

# HUAWEI NetEngine 8000 F Series Router V800R012C00SPC300

## Product Description

Issue 04  
Date 2020-04-30



**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)

---

# Contents

---

<b>1 About This Document.....</b>	<b>1</b>
<b>2 Product Positioning and Features.....</b>	<b>5</b>
2.1 Product Positioning.....	5
2.2 Product Features.....	6
<b>3 Applicable Scenarios.....</b>	<b>9</b>
<b>4 Product Architecture.....</b>	<b>10</b>
4.1 Physical Architecture.....	10
4.2 Logical Architecture.....	11
4.3 Software Architecture.....	12
4.4 Data Forwarding Process.....	13
<b>5 List of Software Features.....</b>	<b>15</b>
<b>6 Energy Conservation and Emission Reduction.....</b>	<b>76</b>
<b>7 NMS.....</b>	<b>78</b>
<b>8 Acronyms and Abbreviations.....</b>	<b>79</b>

---

## Figures

---

<b>Figure 2-1</b> Appearance (Front).....	5
<b>Figure 3-1</b> Application scenarios.....	9
<b>Figure 4-1</b> Functional host system.....	11
<b>Figure 4-2</b> Logical architecture.....	11
<b>Figure 4-3</b> Software architecture.....	12
<b>Figure 4-4</b> Schematic diagram for the data forwarding process.....	13
<b>Figure 5-1</b> IPv4/IPv6 dual stack structure.....	20

---

# Tables

**Table 5-1** List of software features..... 15

# 1 About This Document

---

## Purpose

This document describes the NetEngine 8000 in terms of its product positioning and features, architecture, technical specifications, supported FPICs, link features, service features, usage scenarios, and operation and maintenance.

## Related Version

The following table lists the product version related to this document.

Product Name	Version
NetEngine 8000 F Series	V800R012C00
NCE (IP Domain)	V100R019C00SPC601

## Intended Audience

This document is intended for:

- Network planning engineers
- Hardware installation engineers
- Commissioning engineers
- Data configuration engineers
- On-site maintenance engineers
- Network monitoring engineers
- System maintenance engineers

## Security Declaration

- Encryption algorithm declaration  
The encryption algorithms DES/3DES/RSA (RSA-2048 or lower)/MD5 (in digital signature scenarios and password encryption)/SHA1 (in digital signature scenarios) have a low security, which may bring security risks. If

protocols allowed, using more secure encryption algorithms, such as AES/RSA (RSA-2048 or higher)/SHA2/HMAC-SHA2 is recommended.

- Password configuration declaration
  - Do not set both the start and end characters of a password to "%^%#". This causes the password to be displayed directly in the configuration file.
  - To further improve device security, periodically change the password.
- Personal data declaration

Your purchased products, services, or features may use users' some personal data during service operation or fault locating. You must define user privacy policies in compliance with local laws and take proper measures to fully protect personal data.
- Feature declaration
  - The NetStream feature may be used to analyze the communication information of terminal customers for network traffic statistics and management purposes. Before enabling the NetStream feature, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.
  - The mirroring feature may be used to analyze the communication information of terminal customers for a maintenance purpose. Before enabling the mirroring function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.
  - The packet header obtaining feature may be used to collect or store some communication information about specific customers for transmission fault and error detection purposes. Huawei cannot offer services to collect or store this information unilaterally. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.
- Reliability design declaration

Network planning and site design must comply with reliability design principles and provide device- and solution-level protection. Device-level protection includes planning principles of dual-network and inter-board dual-link to avoid single point or single link of failure. Solution-level protection refers to a fast convergence mechanism, such as FRR and VRRP. If solution-level protection is used, ensure that the primary and backup paths do not share links or transmission devices. Otherwise, solution-level protection may fail to take effect.

## Special Declaration






- This document serves only as a guide. The content is written based on device information gathered under lab conditions. The content provided by this document is intended to be taken as general guidance, and does not cover all scenarios. The content provided by this document may be different from the information on user device interfaces due to factors such as version upgrades and differences in device models, board restrictions, and configuration files. The actual user device information takes precedence over the content

provided by this document. The preceding differences are beyond the scope of this document.

- The maximum values provided in this document are obtained in specific lab environments (for example, only a certain type of board or protocol is configured on a tested device). The actually obtained maximum values may be different from the maximum values provided in this document due to factors such as differences in hardware configurations and carried services.
- Interface numbers used in this document are examples. Use the existing interface numbers on devices for configuration.
- The pictures of hardware in this document are for reference only.
- The supported boards are described in the document. Whether a customization requirement can be met is subject to the information provided at the pre-sales interface.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.

## 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.
	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.

## Change History

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



- **Changes in Issue 04 (2020-04-30)**  
This issue is the fourth official release. The software version of this issue is V800R012C00SPC300.
- **Changes in Issue 03 (2020-03-30)**  
This issue is the third official release. The software version of this issue is V800R012C00SPC300.
- **Changes in Issue 02 (2020-03-15)**  
This issue is the second official release. The software version of this issue is V800R012C00SPC100.
- **Changes in Issue 01 (2019-10-30)**  
This issue is the first official release. The software version of this issue is V800R012C00.

# 2 Product Positioning and Features

---

## About This Chapter

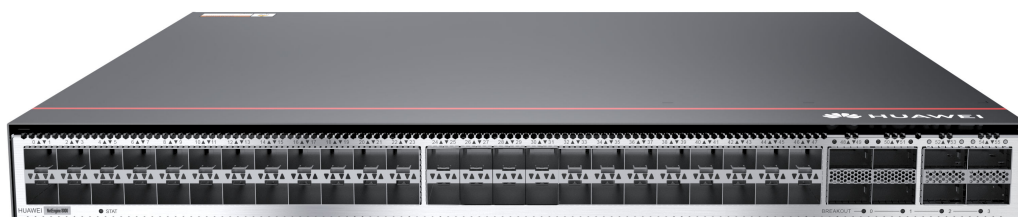
[2.1 Product Positioning](#)

[2.2 Product Features](#)

## 2.1 Product Positioning

HUAWEI NetEngine 8000 F Series comprise routers designed for the 5G and cloud era. This series offers an ultra-large capacity to meet future multi-service expansion requirements. It adopts a low power consumption design, making it suitable for large-scale deployment. In addition, the series supports ultra-large-capacity routing tables as well as rich features, such as Segment Routing over IPv6 (SRv6), In-situ Flow Information Telemetry (iFIT), hierarchical quality of service (HQoS), 1588v2, Layer 2 virtual private network (L2VPN), L3VPN, Ethernet VPN (EVPN), and multicast, to meet edge cloud DC-GW requirements.

**Figure 2-1** Appearance (Front)



### NOTE

For details about hardware and parameters, see *Hardware Description*.

## 2.2 Product Features

### Large capacity and compact design

- Large capacity
  - Offers an ultra-large capacity of 1.2T, meeting future multi-service expansion requirements.
  - Supports various interfaces, such as 100GE, 50GE, 40GE, 25GE, 10GE, and GE, to meet different service requirements.
- Compact design

The 420 mm deep chassis can be flexibly deployed in a 600 mm-deep cabinet, reducing the footprint in equipment rooms.

