A	V600R007C00
Eudemon1000E-G25-AC	N/A	V600R007C00
Eudemon1000E-G25-DC	N/A	V600R007C00
Eudemon1000E-G35-AC	N/A	V600R007C00
Eudemon1000E-G35-DC	N/A	V600R007C00
Eudemon1000E-G55-AC	N/A	V600R007C00
Eudemon1000E-G55-DC	N/A	V600R007C00
Eudemon200E-G85-AC	N/A	V600R007C00
Eudemon200E-G85-DC	N/A	V600R007C00
Eudemon8000E-X3	N/A	V500R005C00
NE40E-FW NE80E-FW	N/A	V5R8C03, V5R8C02, V5R8C01, V5R8C00

NE	New Version	Compatible Version
vRouter6000V1 vRouter6000V2 vRouter6000V4 vRouter6000V8 Eudemon1000E-V1 Eudemon1000E-V2 Eudemon1000E-V4 Eudemon1000E-V8	N/A	V5R1C10

**Table 10-22** NGFW series

NE	New Version	Compatible Version
E1000E-N6 E1000E-N7 E1000E-N7E	N/A	V1R1C10
E1000E-N6 E1000E-N7 E1000E-N7E E1000E-N3 E1000E-N5	N/A	V5R2C10/V5R1C50, V5R2C00/V5R1C30, V5R1C00, V1R1C20
E200E-N1D E200E-N3 E200E-N5	N/A	V1R1C10
E200E-N1D E200E-N3 E200E-N5 E200E-N1 E200E-N2	N/A	V5R2C10/V5R1C50, V5R2C00/V5R1C30, V5R1C00, V1R1C20
Eudemon 1000E-N	N/A	V500R003C00
Eudemon 200E-N	N/A	V500R003C00
LE1D2FW00S01	N/A	V5R2C10/V5R1C50, V5R2C00/V5R1C30, V5R1C00, V500R003C00, V1R1C20, V1R1C10

NE	New Version	Compatible Version
NIP6610-AC NIP6320-AC NIP6320D-AC NIP6330- AC NIP6330D-AC NIP6620-AC NIP6620D- AC NIP6650-AC NIP6650-DC NIP6650D- AC NIP6650D-DC NIP6680-AC NIP6680-DC CE-FWA CE-IPSA	N/A	V5R2C00/V5R1C30, V5R1C00
NIP6860-DC NIP6830 NIP6610-AC NIP6320-AC NIP6320D-AC NIP6330- AC NIP6330D-AC NIP6620-AC NIP6620D- AC NIP6650-AC NIP6650-DC NIP6650D- AC NIP6650D-DC NIP6680-AC NIP6680-DC CE-FWA CE-IPSA	N/A	V5R2C10/V5R1C50

**Table 10-23** USG series

NE	New Version	Compatible Version
1U:USG2210USG2220US G2230USG2250USG2250 - DUSG2260USG2205BSR USG2220BSRUSG2220BS R- DUSG2205HSRUSG2220 HSRUSG2220HSR-D	N/A	V3R1C00
1U:USG5520SUSG5530SE 1000E-X3E1000E- X5E1000E-X2E1000E-X2- D3U:USG5530USG5550U SG5560E1000E- X6E1000E-X7E1000E- X8E1000E-X7-DE1000E- X8-D	N/A	V3R1C00
1U:USG5530SE1000E- X3E1000E- X53U:USG5530USG5550 USG5560E1000E-X6	N/A	V2R2C00, V2R1C00

NE	New Version	Compatible Version
2U: USG5120 USG5120-D 3U: USG5150 USG5160	N/A	V3R1C00
2U:USG5120BSRUSG5120 BSR-D3U:USG5150BSR	N/A	V1R3C01
2U:USG5120BSRUSG5120 HSR3U:USG5150BSRUSG5150 HSR	N/A	V3R1C00
2U:USG5120BSRUSG5120 HSR3U:USG5150BSRUSG5150 HSRUSG5160	N/A	V1R5C00
2U:USG5120USG5120-D 3U:USG5150	N/A	V1R5C00, V1R3C01
AntiDDoS1820-N	N/A	V600R007C00
AntiDDoS8030 AntiDDoS8080 AntiDDoS8160	N/A	V5R1C00
AntiDDoS8030 AntiDDoS8080 AntiDDoS8160 AntiDDoS1520 AntiDDoS1550 AntiDDoS1500-D	N/A	V5R1C60, V5R1C30, V1R1C00
AntiDDoS1820 AntiDDoS1880	N/A	V600R006
AntiDDoS1825	N/A	V600R007C00
E1000E-D E1000E-I	N/A	V1R5C00
USG 6680	N/A	V1R1
USG2110-F USG2110-F-W USG2110-A-W USG2110-A-GW-W USG2110-A-GW-C	N/A	V1R3C03
USG2110-F USG2110-F-W USG2110-A-W USG2110-A-GW-W USG2110-A-GW-C E200E-X1AGW-W E200E-X1 AGW-C E200E-X1 E200E-X1W	N/A	V3R1C00



NE	New Version	Compatible Version
USG2110-F USG2110-F-W USG2110-A-W USG2110-A-GW-W USG2110-A-GW-C E200E-X1AGW-W E200E-X1AGW-C E200E-X1 E200E-X1W	N/A	V1R5C00
USG2130 USG2130W USG2160 USG2160W USG2120BSR USG2130BSR USG2130BSR-W USG2160BSR USG2160BSR-W	N/A	V1R3C01
USG2130 USG2130W USG2160 USG2160W USG2120BSR USG2130BSR USG2130BSR-W USG2160BSR USG2160BSR-W USG2130HSR USG2130HSR-W USG2160HSR USG2160HSR-W	N/A	V3R1C00, V1R5C00
USG2130 USG2130W USG2160 USG2160W	N/A	V1R2C01
USG2205BSR USG2220BSR USG2220BSR-D USG2205HSR USG2220HSR USG2220HSR-D	N/A	V1R5C00
USG2205BSR USG2220BSR USG2220BSR-D USG2205HSR USG2220HSR USG2220HSR-D USG2220TSM USG2250TSM	N/A	V1R3C01
USG2210 USG2220 USG2230 USG2250 USG2250-D	N/A	V1R5C00, V1R3C01, V1R2C01
USG3040 USG3030	N/A	V1R1C03

NE	New Version	Compatible Version
USG50 USG2110 SRG20-10	N/A	V1R1C03
USG5300ADD USG5300ADI	N/A	V1R1C00
USG5320 USG5330 USG5350 USG5360 USG5310 E1000E-U2 E1000E-U3 E1000E-U5 E1000E-U6	N/A	V2R1C00, V1R5C00, V1R3C01, V1R2C01
USG6305E-AC	N/A	V600R007C00
USG6307E-AC	N/A	V600R007C00
USG6309E-AC	N/A	V600R007C00
USG6311E-AC	N/A	V600R007C00
USG6315E-AC	N/A	V600R007C00
USG6325E-AC	N/A	V600R007C00
USG6331E-AC	N/A	V600R007C00
USG6335E-AC	N/A	V600R007C00
USG6355E-AC	N/A	V600R007C00
USG6365E-AC	N/A	V600R007C00
USG6385E-AC	N/A	V600R007C00
USG6395E-AC	N/A	V600R007C00
USG6510E-AC	N/A	V600R007C00
USG6515E USG6550E USG6560E USG6580E	N/A	V600R006
USG6525E-AC	N/A	V600R007C00
USG6530E-AC	N/A	V600R007C00
USG6555E-AC	N/A	V600R007C00
USG6565E-AC	N/A	V600R007C00
USG6585E-AC	N/A	V600R007C00
USG6615E-AC	N/A	V600R007C00
USG6625E-AC	N/A	V600R007C00
USG6630E-AC USG6630E-DC USG6650E USG6680E	N/A	V600R006

NE	New Version	Compatible Version
USG6635E-AC	N/A	V600R007C00
USG6635E-DC	N/A	V600R007C00
USG6655E-AC	N/A	V600R007C00
USG9110 USG9120 E6080E	N/A	V1R1C00

**Table 10-24** SRG series

NE	New Version	Compatible Version
SRG1210 SRG1210W SRG1210-S SRG1220 SRG1220W	N/A	V1R2C02, V1R2C01, V1R1C01
SRG20-11 SRG20-12 SRG20-12W SRG20-15 SRG20-15W	N/A	V1R5C00, V1R3C01, V1R2C01
SRG20-20 SRG20-21 SRG20-30 SRG20-31	N/A	V2R2C01, V1R5C00
SRG20-31-D	N/A	V2R2C01, V1R5C00
SRG2210 SRG2220 SRG2220-D	N/A	V1R1C01
SRG2210SRG2220SRG22 20- D2U:SRG3230SRG3240SR G3240- D3U:SRG3250SRG3260	N/A	V1R2C02, V1R2C01SPC200

**Table 10-25** ASG series

NE	New Version	Compatible Version
ASG2100 ASG2200 ASG2600 ASG2800	N/A	V1R1C00

**Table 10-26** EGW series

NE	New Version	Compatible Version
EGW2112GW(VDF)	N/A	V1R1C02
EGW2112GW(VDF) EGW2112GW	N/A	V1R1C20
EGW2130 EGW2130W EGW2160 EGW2160W	N/A	V1R1C02
EGW2130 EGW2130W EGW2160 EGW2160W EGW2160DC EGW2160W(VDF)	N/A	V1R1C20
EGW2210EGW22202U:E GW3230EGW32403U:EG W3250EGW3260	N/A	V1R1C02
EGW2210EGW2220EGW 2220DC2U:EGW3230EG W3240EGW3240DC3U:E GW3250EGW3260	N/A	V1R1C20

**Table 10-27** SIG series

NE	New Version	Compatible Version
DPI Server	N/A	V5R9C02, V5R9C01, V5R9C00
NE40E-DPI NE80E-DPI	N/A	V5R9C02, V5R9C01, V5R9C00
RADIUS Proxy	N/A	V3R7C00, V3R5C00 V3R6C00 V3R6C10 V3R6C20, V3R3C00, V3R1C00, V300R009C00, V300R008C10, V300R007C10, V2R3C00, V2R2C02
RADIUS Proxy-DPI	N/A	V5R9C02

NE	New Version	Compatible Version
SIG Server	N/A	V3R7C00, V3R5C00 V3R6C00 V3R6C10 V3R6C20, V3R3C00, V3R1C00, V300R009C00, V300R008C10, V300R007C10, V2R3C00, V2R2C02, V2R2C01
SIG9800	N/A	V300R009C00, V300R008C10, V300R007C10
SIG9800-X16	N/A	V300R009C00, V300R008C10, V300R007C10
SIG9800-X3	N/A	V300R009C00, V300R008C10, V300R007C10
SIG9800-X3 SIG9800-X8 SIG9800-X16	N/A	V3R8C10, V3R7C00, V3R5C00 V3R6C00 V3R6C10 V3R6C20, V3R3C00, V3R1C00
SIG9800-X8	N/A	V300R009C00, V300R008C10, V300R007C10
SIG9810 SIG9820	N/A	V3R7C00, V3R5C00 V3R6C00 V3R6C10 V3R6C20, V3R3C00, V3R1C00, V2R3C00, V2R2C02, V2R2C01