### Powerful multi-service capabilities

The device supports various features and provides powerful service processing capabilities. The key highlights are as follows:

- Powerful routing capabilities: The device provides ultra-large-capacity routing tables and supports various routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol version 4 (BGP-4), and multicast routing. In addition, it supports simple and ciphertext authentication as well as fast convergence to ensure network stability and security in complex routing environments.
- Strong service transport capabilities: In addition to supporting Internet Protocol (IP), MPLS, and SRv6, the device supports L2VPN, L3VPN, MVPN, and EVPN services, TE, flexible 802.1Q in 802.1Q (QinQ), and Generic Routing Encapsulation (GRE). This extensive support, meets the requirements of traditional access, emerging services, and multi-service converged transport.
- Powerful expandable multicast capabilities: The device supports various IPv4/IPv6 multicast protocols, such as Protocol Independent Multicast - Sparse Mode (PIM-SM), PIM - Source Specific Multicast (PM SSM), Multicast Listener Discovery Version 1 (MLDv1), MLDv2, Internet Group Membership Protocol Version 3 (IGMPv3), IGMP snooping, and MLD snooping. It can flexibly carry video services, such as Internet Protocol Television (IPTV), and satisfy multicast service requirements on networks of various scales.

### SRv6-powered intelligent connections

SRv6 is a future-oriented, next-generation simplified protocol that inherently supports IPv6, allowing access of numerous terminals. SRv6 and Huawei's Network Cloud Engine (NCE) enable cloud-based network resource adjustment, one-hop access to the cloud, and service provisioning within minutes. SRv6 can identify applications and tenants to implement intelligent traffic steering based on indicators such as latency and bandwidth, ensuring SLAs. In addition, SRv6 simplifies protocols and configurations.

## Full-lifecycle automation

NCE enables full-lifecycle automation and real-time visualization across the entire network. Precise in-band flow detection based on NCE and iFIT enables real-time visualization of service quality and fault locating within minutes.

## High-precision 1588v2 clock solution

- IEEE 1588v2, a standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, defines a Precision Time Protocol (PTP), which can achieve time and frequency synchronization with an accuracy of sub-microseconds.
- The 1588v2 standard enables time and frequency synchronization to meet the requirements of the G8273.2 standard. The high-precision time meet the requirements of wireless and Long Term Evolution (LTE) networks. The time jitter among multiple nodes (less than 30 nodes) is less than 1  $\mu$ s, allowing for large-scale networking. The device automatically selects an external clock source, which can be assigned different priorities, as its reference clock source based on parameters such as these priorities and the number of hops between itself and external clock sources. If the best external clock source fails, the device automatically selects the next-best external clock source as its reference clock source. An NE switchover can be completed within 200 ns, ensuring high clock reliability.
- The NMS provides GUI-based clock management.

## Future-oriented IPv6-compatible solution

The device supports IPv6 static routes and various IPv6 routing protocols, including OSPFv3, IS-ISv6, and Border Gateway Protocol for IPv6 (BGP4+). In addition, the device provide a large-capacity IPv6 forwarding information base (FIB) and supports IPv6 Access Control Lists (ACLs), and IPv6 policy-based routing. It also supports IPv4/IPv6 dual stacks to enhance network scalability. These features lay the foundation for smooth transition from IPv4 to IPv6.

## Multi-level reliability solution

The device provides reliability protection at different levels, including device, network, and service levels. It provides a network-wide reliability solution that fully meets the reliability requirements of different services, and lays the foundation for enterprise service reliability and interconnection with a system availability of 99.999%.

- Network-level reliability: The device uses the following technologies to ensure network-wide reliability and provide end-to-end protection switching within 200 ms for uninterrupted services: IP fast reroute (FRR); Label Distribution Protocol (LDP) FRR; VPN FRR; TE FRR; hot standby; Topology-Independent Loop-free Alternate FRR (TI-LFA); fast convergence of Interior Gateway Protocols (IGP), BGP, and multicast routes; Virtual Router Redundancy Protocol (VRRP); trunk load balancing and backup; Bidirectional Forwarding Detection (BFD); Ethernet OAM; and routing protocol/port/VLAN damping.
- Service-level reliability: The device uses technologies such as VPN FRR, E-VRRP, VLL FRR, Ethernet OAM, multicast dual-root protection, pseudo wire (PW) redundancy, and enhanced trunk (E-Trunk) to provide service-level

redundancy backup for L2VPNs and L3VPNs, ensuring stable, reliable, and uninterrupted services.

## **Energy-efficient design**

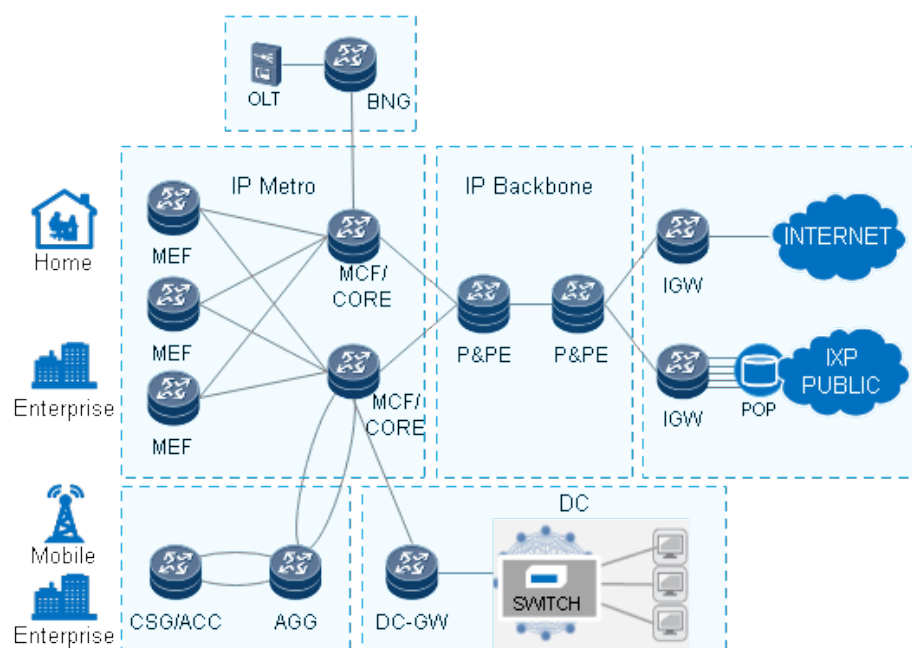
The device adopts an energy-efficient design to ensure environment-friendly operation.

- An advanced cooling and energy-efficient system, including a ventilation and heat dissipation design and intelligent fans, allows the device to automatically sense and adjust the temperature, greatly improving power utilization.
- The device supports dynamic frequency modulation and intelligent fan speed adjustment, which significantly reduces power consumption and gives the device an advantage in energy efficiency.

# 3 Applicable Scenarios

The F1A is mainly used in metro edge aggregation, DC-GW, and 5G transport scenarios.

**Figure 3-1** Application scenarios



# 4 Product Architecture

---

## About This Chapter

- [4.1 Physical Architecture](#)
- [4.2 Logical Architecture](#)
- [4.3 Software Architecture](#)
- [4.4 Data Forwarding Process](#)

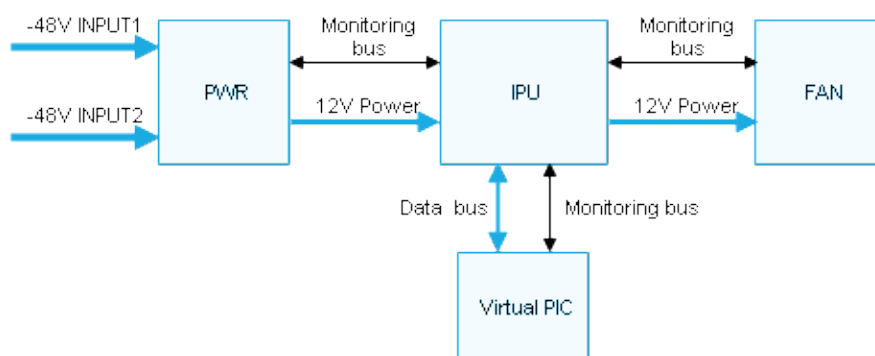
## 4.1 Physical Architecture

The NetEngine 8000 F1A uses the modular architecture. The physical architecture includes the following systems:

- Functional host system
- Power distribution system
- Heat dissipation system

The functional host system is composed of the IPUs and virtual interface cards. The functional host system processes data and monitors and manages the power distribution system and heat dissipation system. [Figure 4-1](#) shows the functional host system.

**Figure 4-1** Functional host system



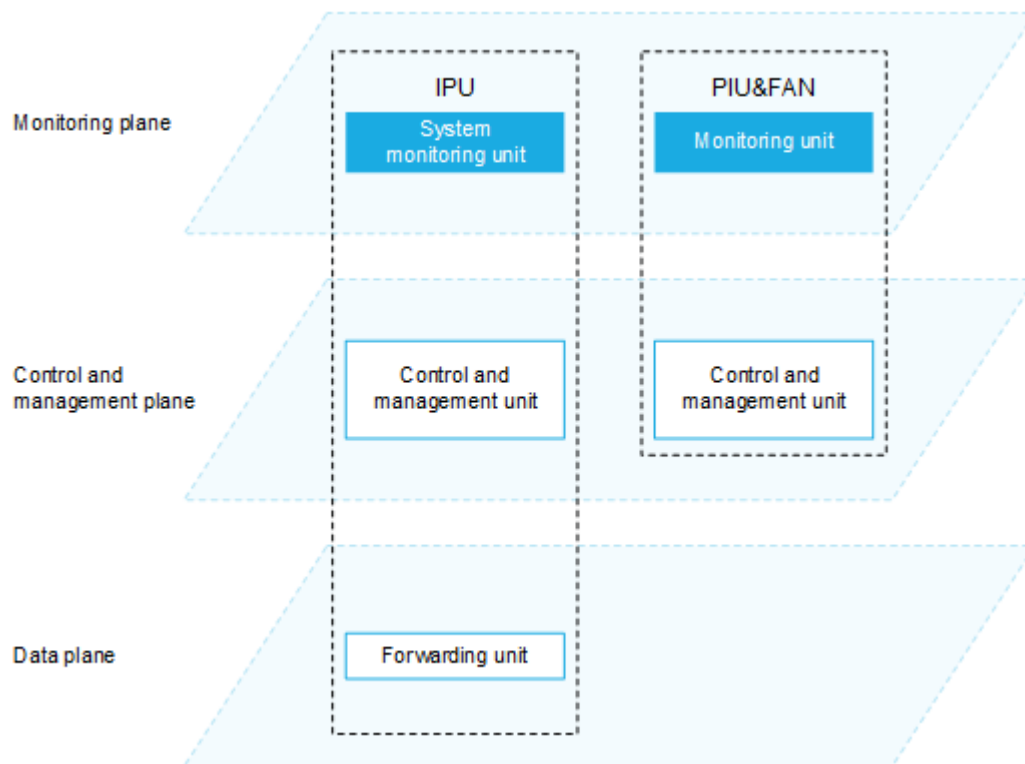
**NOTE**

This figure shows the functional host system of the NetEngine 8000 F1A (DC).

## 4.2 Logical Architecture

The logical architecture of the NetEngine 8000 F1A consists of the data plane, control and management plane, and monitoring plane. **Figure 1** shows the planes.

**Figure 4-2** Logical architecture



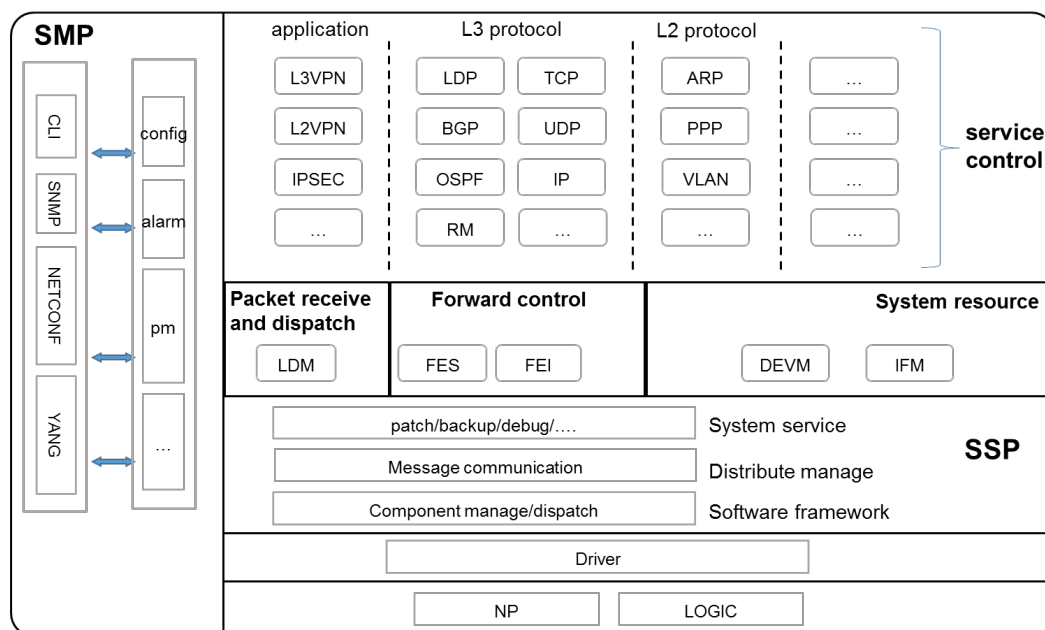


- The data plane is responsible for high-speed processing and congestion-free switching of data packets. It encapsulates and decapsulates packets, forwards IPv4/IPv6/MPLS packets, performs QoS as well as scheduling and internal high-speed switching, and collects statistics.
- The control and management plane provides all control and management functions for the system and is the core of the entire system. Control and management units process protocols and signals and configure, manage, report, and control system status.
- The monitoring plane monitors the ambient environment to ensure the secure and stable operation of the system. It detects voltage levels, controls system power-on and power-off, monitors the temperature, and controls fan modules. If a unit fails, the monitoring plane isolates the faulty unit promptly so that the other units remain unaffected.

### 4.3 Software Architecture

The NetEngine 8000 series provides an optimized software architecture characterized by the following key aspects: multi-component, multi-process, distributed, highly reliable, ultra-large-capacity, all-service, customer-oriented, scalable, and flexible, as shown in Figure 1.

Figure 4-3 Software architecture



Acronyms and abbreviations:

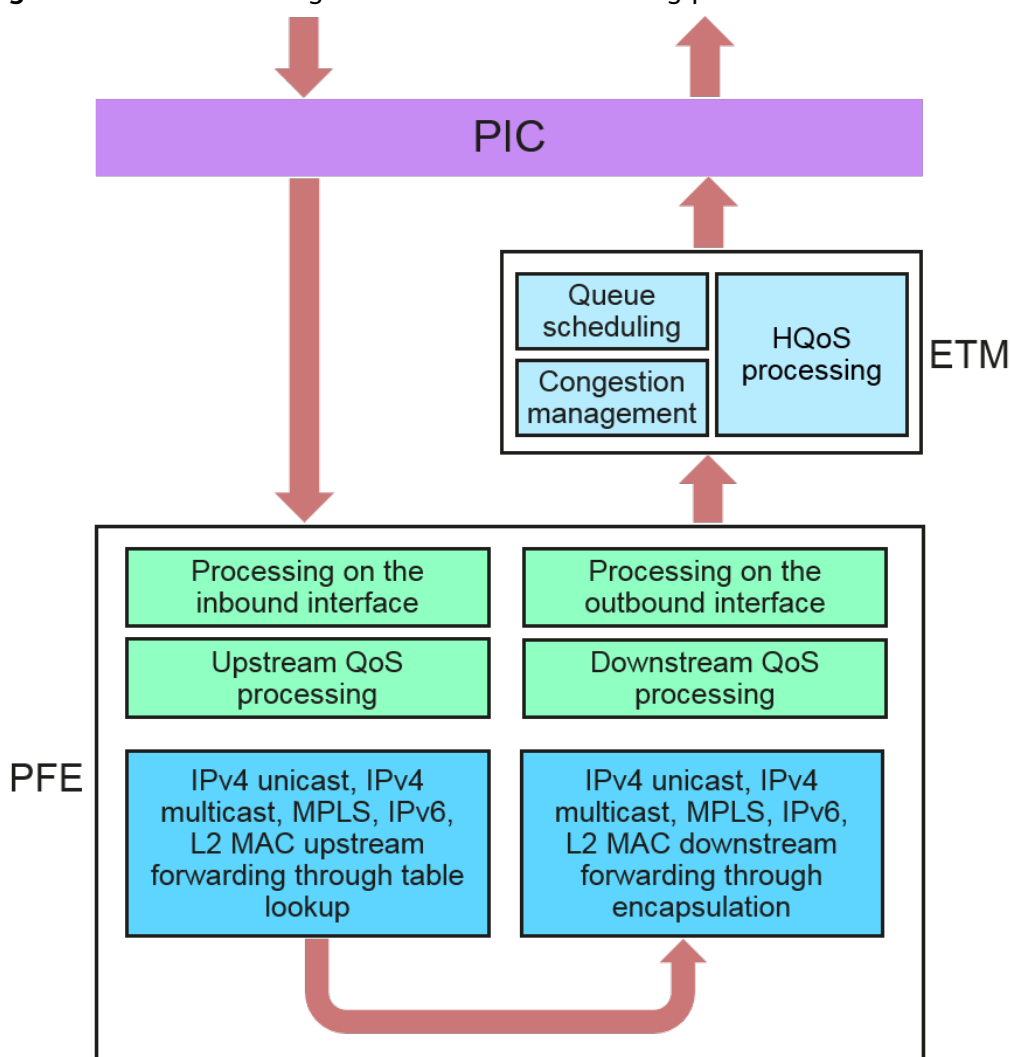
- SSP: system support platform
- SMP: system management plane
- NP: network processor
- LDM: local dispatch module
- FES: forwarding engine service

- FEI: forwarding engine service
- DEVM: device management
- IFM: interface management
- RM: routing management
- PM: performance management

## 4.4 Data Forwarding Process

### Data Forwarding Process

Figure 4-4 Schematic diagram for the data forwarding process



Data forwarding is processed on the in both the upstream and downstream directions.

- Upstream process: The PIC encapsulates packets into frames and sends them to the PFE. The processing module on the inbound interface parses the link-layer protocol information and identifies the packet type. Then, the upstream traffic classification module classifies traffic based on QoS configurations on

the inbound interface. After traffic classification, the PFE searches for forwarding entries to determine where to forward the packets. For example, to forward IPv4 unicast packets, the PFE searches the FIB for the outbound interfaces and next hops of the packets based on the packets' destination IP addresses.

- Downstream process: The PFE encapsulates link-layer information in the packets based on the packet type and outbound interface type. For example, for an IPv4 packet destined for an Ethernet interface, the PFE obtains the MAC address of the next hop. Then the downstream traffic classification module classifies traffic based on the QoS configurations on the outbound interface. The outbound interface processing module encapsulates the packets with new Layer 2 headers and sends them to the PIC.

# 5 List of Software Features

**Table 5-1** List of software features

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Link Features	Ethernet Link Features	-	<p>Ethernet interfaces on the NetEngine 8000 F1A support the following features:</p> <ul style="list-style-type: none"> <li>• Flow control and rate autonegotiation on GE interfaces</li> <li>• Bundling of interfaces at different rates</li> <li>• Addition or deletion of Eth-Trunk member interfaces; The NetEngine 8000 F1A can detect the up or down state of member interfaces and dynamically change the Eth-Trunk link bandwidth.</li> <li>• Layer 2 and Layer 3 Eth-Trunk interfaces</li> <li>• BFD for Eth-Trunk</li> <li>• Link Aggregation Control Protocol (LACP) defined in 802.3ad LACP maintains the link status based on the interface status. LACP adjusts or disables link aggregation when aggregation conditions change.</li> <li>• Virtual Ethernet (VE) interfaces</li> <li>• Synchronous Ethernet</li> <li>• 1588v2 clock</li> <li>• VLAN sub-interfaces</li> <li>• VLANIF interfaces</li> <li>• Local and remote interface loopback</li> <li>• Channelized Sub-Interfaces</li> </ul>