NE	New Version	Compatible Version
URL Classify Server	N/A	V3R7C00, V3R5C00 V3R6C00 V3R6C10 V3R6C20, V3R3C00, V3R1C00, V300R009C00, V300R008C10, V300R007C10, V1R2C01, V1R1C00
URL Classify Server-DPI	N/A	V5R9C02

**Table 10-28** NE40E/80E-FW series

NE	New Version	Compatible Version
NE40E-FW	N/A	V500R008C03, V500R008C02, V500R008C01, V500R008C00
NE80E-FW	N/A	V500R008C03, V500R008C02, V500R008C01, V500R008C00

**Table 10-29** OP-Bypass series

NE	New Version	Compatible Version
OP-Bypass	N/A	V1R1C00

**Table 10-30** SVN series

NE	New Version	Compatible Version
SVN2230 SVN2260 SVN5300 SVN5530 SVN5560	N/A	V2R1C00

NE	New Version	Compatible Version
SVN2230 SVN2260 SVN5530 SVN5560	N/A	V2R1C01
SVN3000	N/A	V1R2C02
SVN5630 SVN5660 SVN5830 SVN5850 SVN5860 SVN5880 SVN5880-C	N/A	V2R3C00

**Table 10-31** NIP series

NE	New Version	Compatible Version
IPS6309E-AC	N/A	V600R007C00
IPS6315E-AC	N/A	V600R007C00
IPS6515E-AC	N/A	V600R007C00
IPS6555E-AC	N/A	V600R007C00
IPS6555ED-AC	N/A	V600R007C00
NIP6305E NIP6310E NIP6510E NIP6550E NIP6610E NIP6620E NIP6650ED-AC NIP6620E-DC	N/A	V600R006

**Table 10-32** CE series

NE	New Version	Compatible Version
CE-FWA	N/A	V500R003C00

**Table 10-33** SeMG9811 series

NE	New Version	Compatible Version
3U:SeMG9811- X38U:SeMG9811- X816U:SeMG9811-X16	N/A	V5R1C50

## 10.10 iCache Series

The following table lists the iCache series NEs supported.

**Table 10-34** iCache series

NE	New Version	Compatible Version
iCache9200 CSS	N/A	V200R001C00
iCache9200 CSS	N/A	V100R002C00
iCache9200 DSS	N/A	V200R001C00, V100R002C00
iCache9200 MSS	N/A	V200R001C00
iCache9200 MSS	N/A	V100R002C00
iCache9200 RSS	N/A	V200R001C00, V100R002C00

## 10.11 FTTx Series

The following table lists the manageable FTTx series NEs supported.

**Table 10-35** OLT series

NE	New Version	Compatible Version
SmartAX EA5800-X15	N/A	EA5800 V100R019C20, EA5800 V100R019C10, EA5800 V100R019C00, EA5800 V100R018C10, EA5800 V100R018C00
SmartAX EA5800-X17	N/A	EA5800 V100R019C20, EA5800 V100R019C10, EA5800 V100R019C00, EA5800 V100R018C10, EA5800 V100R018C00



NE	New Version	Compatible Version
SmartAX EA5800-X2	N/A	EA5800 V100R019C20, EA5800 V100R019C10, EA5800 V100R019C00, EA5800 V100R018C10, EA5800 V100R018C00
SmartAX EA5800-X7	N/A	EA5800 V100R019C20, EA5800 V100R019C10, EA5800 V100R019C00, EA5800 V100R018C10, EA5800 V100R018C00
SmartAX EA5801-CG04	N/A	EA5801 V100R019C20, EA5801 V100R019C10, EA5801 V100R019C00
SmartAX EA5801-GP08	N/A	EA5801 V100R019C20, EA5801 V100R019C10, EA5801 V100R019C00

NE	New Version	Compatible Version
SmartAX MA5600T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00SPC200, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C02, MA5600 V800R008C01, MA5600 V800R008C00, MA5600 V800R007C01, MA5600 V800R007C00, MA5600 V800R006C72, MA5600 V800R006C32, MA5600 V800R006C31, MA5600 V800R006C02SPC100, MA5600 V800R006C02

NE	New Version	Compatible Version
SmartAX MA5603T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00SPC200, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C02, MA5600 V800R008C01, MA5600 V800R008C00, MA5600 V800R007C01, MA5600 V800R007C00, MA5600 V800R006C73, MA5600 V800R006C32, MA5600 V800R006C02SPC100, MA5600 V800R006C02

NE	New Version	Compatible Version
SmartAX MA5608T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00SPC200, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00

NE	New Version	Compatible Version
SmartAX MA5680T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00SPC200, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C02, MA5600 V800R008C01, MA5600 V800R008C00, MA5600 V800R007C01, MA5600 V800R007C00, MA5600 V800R006C72, MA5600 V800R006C32, MA5600 V800R006C31, MA5600 V800R006C02SPC100, MA5600 V800R006C02

NE	New Version	Compatible Version
SmartAX MA5683T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00SPC200, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C01, MA5600 V800R007C01, MA5600 V800R007C00, MA5600 V800R006C72, MA5600 V800R006C32, MA5600 V800R006C02SPC100, MA5600 V800R006C02
SmartAX MA5800-X15	N/A	MA5800 V100R019C20, MA5800 V100R019C10, MA5800 V100R019C00, MA5800 V100R018C10, MA5800 V100R018C00, MA5800 V100R017C10, MA5800 V100R017C00, MA5800 V100R016C10

NE	New Version	Compatible Version
SmartAX MA5800-X17	N/A	MA5800 V100R019C20, MA5800 V100R019C10, MA5800 V100R019C00, MA5800 V100R018C10, MA5800 V100R018C00, MA5800 V100R017C10, MA5800 V100R017C00, MA5800 V100R016C10, MA5800 V100R016C00, MA5800 V100R015C00
SmartAX MA5800-X2	N/A	MA5800 V100R019C20, MA5800 V100R019C10, MA5800 V100R019C00, MA5800 V100R018C10, MA5800 V100R018C00, MA5800 V100R017C10
SmartAX MA5800-X7	N/A	MA5800 V100R019C20, MA5800 V100R019C10, MA5800 V100R019C00, MA5800 V100R018C10, MA5800 V100R018C00, MA5800 V100R017C10, MA5800 V100R017C00, MA5800 V100R016C10, MA5800 V100R016C00
SmartAX MA5801-CG04	N/A	MA5801 V100R019C20, MA5801 V100R019C10, MA5801 V100R019C00
SmartAX MA5801-GP08	N/A	MA5801 V100R019C20, MA5801 V100R019C10, MA5801 V100R019C00

**Table 10-36** MDU series

NE	New Version	Compatible Version
SmartAX EA5821	N/A	EA5821 V800R018C00

NE	New Version	Compatible Version
SmartAX MA5606T	N/A	MA5600V800R007C01, MA5600V800R007C00, MA5600V800R006C62, MA5600V800R006C22, MA5600V800R006C21, MA5600V800R006C02
SmartAX MA5611S	N/A	MA5611S V800R018C10, MA5611S V800R018C00, MA5611S V800R017C10, MA5611S V800R016C00, MA5611S V800R015C10, MA5611S V800R015C00, MA5611S V800R313C10, MA5611S V800R313C00
SmartAX MA5610	N/A	MA5610 V800R307C01, MA5610 V800R306C01
SmartAX MA5612	N/A	MA5612 V800R312C00, MA5612 V800R311C00, MA5612 V800R310C00, MA5612 V800R308C03, MA5612 V800R308C01, MA5612 V800R308C00, MA5612 V800R018C10, MA5612 V800R017C00, MA5612 V800R015C00, MA5612 V800R307C01
SmartAX MA5612A	N/A	MA5612 V800R015C00, MA5612 V800R312C00, MA5612 V800R311C00, MA5612 V800R310C00, MA5612 V800R308C01



NE	New Version	Compatible Version
SmartAX MA5616	N/A	MA5616 V800R313C10, MA5616 V800R313C00, MA5616 V800R312C00, MA5616 V800R311C00, MA5616 V800R310C00, MA5616 V800R309C00, MA5616 V800R308C03, MA5616 V800R308C02, MA5616 V800R308C01, MA5616 V800R308C00, MA5616 V800R307C02, MA5616 V800R307C01, MA5616 V800R307C00, MA5616 V800R306C01, MA5616 V800R019C10, MA5616 V800R019C00, MA5616 V800R018C10, MA5616 V800R018C00, MA5616 V800R017C10, MA5616 V800R017C00, MA5616 V800R016C10, MA5616 V800R016C00, MA5616 V800R015C10, MA5616 V800R015C00
SmartAX MA5620	N/A	MA5620 V800R016C10, MA5620 V800R312C00, MA5620 V800R310C00, MA5620 V800R308C02, MA5620 V800R308C00, MA5620 V800R307C01, MA5620 V800R307C00
SmartAX MA5620E	N/A	MA5620E V800R307C01, MA5620E V800R307C00, MA5600 V800R305C01
SmartAX MA5620G	N/A	MA5620G V800R307C01, MA5620G V800R307C00, MA5600 V800R305C01

NE	New Version	Compatible Version
SmartAX MA5621	N/A	MA5621 V800R017C00, MA5621 V800R312C00, MA5621 V800R310C00, MA5621 V800R309C00
SmartAX MA5621A	N/A	MA5621 V800R016C00, MA5621 V800R312C00, MA5621 V800R311C00
SmartAX MA5623A	N/A	MA5623 V800R016C00, MA5623 V800R313C10, MA5623 V800R313C00, MA5623 V800R312C00, MA5623 V800R311C01
SmartAX MA5626	N/A	MA5626 V800R016C10, MA5626 V800R312C00, MA5626 V800R310C00, MA5626 V800R308C00, MA5626 V800R307C01, MA5626 V800R307C00
SmartAX MA5622A	N/A	MA5622 V800R313C00, MA5622 V800R311C00
SmartAX MA5626E	N/A	MA5626E V800R307C01, MA5626E V800R307C00, MA5600 V800R305C01
SmartAX MA5651S	N/A	MA5651S V800R018C00, MA5651S V800R017C10, MA5651S V800R017C00, MA5651S V800R016C10, MA5651S V800R313C10
SmartAX MA5652S	N/A	MA5652S V800R018C00, MA5652S V800R017C10, MA5652S V800R017C00, MA5652S V800R313C10
SmartAX MA5626G	N/A	MA5626G V800R307C01, MA5626G V800R307C00, MA5600 V800R305C01

NE	New Version	Compatible Version
SmartAX MA5628	N/A	MA5628 V800R310C00, MA5628 V800R309C00, MA5628 V800R308C01
SmartAX MA5631	N/A	MA5631 V800R310C00, MA5631 V800R308C02
SmartAX MA5632	N/A	MA5632 V800R310C00
SmartAX MA5651	N/A	MA5651 V800R305C03
SmartAX MA5652G	N/A	MA5652G V800R308C02, MA5652G V800R307C00, MA5652G V800R306C01
SmartAX MA5658	N/A	MA5658 V800R312C00
SmartAX MA5671	N/A	MA5671 V800R017C00, MA5671 V800R016C10, MA5671 V800R016C00, MA5671 V800R313C00
SmartAX MA5671A	N/A	MA5671A V800R015C10
SmartAX MA5671A-G1	N/A	MA5671A V800R016C00
SmartAX MA5672-16	N/A	MA5672 V800R016C00
SmartAX MA5672-24	N/A	MA5672 V800R016C00
SmartAX MA5672-8	N/A	MA5672 V800R016C00
SmartAX MA5672M	N/A	MA5672M V800R017C00, MA5672M V800R313C00
SmartAX MA5673	N/A	MA5673 V800R016C00, MA5673 V800R313C00
SmartAX MA5675	N/A	MA5675 V800R017C00, MA5675 V800R016C00, MA5675 V800R313C00
SmartAX MA5675-G1F1	N/A	MA5675 V800R016C00
SmartAX MA5675-G1F1P1	N/A	MA5675 V800R017C00, MA5675 V800R016C00