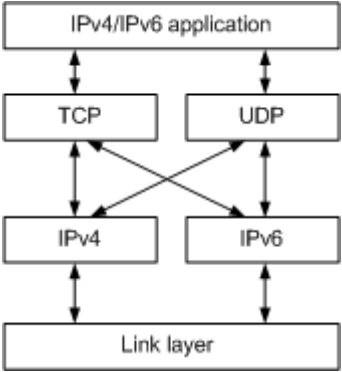
Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Ethernet Features	Layer 2 Ethernet Features	<p>Ethernet interfaces on the NetEngine 8000 F1A can work in Layer 2 switched mode and support VLAN, VPLS, and QoS services. Layer 2 Ethernet interfaces that are used as UNIs support MPLS VPN services.</p> <p>The NetEngine 8000 F1A supports the following Layer 2 Ethernet features:</p> <ul style="list-style-type: none"> <li>• Default VLAN</li> <li>• VLAN trunk</li> <li>• VLANIF interfaces</li> <li>• Intra-VLAN port isolation</li> <li>• Ethernet sub-interfaces</li> <li>• VLAN aggregation sub-interfaces</li> <li>• Port-based VLAN classification</li> <li>• VLAN mapping</li> <li>• VLAN stacking</li> <li>• Unqualified MAC learning and qualified MAC learning (user MAC addresses are learned based on VSI+VLAN)</li> <li>• MAC entry limit</li> <li>• Suppression of multicast, broadcast, and unknown unicast traffic</li> <li>• Y.1731 Eth-LCK, Eth-Test, and Eth-SLM</li> </ul>
Service Features	Ethernet Features	Layer 3 Ethernet Features	<p>The NetEngine 8000 F1A supports the following Layer 3 Ethernet features:</p> <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> <li>• MPLS</li> <li>• Multicast</li> <li>• VLAN sub-interfaces</li> <li>• QoS</li> <li>• VLAN aggregation sub-interfaces</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Ethernet Features	QinQ	<p>The NetEngine 8000 F1A supports the following QinQ features to satisfy different networking requirements:</p> <ul style="list-style-type: none"> <li>● Identification of inner and outer VLAN tags</li> <li>● Outer VLAN tag modification</li> <li>● Removal of double VLAN tags and addition of new double VLAN tags</li> <li>● Mapping of outer VLAN tags</li> <li>● Change of the EtherType value and 802.1p priority in the outer VLAN tag and copy of the 802.1p priority in the inner VLAN tag to the outer VLAN tag of double-tagged packets</li> <li>● Traffic classification based on the 802.1p priorities in the outer VLAN tags of packets</li> <li>● Rate limiting on interfaces based on the 802.1p priorities in both inner and outer VLAN tags</li> <li>● Interface-based QinQ</li> </ul> <p>Interface-based QinQ is applicable to the following scenarios:</p> <ul style="list-style-type: none"> <li>- Access to VPLS networks to transparently transmit VLAN packets</li> <li>- Access to L2VPNs or PWE3 networks to transparently transmit VLAN packets</li> </ul> <ul style="list-style-type: none"> <li>● VLAN-based QinQ</li> <li>● 802.1ag</li> <li>● QinQ termination</li> <li>● EtherType value in the outer VLAN tags of QinQ packets used for interoperation with non-Huawei devices</li> <li>● Multicast QinQ</li> <li>● QinQ-based VLAN swapping on main interfaces</li> <li>● VLAN stacking is applicable to the following scenarios: <ul style="list-style-type: none"> <li>- Access to VPLS networks</li> <li>- Access to VLL or PWE3 networks</li> </ul> </li> <li>● Translation sub-interfaces on which 1 to 1 VLAN tag translation can be implemented</li> <li>● IPv4 URPF for QinQ VLAN tag termination sub-interfaces</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Ethernet Features	Flexible Access to VPNs	In traditional access identification, user or service information is identified by a single tag or double tags. For example, the inner tag identifies user information, and the outer tag identifies service information. Interfaces have different double tags configured to access different VPNs. In some scenarios, the access device does not support QinQ or a single tag is used for multiple services. In this case, the access device may fill service access information in the 802.1p or DSCP field. Then, the NetEngine 8000 F1A connected to the access device needs to use the 802.1p or DSCP value to identify access users. This helps implement access to different VPNs using different QoS scheduling policies.
Service Features	Ethernet Features	Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) / Multiple Spanning Tree Protocol (MSTP) Features	<p>The NetEngine 8000 F1A supports STP, RSTP and MSTP.</p> <ul style="list-style-type: none"> <li>• STP</li> <li>• RSTP</li> <li>• MSTP</li> </ul> <p>MSTP provides BPDU protection to defend against attacks. After BPDU protection is enabled on the device, it disables the edge port that receives BPDUs. The disabled edge port can only be enabled by the network administrator.</p>
Service Features	Ethernet Features	BPDU Tunneling	<p>The NetEngine 8000 F1A supports the following BPDU tunneling types:</p> <ul style="list-style-type: none"> <li>• Port-based BPDU tunneling</li> <li>• VLAN-based BPDU tunneling</li> <li>• QinQ-based BPDU tunneling</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Ethernet Features	VXLAN	<p>Virtual eXtensible Local Area Network (VXLAN) is a Network Virtualization over Layer 3 (NVO3) technology that uses MAC-in-UDP encapsulation.</p> <p>The NetEngine 8000 F1A supports the following VXLAN features:</p> <ul style="list-style-type: none"> <li>Layer 3 forwarding between VXLAN tunnels</li> <li>Use of integrated routing and bridging (IRB) routes to advertise host routes between VXLAN tunnels</li> <li>Application of traffic policies to VXLAN tunnels</li> <li>DHCP relay for VXLAN tunnels</li> <li>VNI-based rate limiting</li> <li>VXLAN Layer 2 gateway</li> <li>VXLAN Layer 2 gateway supporting the Spoken split horizon mode</li> <li>MAC address learning using EVPN on the VXLAN control plane</li> <li>VXLAN tunnel encapsulation before forwarding over L3VPN in Ethernet access scenarios</li> <li>Interface-based sampling, packet parsing after sampling, VNI identification, and flow aggregation and output based on VNI and IP</li> <li>BA classification and MF classification</li> <li>VXLAN segments</li> </ul>
Service Features	Ethernet Features	ERPS over VPLS	<p>ERPS over VPLS allows an ERPS ring to connect to a VPLS network. This function supports the following VPLS access modes:</p> <ul style="list-style-type: none"> <li>• A VLANIF interface is single-homed to a VPLS network.</li> <li>• A VLANIF interface is dual-homed to a VPLS network.</li> <li>• A sub-interface is single-homed to a VPLS network. The sub-interfaces can be: <ul style="list-style-type: none"> <li>– QinQ mapping 1:1 and dot1q VLAN sub-interfaces</li> </ul> </li> <li>• A sub-interface is dual-homed to a VPLS network. The sub-interfaces can be: <ul style="list-style-type: none"> <li>– QinQ mapping 1:1 and dot1q VLAN sub-interfaces</li> </ul> </li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	IP Features	IPv4/IPv6 Dual Stack	<p>The IPv4/IPv6 dual stack is highly interoperable and easy to implement. The following figure shows the IPv4/IPv6 dual stack structure.</p> <p><b>Figure 5-1 IPv4/IPv6 dual stack structure</b></p>  <pre> graph TD     App[IPv4/IPv6 application] &lt;--&gt; TCP[TCP]     App &lt;--&gt; UDP[UDP]     TCP &lt;--&gt; IPv4[IPv4]     TCP &lt;--&gt; IPv6[IPv6]     UDP &lt;--&gt; IPv4[IPv4]     UDP &lt;--&gt; IPv6[IPv6]     IPv4 &lt;--&gt; Link[Link layer]     IPv6 &lt;--&gt; Link[Link layer]     </pre>
Service Features	IP Features	IPv4 Features	<p>The NetEngine 8000 F1A supports the following IPv4 features:</p> <ul style="list-style-type: none"> <li>• TCP/IP protocol suite, including ICMP, IP, TCP, UDP, socket (TCP/UDP/Raw IP), and ARP</li> <li>• FTP client/server and TFTP client</li> <li>• DHCP relay agent/DHCP server</li> <li>• DHCP flooding suppression</li> <li>• Ping, tracert, and NQA</li> </ul> <p>NQA can detect the status of ICMP and UDP services and test the service response time.</p> <ul style="list-style-type: none"> <li>• IP policy-based routing (PBR) and flow-based next hop to which packets are forwarded</li> <li>• IP PBR-based load balancing</li> <li>• Load balancing in unequal cost multi-path (UCMP) mode</li> <li>• Configuration of secondary IP addresses for all physical and logical interfaces</li> </ul> <p>Each interface supports a maximum of 255 secondary IP addresses with 31-bit masks.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	IP Features	IPv6 Features	<p>The NetEngine 8000 F1A supports the following IPv6 features:</p> <ul style="list-style-type: none"> <li>● IPv6 neighbor discovery (ND)</li> <li>● Path MTU (PMTU) discovery</li> <li>● TCP6, IPv6 ping, IPv6 tracer, and IPv6 socket</li> <li>● Static IPv6 DNS and specified IPv6 DNS server</li> <li>● TFTP IPv6 client</li> <li>● IPv6 PBR</li> <li>● Telnet and SSH</li> </ul>