NE	New Version	Compatible Version
SmartAX MA5675M	N/A	MA5675M V800R017C00, MA5675M V800R016C00, MA5675M V800R313C00
SmartAX MA5676	N/A	MA5676 V800R016C10
SmartAX MA5676-G1F1	N/A	MA5676 V800R016C00
SmartAX MA5694	N/A	MA5694 V800R016C00, MA5694 V800R015C00, MA5694 V800R313C00
SmartAX MA5694S	N/A	MA5694S V800R015C00, MA5694S V800R313C10
SmartAX MA5698	N/A	MA5698 V800R015C00, MA5698 V800R313C00
SmartAX MA5811S	N/A	MA5811S V800R019C00, MA5811S V800R018C10, MA5811S V800R018C00, MA5811S V800R017C10, MA5811S V800R017C00, MA5811S V800R016C10, MA5811S V800R016C00
SmartAX MA5818	N/A	MA5818 V800R020C00, MA5818 V800R019C10, MA5818 V800R019C00, MA5818 V800R018C10, MA5818 V800R018C00, MA5818 V800R017C10, MA5818 V800R017C00, MA5818 V800R313C00, MA5818 V800R016C00, MA5818 V800R015C10, MA5818 V800R015C00
SmartAX MA5821	N/A	MA5821 V800R018C00, MA5821 V800R017C10, MA5821 V800R017C00, MA5821 V800R313C10, MA5821 V800R313C00

NE	New Version	Compatible Version
SmartAX MA5822	N/A	MA5822 V800R017C00, MA5822 V800R313C00
SmartAX MA5871-G4	N/A	MA5871 V800R016C00
SmartAX MA5871D	N/A	MA5871 V800R019C00
SmartAX MA5875-5E4P	N/A	MA5875 V300R019C20
SmartAX MA5875-8E8P	N/A	MA5875 V300R019C20
SmartAX MA5878	N/A	MA5878 V800R017C00
SmartAX MA5898	N/A	MA5898 V800R018C00, MA5898 V800R017C10, MA5898 V800R015C00, MA5898 V800R313C00

## 10.12 MSAN Series

The following table lists the MSAN series NEs supported.

**Table 10-37** UA5000 series

NE	New Version	Compatible Version
UA5000 IPMB	N/A	UA5000IPMB V100R019C07, UA5000IPMB V100R019C02, UA5000IPMB V100R019C01, UA5000IPMB V100R019C00, UA5000IPMB V100R017C02, UA5000IPMB V100R015C09, UA5000IPMB V100R015C02

NE	New Version	Compatible Version
UA5000 PVM	N/A	UA5000PVM V100R019C07, UA5000PVM V100R019C06, UA5000PVM V100R019C02, UA5000PVM V100R019C01, UA5000PVM V100R019C00, UA5000PVM V100R017C03, UA5000PVM V100R017C02, UA5000PVM V100R017C01

## 10.13 DSLAM Series

The following table lists the DSLAM series NEs supported.

**Table 10-38** MA5600 series

NE	New Version	Compatible Version
SmartAX MA5600	N/A	MA5600 V300R003C07, MA5600 V300R003C06, MA5600 V300R003C05

**Table 10-39** MA5600V8 series

NE	New Version	Compatible Version
SmartAX MA5600T	N/A	MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C02, MA5600 V800R008C01, MA5600 V800R008C00, MA5600 V800R007C01, MA5600 V800R007C00, MA5600 V800R006C72, MA5600 V800R006C32, MA5600 V800R006C31, MA5600 V800R006C02SPC100, MA5600 V800R006C02

NE	New Version	Compatible Version
SmartAX MA5603T	N/A	MA5603 V800R008C00, MA5603 V800R007C01, MA5603 V800R007C00, MA5600 V800R019C20, MA5600 V800R019C10, MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00, MA5600 V800R011C00, MA5600 V800R010C00, MA5600 V800R009C00, MA5600 V800R008C05, MA5600 V800R008C03, MA5600 V800R008C02, MA5600 V800R008C01, MA5600 V800R006C73, MA5600 V800R006C32, MA5600 V800R006C02SPC100, MA5600 V800R006C02
SmartAX MA5606T	N/A	MA5600V800R007C01, MA5600V800R007C00, MA5600V800R006C62, MA5600V800R006C22, MA5600V800R006C21, MA5600V800R006C02



NE	New Version	Compatible Version
SmartAX MA5608T	N/A	MA5600 V800R018C10SPC200, MA5600 V800R018C10, MA5600 V800R018C00, MA5600 V800R017C10, MA5600 V800R017C00, MA5600 V800R016C10, MA5600 V800R016C00, MA5600 V800R015C10, MA5600 V800R015C00, MA5600 V800R013C10, MA5600 V800R013C00, MA5600 V800R012C00

## 10.14 BITS/iSite/EDFA Series

The following table lists the BITS/iSite/EDFA series NEs supported.

**Table 10-40** BITS series

NE	New Version	Compatible Version
SYNLOCK T6020	N/A	BITS V6
SYNLOCK V3/V5	N/A	BITS V5, BITS V3
T8010	N/A	V8R18C00

**Table 10-41** EDFA series

NE	New Version	Compatible Version
EDFA0820-D	N/A	EDFA&WDM1r V100R019C00
EDFA0820-D2	N/A	EDFA&WDM1r V100R019C00
EDFA3220-D	N/A	EDFA&WDM1r V100R006C00
EDFA3220-D2	N/A	EDFA&WDM1r V100R018C10

**Table 10-42** iSite series

<b>NE</b>	<b>New Version</b>	<b>Compatible Version</b>
CCU	N/A	CCU V200R001C00, CCU V100R001C00
RPS	N/A	ETPC1701 V100R001C30 (iSite V300R016C10), ETPC1701 V100R001C20 (iSite V300R016C00), ETPC1701 V100R001C20 (iSite V300R015C92)
SMU11B	N/A	V500R002C50

# A Appendix

## A.1 Standards Compliance

NCE complies with ITU-T, IETF, and TMF standards and protocols.

**Table A-1** Standards and protocols

Standard/Protocol	Name
CIS	Center for Internet Security Benchmarks
Sif99025	EML-NML interface models
TMF513 V2.0	Multi-Technology Network Management Business Agreement NML-EML Interface Version 2.0
TMF518	MTOSI Business Agreement
TMF608 V2.0	Multi-Technology Network Management Information Agreement NML-EML Interface Version 2.0
TMF612	MTOSI Information Agreement
TMF814 V2.0	Multi Technology Network Management Solution Set Conformance Document Version 2.0
TMF814A	MTNM Implementation Statement and Guidelines for MTNM Release 3.5M
TMF864	MTOSI Interface Implementation Specifications
ISO 8824-4-2000	Information Technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications Amendment 1: ASN.1 semantic model
ISO 8825-2-1998	Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER) Second Edition; Technical Corrigendum 1: 12/15/1999; Amendment 1: 12/01/2000

Standard/Protocol	Name
ITU-T G.707	Network node interface for the synchronous digital hierarchy (SDH)
ITU-T G.7710	Common equipment management function requirements
ITU-T G.773	Protocol suites for Q-interfaces for management of transmission systems
ITU-T G.774 (01, 02, 03, 04)	Synchronous digital hierarchy (SDH) - Management information model for the network element view
ITU-T G.783	Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks
ITU-T G.784	Synchronous digital hierarchy (SDH) management
ITU-T G.803	Architecture of transport networks based on the synchronous digital hierarchy (SDH)
ITU-T G.831	Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)
ITU-T G.851.1	Management of the transport network - Application of the RM-ODP framework
ITU-T G.852.1	Enterprise viewpoint for simple subnetwork connection management
ITU-T G.852.2	Enterprise viewpoint description of transport network resource model
ITU-T G.852.3	Enterprise viewpoint for topology management
ITU-T G.852.6	Enterprise viewpoint for trail management
ITU-T G.853.1	Common elements of the information viewpoint for the management of a transport network
ITU-T G.853.2	Subnetwork connection management information viewpoint
ITU-T G.853.3	Information viewpoint for topology management
ITU-T G.853.6	Information viewpoint for trail management
ITU-T G.854.1	Computational interfaces for basic transport network model
ITU-T G.854.3	Computational viewpoint for topology management
ITU-T G.854.6	Computational viewpoint for trail management
ITU-T M.3000	Overview of TMN recommendations
ITU-T M.3010	Principles for a telecommunications management network

Standard/Protocol	Name
ITU-T M.3013	Considerations for a telecommunications management network
ITU-T M.3017	Framework for the integrated management of hybrid circuit/packet networks
ITU-T M.3020	TMN interface specification methodology
ITU-T M.3100	Generic network information model
ITU-T M.3101	Managed Object Conformance statements for the generic network information model
ITU-T M.3180	Catalogue of TMN management information
ITU-T M.3200	TMN management services and telecommunications managed areas: overview
ITU-T M.3300	TMN F interface requirements
ITU-T M.3400	TMN management functions
ITU-T X.720	Management information model
ITU-T X.721	Definition of management information
ITU-T X.722	Guidelines for the definition of managed objects
ITU-T X.733	Information technology - Open Systems Interconnection - Systems Management: alarm reporting function
ITU-T X.735	Information technology - Open Systems Interconnection - Systems Management: log control function
ITU-T X.903	Information technology - Open distributed processing - Reference Model: architecture
ITU-T Y.1701	Common equipment management function requirements
M.3016.0	Security for the management plane: Overview
M.3016.1	Security for the management plane: Security requirements
M.3016.2	Security for the management plane: Security services
M.3016.3	Security for the management plane: Security mechanism
M.3016.4	Security for the management plane: Profile proforma
M.3703	Common management services - Alarm management - Protocol neutral requirements and analysis

Standard/Protocol	Name
MEF 15	Requirements for Management of Metro Ethernet Phase 1 Network Elements
Rational Unified Process 5.5	Rational Unified Process
RFC793	Transmission Control Protocol (Darpa Internet Program Protocol Specification)
RFC1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1212	Concise MIB Definitions
RFC1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1215	A Convention for Defining Traps for use with the SNMP
RFC1905	Protocol Operations for Version 2 of the Simple Network Management Protocol
RFC1906	Transport Mappings for Version 2 of the Simple Network Management Protocol
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol
RFC1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC2012	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC2013	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC2396	Uniform Resource Identifiers (URL)
RFC2544	Benchmarking Methodology for Network Interconnect Devices
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol

Standard/Protocol	Name
RFC2576	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC2578	Structure of Management Information Version 2 (SMIv2)
RFC2579	Textual Conventions for SMIv2
RFC2580	Conformance Statements for SMIv2
RFC2616	Hypertext Transfer Protocol -- HTTP/1.1
RFC2617	HTTP- Authentication: Basic and Digest Access Authentication
RFC2818	HTTP Over TLS (HTTPS)
RFC2890	Key and Sequence Number Extensions to GRE
RFC3164	The BSD syslog Protocol
RFC3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413	Simple Network Management Protocol (SNMP) Applications
RFC3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC4271	A Border Gateway Protocol 4 (BGP-4)
RFC4346	Transport Layer Security (TLS) Protocol Version 1.1
RFC5246	Transport Layer Security (TLS) Protocol Version 1.2
RFC6241	Network Configuration Protocol (NETCONF)
RFC8040	RESTCONF Protocol

Standard/Protocol	Name
OpenStack.GBP	The Group-based Policy (GBP) abstractions for OpenStack provide an intent-driven declarative policy model that presents simplified application-oriented interfaces to the user.
RFC7951	JSON Encoding of Data Modeled with YANG
RFC7936	Clarifying Registry Procedures for the WebSocket Subprotocol Name Registry
RFC6455	The WebSocket Protocol
RFC8259	The JavaScript Object Notation (JSON) Data Interchange Format
RFC6020	YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)
W3C.REC-eventsource-20150203	Server-Sent Events, a server push technology enabling a browser to receive automatic updates from a server via HTTP connection.
RFC8340	YANG Tree Diagrams
RFC8199	YANG Module Classification
RFC8071	NETCONF Call Home and RESTCONF Call Home
RFC7950	The YANG 1.1 Data Modeling Language
RFC5277	NETCONF Event Notifications
RFC4880	OpenPGP is the most widely used email encryption standard. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a Proposed Standard in RFC 4880. OpenPGP was originally derived from the PGP software, created by Phil Zimmermann.
RFC7047	OVSDB Management Protocol
RFC3173	InMon Corporation's sFlow
RFC4627	JavaScript Object Notation (JSON)
RFC2460	Internet Protocol, Version 6 (IPv6)
RFC5988	Internet Engineering Task Force (IETF)
draft-ietf-secsh-filexfer-13	sftp draft
RFC4253	The Secure Shell (SSH) Transport Layer Protocol
RFC1157	A Simple Network Management Protocol (SNMP)



Standard/Protocol	Name
RFC1902	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
draft-ietf-ccamp-alarm-module-01	This document defines a YANG [RFC7950] module for alarm management.
SSE	Server-Sent Events
RFC1951	DEFLATE Compressed Data Format
RFC2096	IP Forwarding Table MIB
RFC2328	OSPF Version 2
RFC2784	Generic Routing Encapsulation (GRE)
RFC3101	The OSPF Not-So-Stubby Area (NSSA) Option
RFC3509	Alternative Implementations of OSPF Area Border Routers
RFC3623	Graceful OSPF Restart
RFC3630	Traffic Engineering (TE) Extensions to OSPF Version 2
RFC4203	OSPF Extensions in Support of Generalized Multi-Protocol Label Switching
RFC4940	IANA Considerations for OSPF
RFC5250	The OSPF Opaque LSA Option
draft-ietf-pce-gmpls-pcep-extensions-09	PCEP extensions for GMPLS
draft-ietf-pce-pce-initiated-lsp-04	PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model
draft-ietf-pce-pcep-stateful-pce-gmpls-03	Path Computation Element (PCE) Protocol Extensions for Stateful PCE Usage in GMPLS-controlled Networks
draft-ietf-pce-stateful-pce-11	PCEP Extensions for Stateful PCE
RFC8282	draft-ietf-pce-inter-layer-ext-00/Extensions to the Path Computation Element Communication Protocol (PCEP) for Inter-Layer MPLS and GMPLS Traffic Engineering
RFC4674	Requirements for Path Computation Element (PCE) Discovery

Standard/Protocol	Name
RFC5541	Encoding of Objective Functions in the Path Computation Element Communication Protocol (PCEP)
RFC2890	Key and Sequence Number Extensions to GRE
RFC5088	OSPF Protocol Extensions for Path Computation Element (PCE) Discovery
draft-ietf-pce-remote-initiated-gmpls-lsp-04	Path Computation Element Communication Protocol (PCEP) Extensions for remote-initiated GMPLS LSP Setup
RFC8453	ACTN Architecture
RFC7895	YANG Library
RFC8342	NMDA 1.1
draft-ietf-netconf-subscribed-notifications-20	ietf-subscribed-notifications
draft-ietf-netconf-yang-push-14	ietf-yang-push
RFC8345	ietf-network, ietf-network-topology
draft-ietf-teas-yang-te-topo-15	ietf-te-topology
draft-ietf-ccamp-otn-topo-yang-03	ietf-otn-topology
draft-zheng-ccamp-client-topo-yang-02	ietf-eth-te-topology
draft-ietf-teas-yang-te-14	ietf-te, ietf-te-types, ietf-te-mpls-types
draft-ietf-ccamp-wson-tunnel-model-00	ietf-wson-tunnel
draft-ietf-ccamp-otn-tunnel-model-02	ietf-otn-tunnel, ietf-otn-types
draft-zheng-ccamp-client-tunnel-yang-04	ietf-eth-te-tunnel
draft-busizheng-teas-mpls-tp-yang-00	ietf-mpls-tp-tunnel, ietf-mpls-tp-types
draft-zheng-ccamp-client-signal-yang-06	ietf-trans-client-service, ietf-eth-tran-service, ietf-eth-tran-types

Standard/Protocol	Name
draft-ietf-ccamp-wson-yang-10	ietf-te-wson-types
RFC8072	ietf-yang-patch
RFC8231	Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE
RFC8281	Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model
draft-ietf-spring-segment-routing-policy-03	Segment Routing Policy Architecture
draft-ietf-idr-segment-routing-te-policy-07	Advertising Segment Routing Policies in BGP
draft-ietf-idr-te-lsp-distribution-11	Distribution of Traffic Engineering (TE) Policies and State using BGP-LS
draft-ietf-idr-tunnel-encaps-12	The BGP Tunnel Encapsulation Attribute
draft-ietf-idr-bgp-ls-segment-routing-ext-16	BGP Link-State extensions for Segment Routing
draft-ietf-idr-te-pm-bgp-18	BGP-LS Advertisement of IGP Traffic Engineering Performance Metric Extensions
RFC4655	A Path Computation Element (PCE) Based Architecture
RFC4657	Path Computation Element (PCE) Communication Protocol Generic Requirements
RFC5440	Path Computation Element (PCE) Communication Protocol (PCEP)
RFC5521	Extensions to the Path Computation Element Communication Protocol (PCEP) for Route Exclusions
RFC7752	North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP
draft-ietf-idr-bgp-ls-segment-routing-ext-08	BGP Link-State extensions for Segment Routing
RFC4724	Graceful Restart Mechanism for BGP
RFC8232	Optimizations of Label Switched Path State Synchronization Procedures for a Stateful PCE
RFC8408	Conveying Path Setup Type in PCE Communication Protocol (PCEP) Messages

Standard/Protocol	Name
RFC8051	Applicability of a Stateful Path Computation Element (PCE)
RFC7470	Conveying Vendor-Specific Constraints in the Path Computation Element Communication Protocol
RFC7896	Update to the Include Route Object (IRO) Specification in the Path Computation Element Communication Protocol (PCEP)
RFC8402	Segment Routing Architecture
draft-ietf-pce-segment-routing-12	PCEP Extensions for Segment Routing
draft-minei-pce-association-group-04	PCEP Extensions for Establishing Relationships Between Sets of LSPs
draft-ietf-pce-association-group-06	PCEP Extensions for Establishing Relationships Between Sets of LSPs
draft-sivabalan-pce-binding-label-sid-06	Carrying Binding Label/Segment-ID in PCE-based Networks
draft-li-idr-flowspec-rpd-04	BGP Extensions for Routing Policy Distribution (RPD)
RFC5575	Dissemination of Flow Specification Rules
draft-ietf-pce-stateful-path-protection-02	PCEP Extensions for Associating Working and Protection LSPs with Stateful PCE
RFC 6991	Common YANG Data Types
ISO/IEC 20922:2016	Information technology -- Message Queuing Telemetry Transport (MQTT) v3.1.1
WT385	bbf xpon models yang
TR-383a1	bbf-forwarding,sub-interfaces
RFC7317	YANG for System Management
RFC 6470	NETCONF Base Notifications
RFC 791	Internet Protocol
RFC 2697	A Single Rate Three Color Marker
RFC 2698	A Two Rate Three Color Marker
RFC 2863	The Interfaces Group MIB
RFC 3164	The BSD Syslog Protocol

Standard/Protocol	Name
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. SNMP-FRAMEWORK-MIB.SnmpAdminString
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) SNMPv2-MIB.sysContact
RFC 3419	Textual Conventions for Transport Addresses
RFC 3433	Entity Sensor Management Information Base
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC 4007	IPv6 Scoped Address Architecture
RFC 4268	Entity State MIB
RFC 4291	IP Version 6 Addressing Architecture
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 5277	An Architecture for Describing Simple Network
RFC 5424	The Syslog Protocol
RFC 5426	Transmission of Syslog Messages over UDP
RFC 5519	description of object xxxInterfaceVersion
RFC 5656	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
RFC 5952	A Recommendation for IPv6 Address Text Representation

Standard/Protocol	Name
RFC 6234	US Secure Hash Algorithms
RFC 6241	Network Configuration Protocol
RFC 6536	Network Configuration Protocol (NETCONF) Access Control Model
RFC 6557	Procedures for Maintaining the Time Zone Database
RFC 6933	Entity MIB (Version 4)
RFC 7217	A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)
RFC 7223	A YANG Data Model for Interface Management
RFC 7224	IANA Interface Type YANG Module
RFC 7277	A YANG Data Model for IP Management
RFC 7317	A YANG Data Model for System Management
RFC 7407	A YANG Data Model for SNMP Configuration
RFC 8022	A YANG Data Model for Routing Management
RFC 8348	A YANG Data Model for Hardware Management
GR831	Operations Application Messages – Language for Operations Application Messages
RFC2662	Definitions of Managed Objects for the ADSL Lines
RFC4706	Definitions of Managed Objects for Asymmetric Digital Subscriber Line 2 (ADSL2)
SOAP 1.1	Llightweight protocol for exchange of information in a decentralized, distributed environment
WSDL 1.1	W3C Web Services Description Language (WSDL) 1.1
RFC 2571	An Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 2573	SNMP Applications
RFC 2574	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 6455	The WebSocket Protocol

Standard/Protocol	Name
TR-383	Common YANG Modules for Access Networks
TR-385	ITU-T PON YANG Modules
TR-355	YANG Modules for FTTdp Management

## A.2 Glossary

### Numerics

#### 3G

See [Third Generation](#).

#### 802.1Q in 802.1Q (QinQ)

A VLAN feature that allows the equipment to add a VLAN tag to a tagged frame. The implementation of QinQ is to add a public VLAN tag to a frame with a private VLAN tag to allow the frame with double VLAN tags to be transmitted over the service provider's backbone network based on the public VLAN tag. This provides a layer 2 VPN tunnel for customers and enables transparent transmission of packets over private VLANs.

### A

#### ACL

See [Access Control List](#).

#### ADMC

automatically detected and manually cleared

#### ADSL

See [asymmetric digital subscriber line](#).