Service Features	IP Features	IPv4/IPv6 Transition	<p>The NetEngine 8000 F1A supports the following IPv4/IPv6 transition features:</p> <ul style="list-style-type: none"> <li>● IPv6 over IPv4 tunnels</li> </ul> <p>The NetEngine 8000 F1A supports the following IPv6 over IPv4 tunnels:</p> <ul style="list-style-type: none"> <li>- IPv6 manual tunnel</li> <li>- 6to4 tunnel</li> <li>- 6to4 relay tunnel</li> </ul> <ul style="list-style-type: none"> <li>● 6PE and 6VPE tunnels</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Routing Protocols	Unicast Routing	<p>The NetEngine 8000 F1A supports the following unicast routing features:</p> <ul style="list-style-type: none"> <li>● IPv4 routing protocols, including RIP, OSPF, IS-IS, and BGP4</li> <li>● IPv6 routing protocols, including Routing Information Protocol Next Generation (RIPng), OSPFv3, IS-ISv6, and BGP4+</li> <li>● Static routes that are manually configured by the network administrator to simplify network configurations and improve network performance</li> <li>● Large-capacity routing table that effectively supports MAN operations</li> <li>● Selection of the optimal route using routing policies</li> <li>● Import of routes from other protocols</li> <li>● Route advertisement and reception through routing policies and router filtering through route attributes</li> <li>● Password authentication and MD5 authentication to improve network security</li> </ul> <p><b>NOTE</b> For the sake of security, using the HMAC-SHA256 algorithm rather than the MD5 algorithm is recommended.</p> <ul style="list-style-type: none"> <li>● Restart of protocol processes using command lines</li> <li>● RIPv1 (classful routing protocol) and RIPv2 (classless routing protocol)</li> <li>● Advertisement of a default route from a RIP-enabled device to its peers and setting of the metric of this route</li> <li>● RIP-triggered updates</li> <li>● Disabling a specified interface from sending or receiving OSPF or RIP packets</li> <li>● OSPF-BGP synchronization</li> <li>● OSPF-LDP synchronization</li> <li>● OSPF fast convergence, which can be implemented using either of the following methods: <ul style="list-style-type: none"> <li>– Adjust the LSA transmission interval.</li> <li>– Configure BFD for OSPF.</li> </ul> </li> <li>● OSPF I-SPF and IS-IS I-SPF (I-SPF re-calculates only the changed routes of an SPT and not the entire SPT.)</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<ul style="list-style-type: none"> <li>● OSPF PRC</li> <li>● OSPF link cost calculation based on the reference bandwidth                      Link costs can be manually configured or automatically calculated by the system based on the reference bandwidth by using the following formula:                      Link cost = Reference bandwidth/Interface bandwidth                      The integer of the calculated result is the link cost. If the calculated result is smaller than 1, the cost is 1. The link cost can be changed by changing the reference bandwidth. The reference bandwidth ranges from 1 to 2147483648, in Mbit/s. The default reference bandwidth of the NetEngine 8000 F1A is 100 Mbit/s. The value ranges from 1 to 2147483648 Mbit/s. The link cost can be calculated based on the reference link delay.</li> <li>● Two-level IS-IS in a routing domain</li> <li>● IS-IS and LDP synchronization</li> <li>● BGP indirect next hop and dynamic update peer-groups</li> <li>● IPv6 indirect next hop</li> <li>● Policy-based BGP route selection when multiple routes are available to the same destination</li> <li>● BGP route reflector (RR)                      If there are many IBGP peers, it is costly to establish a full-mesh network. To prevent this problem, deploy RRs so that IBGP peers establish peer relationships only with RRs.</li> <li>● Transmission of BGP Update packets that do not carry private AS numbers</li> <li>● BGP route dampening, which suppresses unstable routes (Unstable routes are neither added to the BGP routing table nor advertised to other BGP peers.)</li> <li>● Routing policy</li> <li>● BGP fast convergence                      The device uses a new route convergence mechanism and algorithm to accelerate BGP route convergence. The mechanism can be:                     <ul style="list-style-type: none"> <li>- Indirect next hop</li> </ul> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<ul style="list-style-type: none"> <li>- On-demand route recursion</li> <li>• BGP load balancing in multi-homing networking</li> </ul> <p>The formula for calculating the interface bandwidth consumed by LSAs in the same area is as follows:                      For example, if 10000 routes and Ethernet interfaces are used and the MTU of each Ethernet interface is 1500 bytes, the Ethernet frame header+FCS is 18 bytes, and each LSA is 44 bytes. Each LSA carries information about a route.</p> <p><math>(1500 - 18)/44 = 33</math>. This formula indicates that an Ethernet frame can carry information about 33 routes. Therefore, 304 Ethernet frames are required to carry information about 10,000 routes.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Routing Protocols	Multicast Routing	<p>The NetEngine 8000 F1A supports the following multicast features:</p> <ul style="list-style-type: none"> <li>● Multicast protocols include the Internet Group Management Protocol (IGMP), Protocol Independent Multicast-Sparse Mode (PIM-SM), Multicast Source Discovery Protocol (MSDP), and Multiprotocol Border Gateway Protocol (MBGP). IGMP can be IGMPv1, IGMPv2, or IGMPv3.</li> <li>● Reverse Path Forwarding (RPF)</li> <li>● PIM-SSM</li> <li>● Anycast RP</li> <li>● IPv6 multicast routing protocols that include PIM-IPv6-SM and PIM-IPv6-SSM</li> <li>● Multicast Listener Discovery (MLD) <ul style="list-style-type: none"> <li>– MLDv1 <p>MLDv1 supports Any-Source Multicast (ASM) and can implement Source-Specific Multicast (SSM) using SSM mapping.</p> </li> <li>– MLDv2 <p>MLDv2 supports ASM and SSM.</p> </li> </ul> </li> <li>● Multicast static routes</li> <li>● Configuration of multicast protocols on Ethernet and trunk interfaces</li> <li>● Route filtering based on routing policies when the multicast routing module receives, imports, or advertises multicast routes multicast packet filtering and forwarding based on routing policies when IP multicast packets are forwarded</li> <li>● Addition and deletion of dummy entries</li> <li>● Query of PIM neighbors and the number of control messages</li> <li>● PIM neighbor filtering, forwarding boundary control, and BSR service and management boundary control</li> <li>● PIM Register message filtering and suppression</li> <li>● MSDP authentication</li> <li>● IGMP rate limiting</li> <li>● Prompt leave of IGMP and MLD group members and use of group-policies to restrict the generation of forwarding entries</li> <li>● Configuration of ACLs, including source-address-based packet filtering, generation of multicast</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>forwarding entries, and Switch-MDT switching, to ensure multicast security</p> <ul style="list-style-type: none"> <li>● Multicast-group-based, multicast-source-based, multicast-source/group-based, and stable-preferred load balancing</li> <li>● IGMP snooping</li> <li>● MLD Snooping</li> <li>● Multicast flow control</li> </ul> <p>The NetEngine 8000 F1A discards or broadcasts unknown multicast packets in the VLAN to which the interface that received the packets belongs. Unknown multicast packets do not have matching forwarding entries in the multicast forwarding table. In addition, the NetEngine 8000 F1A limits the maximum percentage of multicast flows on Ethernet interfaces to control multicast traffic.</p> <ul style="list-style-type: none"> <li>● VSI-based IGMP CP-CAR</li> <li>● Distributed multicast</li> <li>● Multicast CAC</li> </ul> <p>The NetEngine 8000 F1A supports multicast Call Admission Control (CAC). When multicast CAC rules are configured, the number of multicast groups and bandwidth are restricted for IGMP snooping on interfaces or the entire system.