#### ADSL2+

asymmetric digital subscriber line 2 plus

#### ANCP

See [Access Node Control Protocol](#).

#### API

See [application programming interface](#).

#### APS

automatic protection switching

#### AS

See [autonomous system](#).

#### ASBR

See [autonomous system boundary router](#).

#### ASN.1

See [Abstract Syntax Notation One](#).

#### ASON

automatically switched optical network

#### Abstract Syntax Notation One (ASN. 1)

A syntax notation type employed to specify protocols. Many protocols defined by the ITU-T use this syntax format. Other alternatives are standard text or Augmented Backus-Naur Form (ABNF).

#### Access Control List (ACL)

A list of entities, together with their access rights, which are authorized to access a resource.

#### Access Node Control Protocol (ANCP)

An IP-based protocol that operates between the access node (AN) and the network access server (NAS), over a DSL access and aggregation network.

#### application programming interface (API)

An application programming interface is a particular set of rules and specifications that are used for communication between software programs.

<b>asymmetric digital subscriber line (ADSL)</b>	A technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection. ADSL is asymmetric in that it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. ADSL simultaneously accommodates analog (voice) information on the same line. ADSL is generally offered at downstream data rates from 512 kbit/s to about 6 Mbit/s.
<b>autonomous system (AS)</b>	A network set that uses the same routing policy and is managed by the same technology administration department. Each AS has a unique identifier that is an integer ranging from 1 to 65535. The identifier is assigned by IANA. An AS can be divided into areas.
<b>autonomous system boundary router (ASBR)</b>	A router that exchanges routing information with other autonomous system boundary routers.
<b>B</b>	
<b>B/S</b>	Browser/Server
<b>BFD</b>	See <a href="#">Bidirectional Forwarding Detection</a> .
<b>BGP</b>	Border Gateway Protocol
<b>BIOS</b>	See <a href="#">basic input/output system</a> .
<b>BITS</b>	See <a href="#">building integrated timing supply</a> .
<b>BOD</b>	bandwidth on demand
<b>BRA</b>	See <a href="#">basic rate access</a> .
<b>BRAS</b>	See <a href="#">broadband remote access server</a> .
<b>BSS</b>	Business Support System
<b>BWS</b>	backbone wavelength division multiplexing system
<b>Bidirectional Forwarding Detection (BFD)</b>	A fast and independent hello protocol that delivers millisecond-level link failure detection and provides carrier-class availability. After sessions are established between neighboring systems, the systems can periodically send BFD packets to each other. If one system fails to receive a BFD packet within the negotiated period, the system regards that the bidirectional link fails and instructs the upper layer protocol to take actions to recover the faulty link.
<b>basic input/output system (BIOS)</b>	Firmware stored on the computer motherboard that contains basic input/output control programs, power-on self test (POST) programs, bootstraps, and system setting information. The BIOS provides hardware setting and control functions for the computer.
<b>basic rate access (BRA)</b>	An ISDN interface typically used by smaller sites and customers. This interface consists of a single 16 kbit/s data (or "D") channel plus two bearer (or "B") channels for voice and/or data. Also known as Basic Rate Access, or BRI.



**broadband remote access server (BRAS)** A new type of access gateway for broadband networks. As a bridge between backbone networks and broadband access networks, BRAS provides methods for fundamental access and manages the broadband access network. It is deployed at the edge of network to provide broadband access services, convergence, and forwarding of multiple services, meeting the demands for transmission capacity and bandwidth utilization of different users. BRAS is a core device for the broadband users' access to a broadband network.

**building integrated timing supply (BITS)** In the situation of multiple synchronous nodes or communication devices, one can use a device to set up a clock system on the hinge of telecom network to connect the synchronous network as a whole, and provide satisfactory synchronous base signals to the building integrated device. This device is called BITS.

## C

**CAS** See [Central Authentication Service](#).

**CBU** See [cellular backhaul unit](#).

**CC** See [continuity check](#).

**CCC** circuit cross connect

**CES** See [circuit emulation service](#).

**CIR** committed information rate

**CLEI** common language equipment identification

**CLI** See [command-line interface](#).

**CORBA** See [Common Object Request Broker Architecture](#).

**CPE** See [customer-premises equipment](#).

**CPU** See [Central Processing Unit](#).

**CSV** See [comma separated values](#).

**Central Authentication Service (CAS)** A single sign-on protocol for the web. Its purpose is to permit users to access multiple applications by providing their credentials (such as user names and passwords) only once. It also allows web applications to authenticate users without gaining access to the users' security credentials (such as passwords). CAS also refers to a software package that implements this protocol.

**Central Processing Unit (CPU)** The computational and control unit of a computer. The CPU is the device that interprets and executes instructions. The CPU has the ability to fetch, decode, and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus.

<b>Common Object Request Broker Architecture (CORBA)</b>	A specification developed by the Object Management Group in 1992 in which pieces of programs (objects) communicate with other objects in other programs, even if the two programs are written in different programming languages and are running on different platforms. A program makes its request for objects through an object request broker, or ORB, and therefore does not need to know the structure of the program from which the object comes. CORBA is designed to work in object-oriented environments.
<b>Coordinated Universal Time (UTC)</b>	The world-wide scientific standard of timekeeping. It is based upon carefully maintained atomic clocks and is kept accurate to within microseconds worldwide.
<b>cellular backhaul unit (CBU)</b>	A network access unit used for access base transceiver stations. It provides Ethernet, IP, and TDM services; has multiple Ethernet and 1PPS+ToD interfaces and optionally E1 interfaces. It is mainly applicable to backhaul in mobile base transceiver stations.
<b>circuit emulation service (CES)</b>	A function with which the E1/T1 data can be transmitted through ATM networks. At the transmission end, the interface module packs timeslot data into ATM cells. These ATM cells are sent to the reception end through the ATM network. At the reception end, the interface module re-assigns the data in these ATM cells to E1/T1 timeslots. The CES technology guarantees that the data in E1/T1 timeslots can be recovered to the original sequence at the reception end.
<b>comma separated values (CSV)</b>	A CSV file is a text file that stores data, generally used as an electronic table or by the database software.
<b>command-line interface (CLI)</b>	A means of communication between a program and its user, based solely on textual input and output. Commands are input with the help of a keyboard or similar device and are interpreted and executed by the program. Results are output as text or graphics to the terminal.
<b>continuity check (CC)</b>	An Ethernet connectivity fault management (CFM) method used to detect the connectivity between MEPs by having each MEP periodically transmit a Continuity Check Message (CCM).
<b>customer-premises equipment (CPE)</b>	Customer-premises equipment or customer-provided equipment (CPE) is any terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point ("demarc"). The demarc is a point established in a building or complex to separate customer equipment from the equipment located in either the distribution infrastructure or central office of the communications service provider. CPE generally refers to devices such as telephones, routers, network switches, residential gateways (RG), set-top boxes, fixed mobile convergence products, home networking adapters and Internet access gateways that enable consumers to access communications service providers' services and distribute them around their house via a local area network (LAN).
<b>D</b>	
<b>DB</b>	database
<b>DC</b>	data center

<b>DCC</b>	data communication channel
<b>DCI</b>	See <a href="#">Data Center Interconnect</a> .
<b>DCM</b>	See <a href="#">dispersion compensation module</a> .
<b>DCN</b>	See <a href="#">data communication network</a> .
<b>DDoS</b>	See <a href="#">distributed denial of service</a> .
<b>DSLAM</b>	See <a href="#">digital subscriber line access multiplexer</a> .
<b>DWDM</b>	See <a href="#">dense wavelength division multiplexing</a> .
<b>Data Center Interconnect (DCI)</b>	DCI refers to network interconnection between two data centers for cross-DC service transmission and migration.
<b>DoS</b>	See <a href="#">denial of service</a> .
<b>data communication network (DCN)</b>	A communication network used in a TMN or between TMNs to support the data communication function.
<b>denial of service (DoS)</b>	DoS attack is used to attack a system by sending a large number of data packets. As a result, the system cannot receive requests from the valid users or the host is suspended and cannot work normally. DoS attack includes SYN flood, Fraggle, and others. The DoS attacker only stops the valid user from accessing resources or devices instead of searching for the ingresses of the intranet.
<b>dense wavelength division multiplexing (DWDM)</b>	The technology that utilizes the characteristics of broad bandwidth and low attenuation of single mode optical fiber, employs multiple wavelengths with specific frequency spacing as carriers, and allows multiple channels to transmit simultaneously in the same fiber.
<b>digital subscriber line access multiplexer (DSLAM)</b>	A network device, usually situated in the main office of a telephone company, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and uses multiplexing techniques to put these signals on a high-speed backbone line.
<b>dispersion compensation module (DCM)</b>	A type of module that contains dispersion compensation fibers to compensate for the dispersion of the transmitting fiber.
<b>distributed denial of service (DDoS)</b>	Distributed Denial of Service attack is one in which a multitude of compromised systems attack a single target, therefore causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially and occupies the resources of it, therefore denying services to legitimate users.
<b>E</b>	
<b>E-LAN</b>	See <a href="#">Ethernet local area network</a> .
<b>E-Line</b>	See <a href="#">Ethernet line</a> .
<b>E2E</b>	end to end
<b>ECC</b>	See <a href="#">embedded control channel</a> .
<b>EDFA</b>	See <a href="#">erbium-doped fiber amplifier</a> .
<b>EPL</b>	See <a href="#">Ethernet private line</a> .

<b>EPON</b>	See <a href="#">Ethernet passive optical network</a> .
<b>EVPL</b>	See <a href="#">Ethernet virtual private line</a> .
<b>EoO</b>	Ethernet over OTN
<b>EoW</b>	Ethernet over WDM
<b>Ethernet line (E-Line)</b>	A type of Ethernet service that is based on a point-to-point EVC (Ethernet virtual connection).
<b>Ethernet local area network (E-LAN)</b>	A type of Ethernet service that is based on a multipoint-to-multipoint EVC (Ethernet virtual connection).
<b>Ethernet passive optical network (EPON)</b>	An Ethernet Passive Optical Network (EPON) is a passive optical network based on Ethernet. It is a new generation broadband access technology that uses a point-to-multipoint structure and passive fiber transmission. It supports upstream/downstream symmetrical rates of 1.25 Gbit/s and a reach distance of up to 20 km. In the downstream direction, the bandwidth is shared based on encrypted broadcast transmission for different users. In the upstream direction, the bandwidth is shared based on TDM. EPON meets the requirements for high bandwidth.
<b>Ethernet private line (EPL)</b>	A type of Ethernet service provided by SDH, PDH, ATM, or MPLS server layer networks. This service is carried over dedicated bandwidth between point-to-point connections.
<b>Ethernet virtual private line (EVPL)</b>	A type of Ethernet service provided by SDH, PDH, ATM, or MPLS server layer networks. This service is carried over shared bandwidth between point-to-point connections.
<b>embedded control channel (ECC)</b>	A logical channel that uses a data communications channel (DCC) as its physical layer to enable the transmission of operation, administration, and maintenance (OAM) information between NEs.
<b>erbium-doped fiber amplifier (EDFA)</b>	An optical device that amplifies optical signals. This device uses a short optical fiber doped with the rare-earth element, Erbium. The signal to be amplified and a pump laser are multiplexed into the doped fiber, and the signal is amplified by interacting with doping ions. When the amplifier passes an external light source pump, it amplifies the optical signals in a specific wavelength range.
<b>F</b>	
<b>FCAPS</b>	fault, configuration, accounting, performance, security
<b>FDN</b>	fixed dialing number
<b>FIB</b>	See <a href="#">forwarding information base</a> .
<b>FPGA</b>	See <a href="#">field programmable gate array</a> .
<b>FRR</b>	See <a href="#">fast reroute</a> .
<b>FTP</b>	See <a href="#">File Transfer Protocol</a> .
<b>FTTB</b>	See <a href="#">fiber to the building</a> .
<b>FTTC</b>	See <a href="#">fiber to the curb</a> .
<b>FTTH</b>	See <a href="#">fiber to the home</a> .

<b>File Transfer Protocol (FTP)</b>	A member of the TCP/IP suite of protocols, used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.
<b>fast reroute (FRR)</b>	A technology which provides a temporary protection of link availability when part of a network fails. The protocol enables the creation of a standby route or path for an active route or path. When the active route is unavailable, the traffic on the active route can be switched to the standby route. When the active route is recovered, the traffic can be switched back to the active route. FRR is categorized into IP FRR, VPN FRR, and TE FRR.
<b>fiber to the building (FTTB)</b>	A fiber-based networking scenario. There are two types of FTTB scenarios: multi-dwelling unit (MDU) and business buildings. Each scenario includes the following service types: FTTB to the MDU and FTTB to the business buildings.
<b>fiber to the curb (FTTC)</b>	A fiber-based networking scenario. The FTTC scenario provides the following services: asymmetric broadband services (such as digital broadcast service, VOD, file download, and online gaming), symmetric broadband services (such as content broadcast, email, file exchange, distance education, and distance medical care), POTS, ISDN, and xDSL backhaul services.
<b>fiber to the home (FTTH)</b>	A fiber-based networking scenario. The FTTH scenario provides the following services: asymmetric broadband services (digital broadcast service, VoD, file download, and online gaming), symmetric broadband services (content broadcast, email, file exchange, distance education, and distance medical care), POTS, and ISDN services.
<b>field programmable gate array (FPGA)</b>	A semi-customized circuit that is used in the Application Specific Integrated Circuit (ASIC) field and developed based on programmable components. FPGA remedies many of the deficiencies of customized circuits, and allows the use of many more gate arrays.
<b>forwarding information base (FIB)</b>	A table that provides information for network hardware (bridges and routers) for them to forward data packets to other networks. The information contained in a routing table differs according to whether it is used by a bridge or a router. A bridge relies on both the source (originating) and destination addresses to determine where and how to forward a packet.
<b>G</b>	
<b>GNE</b>	See <a href="#">gateway network element</a> .
<b>GPON</b>	gigabit-capable passive optical network
<b>GRE</b>	See <a href="#">Generic Routing Encapsulation</a> .
<b>GUI</b>	See <a href="#">graphical user interface</a> .
<b>Generic Routing Encapsulation (GRE)</b>	A mechanism for encapsulating any network layer protocol over any other network. GRE is used for encapsulating IP datagrams tunneled through the Internet. GRE serves as a Layer 3 tunneling protocol and provides a tunnel for transparently transmitting data packets.
<b>gateway network element (GNE)</b>	An NE that serves as a gateway for other NEs to communicate with a network management system.

<b>graphical user interface (GUI)</b>	A visual computer environment that represents programs, files, and options with graphical images, such as icons, menus, and dialog boxes, on the screen.
<b>H</b>	
<b>HA</b>	See <a href="#">high availability</a> .
<b>HFC</b>	See <a href="#">high-level foundation classes</a> .
<b>HMAC</b>	See <a href="#">hash-based message authentication code</a> .
<b>HQoS</b>	See <a href="#">hierarchical quality of service</a> .
<b>HSL</b>	See <a href="#">high-level script language</a> .
<b>HTML</b>	Hypertext Markup Language
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	See <a href="#">Hypertext Transfer Protocol Secure</a> .
<b>HVPLS</b>	hierarchical virtual private LAN service
<b>Hypertext Transfer Protocol Secure (HTTPS)</b>	An HTTP protocol that runs on top of transport layer security (TLS) and Secure Sockets Layer (SSL) for secured transactions. It is used to establish a reliable channel for encrypted communication and secure identification of a network web server. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.
<b>hash-based message authentication code (HMAC)</b>	In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
<b>hierarchical quality of service (HQoS)</b>	A type of QoS that controls the traffic of users and performs the scheduling according to the priority of user services. HQoS has an advanced traffic statistics function, and the administrator can monitor the usage of bandwidth of each service. Hence, the bandwidth can be allocated reasonably through traffic analysis.
<b>high availability (HA)</b>	A scheme in which two modules operate in active/standby mode to achieve high availability. When the active module fails, the standby module automatically takes over the system functions of the active module.
<b>high-level foundation classes (HFC)</b>	A group of encapsulated function databases provided by the iSStar. You can use the provided functions to accelerate script editing.
<b>high-level script language (HSL)</b>	A script language. Based on python, the HSL syntax is simple, clear, and extendable.

## I

<b>IANA</b>	See <a href="#">Internet Assigned Numbers Authority</a> .
<b>ICMP</b>	See <a href="#">Internet Control Message Protocol</a> .
<b>IDC</b>	See <a href="#">Internet Data Center</a> .
<b>IDN</b>	See <a href="#">integrated digital network</a> .
<b>IETF</b>	Internet Engineering Task Force
<b>IGP</b>	See <a href="#">Interior Gateway Protocol</a> .
<b>IOPS</b>	input/output operations per second
<b>IP</b>	See <a href="#">Internet Protocol</a> .
<b>IP RAN</b>	See <a href="#">IP radio access network</a> .
<b>IP radio access network (IP RAN)</b>	A network that uses IP technology to achieve data backhaul on a radio access network.
<b>IPTV</b>	See <a href="#">Internet Protocol television</a> .
<b>IPv4</b>	See <a href="#">Internet Protocol version 4</a> .
<b>IPv6</b>	See <a href="#">Internet Protocol version 6</a> .
<b>ISDN</b>	Integrated Services Digital Network
<b>ISP</b>	See <a href="#">Internet service provider</a> .
<b>ITU-T</b>	International Telecommunication Union-Telecommunication Standardization Sector
<b>Interior Gateway Protocol (IGP)</b>	A routing protocol that is used within an autonomous system. The IGP runs in small-sized and medium-sized networks. The IGPs are RIP, IGRP, EIGRP, OSPF, and IS-IS.
<b>Internet Assigned Numbers Authority (IANA)</b>	A department operated by the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
<b>Internet Control Message Protocol (ICMP)</b>	A network layer protocol that provides message control and error reporting between a host server and an Internet gateway.
<b>Internet Data Center (IDC)</b>	The telecommunications sector uses available Internet communication lines and bandwidth resources to establish a standard and carrier-class equipment environment in which comprehensive services such as server hosting, renting, and other value-added services are provided for enterprises and governments.

<b>Internet Protocol (IP)</b>	The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network and station, and the reassembly of the packets into the original data messages at the destination. IP runs at the internetwork layer in the TCP/IP model—equivalent to the network layer in the ISO/OSI reference model. The IP provides a connectionless datagram network layer and allows an application to communicate transparently across several connected networks.
<b>Internet Protocol television (IPTV)</b>	A system that provides TV services over the IP network. In the IPTV system, media streams from satellites, terrestrial, and studios are converted by the encoder to the media streams applicable to the IP network. Then the media streams are transmitted to the terminal layer on the IP network. Media content is displayed on a TV set after media streams are processed by specified receiving devices (for example, an STB).
<b>Internet Protocol version 4 (IPv4)</b>	The current version of the Internet Protocol (IP). IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each IPv4 address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.
<b>Internet Protocol version 6 (IPv6)</b>	An update version of IPv4, which is designed by the Internet Engineering Task Force (IETF) and is also called IP Next Generation (IPng). It is a new version of the Internet Protocol. The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits.
<b>Internet service provider (ISP)</b>	An organization that offers users access to the Internet and related services.
<b>integrated digital network (IDN)</b>	A set of digital nodes and digital links that uses integrated digital transmission and switches to provide digital connections between two or more defined points.
<b>K</b>	
<b>KPI</b>	key performance indicator
<b>L</b>	
<b>L2VPN</b>	Layer 2 virtual private network
<b>L3VPN</b>	Layer 3 virtual private network
<b>LAG</b>	See <a href="#">link aggregation group</a> .
<b>LAN</b>	See <a href="#">local area network</a> .
<b>LB</b>	See <a href="#">loopback</a> .
<b>LLDP</b>	See <a href="#">Link Layer Discovery Protocol</a> .
<b>LSA</b>	link-state advertisement
<b>LSR</b>	See <a href="#">label switching router</a> .



<b>LTE</b>	See <a href="#">Long Term Evolution</a> .
<b>Link Layer Discovery Protocol (LLDP)</b>	The Link Layer Discovery Protocol (LLDP) is an L2D protocol defined in IEEE 802.1ab. Using the LLDP, the NMS can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand.
<b>Long Term Evolution (LTE)</b>	LTE, an abbreviation for Long-Term Evolution, commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using a different radio interface together with core network improvements.[1][2] The standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9.
<b>label switching router (LSR)</b>	Basic element of an MPLS network. All LSRs support the MPLS protocol. The LSR is composed of two parts: control unit and forwarding unit. The former is responsible for allocating the label, selecting the route, creating the label forwarding table, creating and removing the label switch path; the latter forwards the labels according to groups received in the label forwarding table.
<b>link aggregation group (LAG)</b>	An aggregation that allows one or more links to be aggregated together to form a link aggregation group so that a MAC client can treat the link aggregation group as if it were a single link.
<b>local area network (LAN)</b>	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building, featuring high speed and low error rate. Current LANs are generally based on switched Ethernet or Wi-Fi technology and run at 1,000 Mbit/s (that is, 1 Gbit/s).
<b>loopback (LB)</b>	A troubleshooting technique that returns a transmitted signal to its source so that the signal or message can be analyzed for errors. The loopback can be a inloop or outloop.
<b>M</b>	
<b>MA</b>	maintenance association
<b>MAC</b>	See <a href="#">Media Access Control</a> .
<b>MBB</b>	mobile broadband
<b>MD</b>	See <a href="#">maintenance domain</a> .
<b>MD5</b>	See <a href="#">message digest algorithm 5</a> .
<b>MDF</b>	See <a href="#">main distribution frame</a> .
<b>MDU</b>	See <a href="#">multi-dwelling unit</a> .
<b>ME</b>	See <a href="#">managed element</a> .
<b>MEP</b>	maintenance association end point
<b>MIB</b>	See <a href="#">management information base</a> .
<b>MIP</b>	maintenance association intermediate point
<b>MO</b>	managed object
<b>MOS</b>	mean opinion score