</p> <ul style="list-style-type: none"> <li>● BIER</li> </ul> <p>BIER-MPLS and NG MVPN over BIER</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	MPLS Features	MPLS	<p>The NetEngine 8000 F1A supports the following MPLS features:</p> <ul style="list-style-type: none"> <li>● Basic MPLS functions, service forwarding, and MPLS LDP signaling MPLS LDP distributes labels, establishes LSPs, and exchanges parameters used for LSP establishment. MPLS LDP supports: <ul style="list-style-type: none"> <li>● A maximum of five MPLS labels in a label stack</li> <li>● MPLS LDP supports: <ul style="list-style-type: none"> <li>- Label advertisement in downstream unsolicited (DU) mode</li> <li>- Label distribution in independent mode</li> <li>- Label distribution in ordered mode</li> <li>- Label retention in liberal mode</li> <li>- Basic discovery and extended discovery in LDP sessions</li> </ul> </li> </ul> </li> <li>● MPLS ping and tracer operations in which MPLS Echo Request and MPLS Echo Reply packets are exchanged to monitor LSP availability</li> <li>● Configuration of 64-channel load balancing (including the ingress and intermediate nodes)</li> <li>● MPLS QoS, including the mapping of the ToS fields in IP packets to the EXP fields in MPLS packets, and MPLS uniform, pipe, and short pipe modes</li> <li>● MPLS trap</li> <li>● LDP-IGP synchronization, which minimizes traffic loss in the event of network failures</li> <li>● NetEngine 8000 F1A functioning as a label edge router (LER) or a label switching router (LSR) <p>An LER is an edge device that connects an MPLS network to other networks. It classifies services, distributes labels, and adds or removes labels as required. An LER functioning as an egress supports PHP and can allocate an explicit null label or an implicit null label to the penultimate hop.</p> <p>An LSR is a core router on an MPLS network. The LSR switches and distributes labels.</p> </li> <li>● Establishment of LSPs between routers of different IS-IS levels and between Huawei devices and non-Huawei devices using LDP.</li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	MPLS Features	MPLS TE	<p>MPLS TE integrates MPLS technology with traffic engineering. It reserves resources by establishing LSPs over a specified path in an attempt to avoid network congestion and balance network traffic.</p> <p>In the event of insufficient resources, MPLS TE allows preemption of bandwidth resources of low priority LSPs so these resources can be provided for LSPs with large bandwidth requirements or important services. If an LSP fails or a node is congested, MPLS TE can ensure smooth network communication using the backup path and fast reroute (FRR) function. MPLS TE provides automatic re-optimization and bandwidth adjustment to improve tunnel self-adaptation and properly allocate network resources.</p> <p>The traffic engineering database (TEDB) can be used to update the network topology. If a link goes down, the Constrained Shortest Path First (CSPF) failed link timer starts. Before the failed link timer expires, if the IGP route is deleted or the link is changed, CSPF deletes the timer and updates the TEDB. If the IGP route is not deleted or the link is not changed after the CSPF failed link timer expires, the link is considered up.</p> <p>MPLS TE supports the following functions:</p> <ul style="list-style-type: none"> <li>● Processing of Constrained Route-label switched path (CR-LSP) of various types and route calculation using the CSPF algorithm</li> </ul> <p>CR-LSPs are classified into the following types:</p> <ul style="list-style-type: none"> <li>● RSVP-TE <ul style="list-style-type: none"> <li>RSVP authentication complies with relevant standards.</li> </ul> </li> <li>● Auto routing <ul style="list-style-type: none"> <li>Auto routing works in either of the following modes: <ul style="list-style-type: none"> <li>– IGP shortcut: An LSP is not advertised to neighboring routers. Therefore, other routers cannot use the LSP.</li> <li>– Forwarding adjacency: An LSP is advertised to neighboring routers. Therefore, other routers can use the LSP.</li> </ul> </li> </ul> </li> <li>● FRR <ul style="list-style-type: none"> <li>FRR switching can be completed in 50 ms, which minimizes data loss if network faults occur.</li> </ul> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<ul style="list-style-type: none"> <li data-bbox="724 398 1433 712"> <p>● Auto FRR</p> <p>Auto FRR is an extension of MPLS TE FRR. Configuring bypass tunnel attributes, global auto FRR, and interface-based auto FRR for the primary tunnel facilitates automatic establishment of a bypass tunnel over an LSP. If the primary tunnel changes, the bypass tunnel is automatically deleted, and a new one meeting requirements is established.</p> </li> <li data-bbox="724 723 1433 1025"> <p>● One-to-one backup FRR: an MPLS TE FRR mode. After the detour attribute is configured for the primary tunnel, a detour LSP can be automatically established to protect an LSP on the primary tunnel. The detour LSP is a part of the primary tunnel. When the primary tunnel is established, detour LSPs are automatically established as needed. They are changed or deleted together with the primary tunnel.</p> </li> <li data-bbox="724 1037 1433 1451"> <p>● CR-LSP backup</p> <p>NetEngine 8000 F1A supports the following backup modes:</p> <ul style="list-style-type: none"> <li data-bbox="762 1160 1433 1328"> <p>– Hot standby</p> <p>An HSB CR-LSP is established immediately after the primary CR-LSP is established. If the primary CR-LSP fails, MPLS TE switches traffic immediately to the HSB CR-LSP.</p> </li> <li data-bbox="762 1350 1433 1451"> <p>– Ordinary backup</p> <p>A backup CR-LSP is established after the primary CR-LSP fails.</p> </li> </ul> </li> <li data-bbox="724 1462 1433 1742"> <p>● LDP over TE</p> <p>Not all devices on a live network support MPLS TE. If only core devices support TE and LDP is used on edge devices, LDP over TE can be used. A TE tunnel is considered a hop of the entire LDP LSP. With forwarding adjacency, one MPLS TE tunnel can be used as a virtual link and advertised to an IGP network.</p> </li> <li data-bbox="724 1753 1433 1955"> <p>● Make-before-break</p> <p>Make-before-break is a CR-LSP switching technology that ensures high reliability. Before a new path or CR-LSP is created, the original path or CR-LSP is not deleted. After a new CR-LSP is created, traffic is switched to the new CR-LSP, and</p> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			then the original CR-LSP is deleted. This implements non-stop traffic forwarding.
Service Features	MPLS Features	GMPLS UNI	<ul style="list-style-type: none"> <li>• RSVP neighbor authentication and UNI user access authentication</li> <li>• Protection for traffic on a specified UNI tunnel connected to the ingress CN on a transport network</li> <li>• Collaborative path computation by an IP PCE and optical PCE</li> </ul>
Service Features	MPLS Features	MPLS LDP	<p>LDP remote LFA FRR is a supplement to LFA LDP FRR. LFA LDP FRR uses the LFA FRR algorithm that can only protect LDP LSPs in 70% of all scenarios. After the remote LFA technique is implemented, FRR takes effect in more than 96% of all scenarios.</p> <p>The LDP module receives the remote LFA FRR next-hop address of a route prefix sent by the RM module. The LDP module uses the carried PQ node address to create an LDP remote peer and sends a Target Hello message to its peer to establish a remote LDP session. The PQ node address is used as a next-hop IP address for a remote-LFA FRR LSP. The actual next-hop IP address and outbound interface name are used to establish an LDP LSP destined for the PQ node. This LDP LSP allows for recursion to the remote LFR LSP.</p> <p>On the PQ node, the auto-accept function is configured. This function enables the PQ node to use information in the received Target Hello message to automatically establish a remote LDP peer. The PQ node then sends a Target Hello message to its peer to establish a remote LDP session. Label Mapping messages are then transmitted over the remote LDP session to establish a tunnel.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Segment Routing Features	SR-MPLS TE	<p>Segment Routing (SR) is designed to forward data packets on a network based on source route technology. SR-MPLS is segment routing based on the MPLS forwarding plane.</p> <p>SR-MPLS Traffic Engineering (TE) is a new TE tunnel technology that uses SR as a control protocol. The controller calculates forwarding paths for tunnels and delivers label stacks strictly mapped to the paths to forwarders. The forwarder, which is the ingress of the tunnel, uses a label stack to control the path along which packets are transmitted on a network.</p> <p>The device supports the following SR-MPLS TE functions:</p> <ul style="list-style-type: none"> <li>• Strict label stack</li> <li>• Stitching label</li> <li>• L2VPN, L3VPN, and LDP over SR-MPLS TE</li> <li>• Hot standby (HSB) LSP, and BFD SR-MPLS TE Policy LSP</li> <li>• Class-based tunnel selection (CBTS)</li> <li>• SR-MPLS TE Policy</li> </ul>