<b>MPLS</b>	See <a href="#">Multiprotocol Label Switching</a> .
<b>MPLS VPN</b>	See <a href="#">multiprotocol label switching virtual private network</a> .
<b>MS-PW</b>	See <a href="#">multi-segment pseudo wire</a> .
<b>MSAN</b>	multiservice access node
<b>MSTP</b>	See <a href="#">multi-service transmission platform</a> .
<b>MTOSI</b>	Multi-Technology Operations System Interface
<b>MTTR</b>	See <a href="#">Mean Time to Repair</a> .
<b>Mean Time to Repair (MTTR)</b>	The average time that a device will take to recover from a failure.
<b>Media Access Control (MAC)</b>	A protocol at the media access control sublayer. The protocol is at the lower part of the data link layer in the OSI model and is mainly responsible for controlling and connecting the physical media at the physical layer. When transmitting data, the MAC protocol checks whether to be able to transmit data. If the data can be transmitted, certain control information is added to the data, and then the data and the control information are transmitted in a specified format to the physical layer. When receiving data, the MAC protocol checks whether the information is correct and whether the data is transmitted correctly. If the information is correct and the data is transmitted correctly, the control information is removed from the data and then the data is transmitted to the LLC layer.
<b>Multiprotocol Label Switching (MPLS)</b>	A technology that uses short tags of fixed length to encapsulate packets in different link layers, and provides connection-oriented switching for the network layer on the basis of IP routing and control protocols.
<b>main distribution frame (MDF)</b>	A device at a central office, on which all local loops are terminated.
<b>maintenance domain (MD)</b>	The network or the part of the network for which connectivity is managed by connectivity fault management (CFM). The devices in a maintenance domain are managed by a single Internet service provider (ISP).
<b>managed element (ME)</b>	A particular entity or resource in a networked system environment. It can also represent a physical piece of equipment on the network, the components of the device on the network, or parts of the network itself.
<b>management information base (MIB)</b>	A type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
<b>message digest algorithm 5 (MD5)</b>	A hash function that is used in a variety of security applications to check message integrity. MD5 processes a variable-length message into a fixed-length output of 128 bits. It breaks up an input message into 512-bit blocks (sixteen 32-bit little-endian integers). After a series of processing, the output consists of four 32-bit words, which are then cascaded into a 128-bit hash number.
<b>multi-dwelling unit (MDU)</b>	A network access unit used for multi-dwelling units. It provides Ethernet and IP services and optionally VoIP or CATV services; has multiple broadband interfaces on the user side and optionally POTS ports or CATV RF ports. It is mainly applicable to FTTB, FTTC, or FTTCab networks.

<b>multi-segment pseudo wire (MS-PW)</b>	A collection of multiple adjacent PW segments. Each PW segment is a point-to-point PW. The use of MS-PWs to bear services saves tunnel resources and can transport services over different networks.
<b>multi-service transmission platform (MSTP)</b>	A platform based on the SDH platform, capable of accessing, processing and transmitting TDM services, ATM services, and Ethernet services, and providing unified management of these services.
<b>multiprotocol label switching virtual private network (MPLS VPN)</b>	An Internet Protocol (IP) virtual private network (VPN) based on the multiprotocol label switching (MPLS) technology. It applies the MPLS technology for network routers and switches, simplifies the routing mode of core routers, and combines traditional routing technology and label switching technology. It can be used to construct the broadband Intranet and Extranet to meet various service requirements.
<b>N</b>	
<b>NBI</b>	See <a href="#">northbound interface</a> .
<b>NE</b>	See <a href="#">network element</a> .
<b>NETCONF</b>	See <a href="#">Network Configuration Protocol</a> .
<b>NGFW</b>	See <a href="#">Next-Generation Firewall</a> .
<b>NML</b>	See <a href="#">network management layer</a> .
<b>NMS</b>	See <a href="#">network management system</a> .
<b>NNI</b>	network node interface
<b>NSAP</b>	See <a href="#">network service access point</a> .
<b>NT1</b>	See <a href="#">network termination 1</a> .
<b>NTP</b>	See <a href="#">Network Time Protocol</a> .
<b>Network Configuration Protocol (NETCONF)</b>	NETCONF is the communication management protocol. It uses XML-based data encoding for the configuration data and protocol messages, and provides a mechanism for installing, operating, and deleting NEs.
<b>Network Time Protocol (NTP)</b>	The Network Time Protocol (NTP) defines the time synchronization mechanism. It synchronizes the time between the distributed time server and the client.
<b>Next-Generation Firewall (NGFW)</b>	The Next Generation Firewall is a line-speed device specific to network security. It integrates intelligent interworking with other network devices, visual application identification and control, and legacy firewall functions, fulfilling the needs of enterprises on network security.
<b>network element (NE)</b>	An entity that contains hardware and software. An NE has at least one main control board that manages and monitors the entire network element. The NE software runs on the main control board.
<b>network management layer (NML)</b>	A management layer which is responsible for the management of network elements on an individual or collective basis.
<b>network management system (NMS)</b>	A system in charge of the operation, administration, and maintenance of a network.

<b>network service access point (NSAP)</b>	A network address defined by ISO, at which the OSI Network Service is made available to a Network service user by the Network service provider.
<b>network termination 1 (NT1)</b>	A type of terminal device that provides U-interface and S/T interface, used to connect the ISDN terminals and ISDN exchange equipment. It mainly performs code switch between the U-interface and the S/T interface, such as the code switch between the 2B1Q and the AMI in Chinese standards. The NT1 mostly work at only the physical layer, without software intelligence; the devices, however, support functions of line maintenance and performance monitoring, and ensure the clock synchronization between the ISDN terminals and the network.
<b>northbound interface (NBI)</b>	An interface that connects to the upper-layer device to provision services and report alarms and performance statistics.
<b>O</b>	
<b>OAM</b>	See <a href="#">operation, administration and maintenance</a> .
<b>OCS</b>	optical core switching
<b>OCh</b>	optical channel with full functionality
<b>ODN</b>	optical distribution network
<b>ODU</b>	Optical channel Data Unit
<b>ODUk</b>	optical channel data unit - k
<b>OLA</b>	optical line amplifier
<b>OLT</b>	optical line terminal
<b>OMS</b>	optical multiplexing section
<b>ONT</b>	See <a href="#">optical network terminal</a> .
<b>ONU</b>	See <a href="#">optical network unit</a> .
<b>OPEX</b>	See <a href="#">operating expense</a> .
<b>OPS</b>	See <a href="#">optical physical section</a> .
<b>OSI</b>	open systems interconnection
<b>OSN</b>	optical switch node
<b>OSNR</b>	See <a href="#">optical signal-to-noise ratio</a> .
<b>OSPF</b>	See <a href="#">Open Shortest Path First</a> .
<b>OSPF-TE</b>	Open Shortest Path First-Traffic Engineering
<b>OSS</b>	operations support system
<b>OTN</b>	optical transport network
<b>OTS</b>	See <a href="#">optical transmission section</a> .
<b>OTT</b>	over the top
<b>Open Shortest Path First (OSPF)</b>	A link-state, hierarchical interior gateway protocol (IGP) for network routing that uses cost as its routing metric. A link state database is constructed of the network topology, which is identical on all routers in the area.

<b>OpenStack</b>	OpenStack is a free and open-source software platform for cloud computing, mostly deployed as infrastructure-as-a-service (IaaS), whereby virtual servers and other resources are made available to customers.[2] The software platform consists of interrelated components that control diverse, multi-vendor hardware pools of processing, storage, and networking resources throughout a data center.
<b>operating expense (OPEX)</b>	An operating expense, operating expenditure, operational expense, operational expenditure or OPEX is an ongoing cost for running a product, business, or system.
<b>operation, administration and maintenance (OAM)</b>	A set of network management functions that cover fault detection, notification, location, and repair.
<b>optical network terminal (ONT)</b>	A device that terminates the fiber optical network at the customer premises.
<b>optical network unit (ONU)</b>	A form of Access Node that converts optical signals transmitted via fiber to electrical signals that can be transmitted via coaxial cable or twisted pair copper wiring to individual subscribers.
<b>optical physical section (OPS)</b>	A network segment in the physical layer of optical network.
<b>optical signal-to-noise ratio (OSNR)</b>	The ratio of signal power to noise power in a transmission link. OSNR is the most important index for measuring the performance of a DWDM system.
<b>optical transmission section (OTS)</b>	A section in the logical structure of an optical transport network (OTN). The OTS allows the network operator to perform monitoring and maintenance tasks between NEs.
<b>P</b>	
<b>P2MP</b>	point-to-multipoint
<b>P2P</b>	See <a href="#">point-to-point service</a> .
<b>PE</b>	See <a href="#">provider edge</a> .
<b>PER</b>	packed encoding rules
<b>PKI</b>	See <a href="#">public key infrastructure</a> .
<b>PMS</b>	performance management system
<b>PON</b>	passive optical network
<b>POTS</b>	See <a href="#">plain old telephone service</a> .
<b>PRA</b>	See <a href="#">primary rate access</a> .
<b>PSN</b>	See <a href="#">packet switched network</a> .
<b>PTN</b>	packet transport network
<b>PVC</b>	permanent virtual channel
<b>PW</b>	See <a href="#">pseudo wire</a> .
<b>PWE3</b>	See <a href="#">Pseudowire Emulation Edge-to-Edge</a> .

<b>Pseudowire Emulation Edge-to-Edge (PWE3)</b>	An end-to-end Layer 2 transmission technology. It emulates the essential attributes of a telecommunication service such as ATM, FR or Ethernet in a packet switched network (PSN). PWE3 also emulates the essential attributes of low speed time division multiplexing (TDM) circuit and SONET/SDH. The simulation approximates to the real situation.
<b>packet switched network (PSN)</b>	A telecommunications network that works in packet switching mode.
<b>plain old telephone service (POTS)</b>	The basic telephone service provided through the traditional cabling such as twisted pair cables.
<b>point-to-point service (P2P)</b>	A service between two terminal users. In P2P services, senders and recipients are terminal users.
<b>primary rate access (PRA)</b>	A standardized ISDN user-network interface structure utilizing the capacity of the primary level of the digital hierarchy, that is, 1544 kbit/s or 2048 kbit/s digit rate. Note: The digit rate of any D-channel in this interface structure is 64 kbit/s.
<b>provider edge (PE)</b>	A device that is located in the backbone network of the MPLS VPN structure. A PE is responsible for managing VPN users, establishing LSPs between PEs, and exchanging routing information between sites of the same VPN. A PE performs the mapping and forwarding of packets between the private network and the public channel. A PE can be a UPE, an SPE, or an NPE.
<b>pseudo wire (PW)</b>	An emulated connection between two PEs for transmitting frames. The PW is established and maintained by PEs through signaling protocols. The status information of a PW is maintained by the two end PEs of a PW.
<b>public key infrastructure (PKI)</b>	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).

## Q

**QinQ** See [802.1Q in 802.1Q](#).

## R

**RAID** redundant array of independent disks

**RAN** See [radio access network](#).

**REG** See [regenerator](#).

**REST** See [Representational State Transfer](#).

**RESTCONF** See [RESTCONF](#).

**RESTCONF (RESTCONF)** An HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in the Network Configuration Protocol (NETCONF).

<b>RESTful</b>	RESTful is a software architecture style rather than a standard. It provides a set of software design guidelines and constraints for designing software for interaction between clients and servers. RESTful software is simpler and more hierarchical, and facilitates the implementation of the cache mechanism.
<b>RFC</b>	See <a href="#">Requirement For Comments</a> .
<b>RFS</b>	resource-facing service
<b>RMEP</b>	remote maintenance association end point
<b>RMON</b>	remote network monitoring
<b>RNC</b>	See <a href="#">radio network controller</a> .
<b>ROADM</b>	reconfigurable optical add/drop multiplexer
<b>RPO</b>	See <a href="#">recovery point objective</a> .
<b>RSVP-TE</b>	See <a href="#">Resource Reservation Protocol-Traffic Engineering</a> .
<b>RTN</b>	radio transmission node
<b>RTO</b>	See <a href="#">recovery time objective</a> .
<b>Representational State Transfer (REST)</b>	Representational State Transfer (REST) is a style of software architecture for distributed systems such as the World Wide Web. REST has emerged as a predominant Web service design model. REST facilitates the transaction between web servers by allowing loose coupling between different services.
<b>Requirement For Comments (RFC)</b>	A document about standards, protocols, or other information pertaining to the operation of the Internet. The RFC, under the control of the Internet Architecture Board (IAB), is actually issued after discussion and serves as a standard document. RFCs can be obtained from sources such as InterNIC.
<b>Resource Reservation Protocol-Traffic Engineering (RSVP-TE)</b>	An extension to the RSVP protocol for setting up label switched paths (LSPs) in MPLS networks. The RSVP-TE protocol is used to establish and maintain the LSPs by initiating label requests and allocating label binding messages. It also supports LSP rerouting and LSP bandwidth increasing.
<b>radio access network (RAN)</b>	The network that provides the connection between CPEs and the CN. It isolates the CN from wireless network.
<b>radio network controller (RNC)</b>	A device in a radio network subsystem that is in charge of controlling the usage and integrity of radio resources.
<b>recovery point objective (RPO)</b>	RPO is a service switchover policy, minimizing data loss during DR switchover. The data recovery point is used as the objective to ensure that the data used for DR switchover is the latest backup data.
<b>recovery time objective (RTO)</b>	A service switchover policy that ensures the shortest switchover time. It tasks the recovery time point as the objective and ensures that the redundancy machine can take over services as quickly as possible.
<b>regenerator (REG)</b>	A piece of equipment or device that regenerates electrical signals.
<b>S</b>	
<b>SAML</b>	See <a href="#">Security Assertion Markup Language</a> .

<b>SAN</b>	See <a href="#">storage area network</a> .
<b>SAS</b>	serial attached SCSI
<b>SBU</b>	See <a href="#">single business unit</a> .
<b>SDH</b>	See <a href="#">synchronous digital hierarchy</a> .
<b>SDN</b>	See <a href="#">software-defined networking</a> .
<b>SFTP</b>	See <a href="#">Secure File Transfer Protocol</a> .
<b>SHDSL</b>	See <a href="#">single-pair high-speed digital subscriber line</a> .
<b>SLA</b>	See <a href="#">Service Level Agreement</a> .
<b>SMTP</b>	See <a href="#">Simple Mail Transfer Protocol</a> .
<b>SN</b>	service node
<b>SNCP</b>	subnetwork connection protection
<b>SNMP</b>	See <a href="#">Simple Network Management Protocol</a> .
<b>SOAP</b>	See <a href="#">Simple Object Access Protocol</a> .
<b>SPE</b>	See <a href="#">superstratum provider edge</a> .
<b>SR</b>	See <a href="#">strict routing</a> .
<b>SRG</b>	See <a href="#">shared risk group</a> .
<b>SRLG</b>	shared risk link group
<b>SSH</b>	See <a href="#">Secure Shell</a> .
<b>SSO</b>	single sign-on
<b>STM</b>	synchronous transfer mode
<b>STM-1</b>	See <a href="#">Synchronous Transport Module level 1</a> .
<b>Secure File Transfer Protocol (SFTP)</b>	A network protocol designed to provide secure file transfer over SSH.
<b>Secure Shell (SSH)</b>	SSH is a set of network protocols for securing connections between computers, as well as the utility suite that implements these protocols.
<b>Security Assertion Markup Language (SAML)</b>	An XML-based open standard for exchanging authentication and authorization data between security domains.
<b>Service Level Agreement (SLA)</b>	A service contract between a customer and a (SLA) service provider that specifies the forwarding service a customer should receive. A customer may be a user organization (source domain) or another DS domain (upstream domain). A SLA may include traffic conditioning rules which constitute a TCA in whole or in part.
<b>Simple Mail Transfer Protocol (SMTP)</b>	The TCP/IP protocol which facilitates the transfer of electronic-mail messages, specifies how two systems are to interact, and the format of messages used to control the transfer of electronic mail.



<b>Simple Network Management Protocol (SNMP)</b>	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by a MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
<b>Simple Object Access Protocol (SOAP)</b>	A type of protocol that is lightweight, simple, and XML-based. It is designed to exchange structured information at web.
<b>Synchronous Transport Module level 1 (STM-1)</b>	Synchronous transfer mode at 155 Mbit/s.
<b>shared risk group (SRG)</b>	A group of resources that share a common risk component whose failure can cause the failure of all the resources in the group.
<b>single business unit (SBU)</b>	A network access unit used for individual enterprise users or individual offices. It functions as a broadband access terminal, provides Ethernet, IP, and TDM services and optionally VoIP services; has Ethernet and E1 interfaces and optionally POTS ports. It is mainly applicable to FTTO networks.
<b>single-pair high-speed digital subscriber line (SHDSL)</b>	A symmetric digital subscriber line technology developed from HDSL, SDSL, and HDSL2, which is defined in ITU-T G.991.2. The SHDSL port is connected to the user terminal through the plain telephone subscriber line and uses trellis coded pulse amplitude modulation (TC-PAM) technology to transmit high-speed data and provide the broadband access service.
<b>software-defined networking (SDN)</b>	Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and given to a software application called a controller.
<b>storage area network (SAN)</b>	A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN does not provide file abstraction, only block-level operations. However, file systems built on top of SANs do provide file-level access, and are known as SAN filesystems or shared disk file systems. An architecture to attach remote computer storage devices such as disk array controllers, tape libraries and CD arrays to servers in such a way that to the operating system the devices appear as locally attached devices. An architecture to attach remote computer storage devices such as disk array controllers, tape libraries and CD arrays to servers in such a way that to the operating system the devices appear as locally attached devices.
<b>strict routing (SR)</b>	A routing mode in which the Request-URI specifies the next destination address of a short message. Before delivering a short message, each SIP Proxy replaces the Request-URI of the short message with the address specified by the first route header field, which ensures that the short message passes by all required SIP Proxies.

<b>superstratum provider edge (SPE)</b>	Core devices that are located within a VPLS full-meshed network. The UPE devices that are connected with the SPE devices are similar to the CE devices. The PWs set up between the UPE devices and the SPE devices serve as the ACs of the SPE devices. The SPE devices must learn the MAC addresses of all the sites on UPE side and those of the UPE interfaces that are connected with the SPE. SPE is sometimes called NPE.
<b>synchronous digital hierarchy (SDH)</b>	A transmission scheme that follows ITU-T G.707, G.708, and G.709. SDH defines the transmission features of digital signals, such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN.
<b>T</b>	
<b>TCA</b>	threshold crossing alert
<b>TCO</b>	See <a href="#">total cost of ownership</a> .
<b>TCP</b>	See <a href="#">Transmission Control Protocol</a> .
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TDM</b>	See <a href="#">time division multiplexing</a> .
<b>TE Tunnel</b>	See <a href="#">Traffic Engineered Tunnel</a> .
<b>TFTP</b>	Trivial File Transfer Protocol
<b>TL1</b>	Transaction Language 1
<b>TLS</b>	Transport Layer Security
<b>TMN</b>	See <a href="#">telecommunications management network</a> .
<b>TSDN</b>	Transport Software Defined Networking
<b>TTM</b>	See <a href="#">time to market</a> .
<b>Third Generation (3G)</b>	The third generation of digital wireless technology, as defined by the International Telecommunications Union (ITU). Third generation technology is expected to deliver data transmission speeds between 144 kbit/s and 2 Mbit/s, compared to the 9.6 kbit/s to 19.2 kbit/s offered by second generation technology.
<b>Traffic Engineered Tunnel (TE Tunnel)</b>	A combination of LSPs that is associated with a virtual tunnel interface.
<b>Transmission Control Protocol (TCP)</b>	The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.
<b>telecommunications management network (TMN)</b>	A protocol model defined by ITU-T for managing open systems in a communications network. TMN manages the planning, provisioning, installation, and OAM of equipment, networks, and services.

<b>time division multiplexing (TDM)</b>	A multiplexing technology. TDM divides the sampling cycle of a channel into time slots (TS <sub>n</sub> , n is equal to 0, 1, 2, 3...), and the sampling value codes of multiple signals engross time slots in a certain order, forming multiple multiplexing digital signals to be transmitted over one channel.
<b>time to market (TTM)</b>	The length of time it takes from a product being conceived until its being available for sale.
<b>total cost of ownership (TCO)</b>	Total cost of ownership (TCO) is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system. It is a management accounting concept that can be used in full cost accounting or even ecological economics where it includes social costs.
<b>U</b>	
<b>UNI</b>	See <a href="#">User-to-Network Interface</a> .
<b>UPE</b>	user-end provider edge
<b>URL</b>	See <a href="#">Uniform Resource Locator</a> .
<b>USM</b>	user-based security model
<b>UTC</b>	See <a href="#">Coordinated Universal Time</a> .
<b>Uniform Resource Locator (URL)</b>	A uniform resource locator (URL) is a reference to a resource that specifies the location of the resource on a computer network and acts as a mechanism for retrieving it. Each file on the Internet has a unique URL.
<b>User-to-Network Interface (UNI)</b>	The interface between user equipment and private or public network equipment (for example, ATM switches).
<b>V</b>	
<b>VDSL2</b>	See <a href="#">very-high-speed digital subscriber line 2</a> .
<b>VE</b>	virtual Ethernet
<b>VIP</b>	very important person
<b>VLAN</b>	See <a href="#">virtual local area network</a> .
<b>VLL</b>	virtual leased line
<b>VP</b>	See <a href="#">virtual path</a> .
<b>VPLS</b>	virtual private LAN segment
<b>VPN</b>	virtual private network
<b>VRF</b>	VPN routing and forwarding
<b>VRRP</b>	See <a href="#">Virtual Router Redundancy Protocol</a> .
<b>VXLAN</b>	Virtual Extensible LAN

<b>Virtual Router Redundancy Protocol (VRRP)</b>	A protocol designed for multicast or broadcast LANs such as an Ethernet. A group of routers (including an active router and several backup routers) in a LAN is regarded as a virtual router, which is called a backup group. The virtual router has its own IP address. The host in the network communicates with other networks through this virtual router. If the active router in the backup group fails, one of the backup routers in this backup group becomes active and provides routing service for the host in the network.
<b>VoIP</b>	voice over IP
<b>very-high-speed digital subscriber line 2 (VDSL2)</b>	An extension of the VDSL technology, which complies with ITU G.993.2, supports multiple spectrum profiles and encapsulation modes, and provides short-distance and high-speed access solutions to the next-generation FTTx access service.
<b>virtual local area network (VLAN)</b>	A logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same IP network number. This is often associated with switched Ethernet.
<b>virtual path (VP)</b>	A bundle of virtual channels, all of which are switched transparently across an ATM network based on a common VPI.
<b>W</b>	
<b>WAN</b>	wide area network
<b>X</b>	
<b>xDSL</b>	x digital subscriber line