Service Features	Segment Routing Features	SR-MPLS BE	<ul style="list-style-type: none"> <li>• SR LSPs are established using the segment routing technique, and uses prefix or node segments to guide data packet forwarding. Segment Routing Best Effort (SR-MPLS BE) uses an IGP to run the shortest path algorithm to compute an optimal SR LSP.</li> <li>• SR and LDP interworking</li> </ul>
Service Features	Segment Routing	SRv6 BE	<p>The device supports the following SRv6 BE functions:</p> <ul style="list-style-type: none"> <li>• BGP L3VPN over SRv6 BE</li> <li>• EVPN L3VPNv4 over SRv6 BE</li> <li>• EVPN L3VPNv6 over SRv6 BE</li> <li>• EVPN VPWS over SRv6 BE</li> <li>• EVPN VPLS over SRv6 BE</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Segment Routing	SRv6 TE Policy	<p>The device supports the following SRv6 TE Policy functions:</p> <ul style="list-style-type: none"> <li>• IPv4 public network service over SRv6 TE Policy</li> <li>• BGP L3VPNv4 over SRv6 TE Policy</li> <li>• EVPN L3VPNv4 over SRv6 TE Policy</li> <li>• EVPN L3VPNv6 over SRv6 TE Policy</li> <li>• EVPN VPWS over SRv6 TE Policy</li> <li>• EVPN VPLS over SRv6 TE Policy</li> <li>• BGP-LS</li> </ul>
Service Features	VPN Features	Tunnel Policy	<p>A tunnel policy determines which tunnels are to be selected based on destination IP addresses. If no tunnel policy is configured, the tunnel management module uses the default tunnel policy to select tunnels.</p> <p>The NetEngine 8000 F1A supports the following types of tunnel policies:</p> <ul style="list-style-type: none"> <li>• Select-sequence <ul style="list-style-type: none"> <li>The priority sequence of tunnels and the number of tunnels used for load balancing are configured. The tunnels of the type specified first are selected as long as the tunnels are in the up state, irrespective of whether they are used by other services. The tunnels of the type specified later are not selected unless load balancing is required or the tunnels of the type specified first are all down.</li> </ul> </li> <li>• VPN tunnel binding <ul style="list-style-type: none"> <li>After the peer end of a VPN is bound to an MPLS TE tunnel on a PE on the backbone network, this TE tunnel only transmits data from the VPN to its peer end and not to other VPN services. This ensures QoS for services of the bound VPN.</li> </ul> </li> </ul>
Service Features	VPN Features	VPN Tunnel	<p>The NetEngine 8000 F1A supports the following types of VPN tunnels:</p> <ul style="list-style-type: none"> <li>• LSPs</li> <li>• TE tunnels</li> <li>• GRE tunnel</li> <li>• SR-MPLS TE tunnel</li> <li>• SR-MPLS BE tunnel</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	VPN Features	MPLS L2VPN	<ul style="list-style-type: none"> <li>● VLL <ul style="list-style-type: none"> <li>- Martini VLL Martini VLL supports double labels. The inner label uses extended LDP as signaling, in compliance with relevant standards. The VC FEC type is 128. The VC encapsulation type can be 0x0004 Ethernet Tagged Mode, 0x0005 Ethernet, or 0x000B IP Layer 2 Transport.</li> <li>- CCC VLL CCC VLL supports local switching of packets in 802.1q mode.</li> <li>- VLL heterogeneous interworking VLL heterogeneous interworking is used when the CE link types on both ends of an L2VPN are different. After a PE receives a frame from a CE, the PE removes the link-layer frame header and transparently transmits the IP packet to the peer PE across an MPLS network. Upon receipt, the peer PE encapsulates the link-layer frame header to the IP packet and transmits the frame to the connected CE. PEs process link-layer control packets received from CEs without transmitting them over MPLS networks and discard non-IP packets, such as MPLS and IPX packets.</li> <li>- Transparent transmission of specific types of link layer protocol packets Interfaces can be configured to transparently transmit specific types of link layer protocol packets, such as BPDUs, LACP packets, LLDP packets, UDLD packets, and CDP packets.</li> <li>- VLL over TE ECMP</li> <li>- VLL over LDP ECMP</li> <li>- VLL over LDP over TE ECMP</li> </ul> </li> <li>● VPLS PEs on a VPLS network can be fully meshed and have split horizon configured to prevent Layer 2 loops. VPLS is classified as Kompella VPLS or Martini VPLS, depending on the signaling protocol. <ul style="list-style-type: none"> <li>- Kompella VPLS</li> </ul> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>Kompella VPLS uses BGP as the signaling protocol. Kompella VPLS uses BGP to automatically discover VPLS members and then establishes point-to-point PWs. When a PE is added to the VPLS network, the configurations on existing PEs do not need to be modified. The new PE can automatically establish PWs with other PEs on the network.</p> <ul style="list-style-type: none"> <li>- Martini VPLS</li> </ul> <p>In Martini VPLS, LDP peer relationships must be manually configured between PEs on a full-mesh VPLS network. When a PE is added to the VPLS network, the configurations on all PEs need to be modified. Therefore, Martini VPLS has poor extensibility. However, using LDP to create, maintain, and delete point-to-point PWs is effective.</p> <p>The NetEngine 8000 F1A supports the following VPLS functions:</p> <ul style="list-style-type: none"> <li>- Access to the VPLS network in QinQ mode</li> <li>- H-VPLS</li> <li>- IGMP snooping for VPLS</li> <li>- MLD snooping for VPLS</li> <li>- One MAC address space for each VSI</li> <li>- VPLS/H-VPLS equal-cost load balancing</li> <li>- Fast switching of multicast traffic</li> <li>- mVPLS</li> <li>- Transparent transmission of specific types of link layer protocol packets</li> </ul> <p>Interfaces can be configured to transparently transmit specific types of link layer protocol packets, such as BPDUs, STP packets, LLDP packets, UDLD packets, and CDP packets.</p> <ul style="list-style-type: none"> <li>- Ethernet loop detection</li> <li>- ERPS ring accessing VPLS</li> </ul> <ul style="list-style-type: none"> <li>● PWE3</li> </ul> <p>The NetEngine 8000 F1A supports the following features: The</p> <ul style="list-style-type: none"> <li>- VCCV ping</li> </ul> <p>The NetEngine 8000 F1A can use VCCV ping to detect LDP PW connectivity on the UPE. It is</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>capable of detecting dynamic PWs, single-segment PWs (SS-PWs), and multi-segment PWs (MS-PWs).</p> <ul style="list-style-type: none"> <li>- PW template</li> </ul> <p>The NetEngine 8000 F1A supports binding between a PW and a PW template and PW resets.</p> <p>The NetEngine 8000 F1A uses PWE3 to support heterogeneous interworking and transparent transmission of the following packet types: Ethernet, IP Layer 2 transport, IP-interworking, and Ethernet tagged.</p> <ul style="list-style-type: none"> <li>- PW redundancy</li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	VPN Features	BGP/MPLS L3VPN	<p>The NetEngine 8000 F1A supports BGP/MPLS L3VPN, providing an end-to-end VPN solution. The VPN service is a new type of value-added service. The device supports the following BGP/MPLS L3VPN functions:</p> <ul style="list-style-type: none"> <li>● Access of a CE to an L3VPN through Layer 3 interfaces, such as Ethernet and VLANIF interfaces</li> <li>● CE-PE communication using static routes or routing protocols, such as BGP, RIP, OSPF, and IS-IS</li> <li>● Inter-AS VPN <ul style="list-style-type: none"> <li>– VPN instance to VPN instance, also called Inter-Provider Backbones Option A</li> <li>In Option A, sub-interfaces connecting the autonomous system boundary routers (ASBRs) are used to manage VPN routes.</li> <li>– EBGP redistribution of labeled VPN-IPv4 routes, also called Inter-Provider Backbones Option B</li> <li>In Option B, ASBRs advertise labeled VPN-IPv4 routes to each other using MP-EBGP.</li> <li>– Multi-hop EBGP redistribution of labeled VPN-IPv4 routes, also called Inter-Provider Backbones Option C</li> <li>In Option C, PEs advertise labeled VPN-IPv4 routes to each other using Multihop MP-EBGP.</li> </ul> </li> <li>● Multicast VPN</li> <li>● IPv6 VPN and dual-stack VPN</li> <li>● IPv6 inter-AS VPN (Option A, B, or C)</li> <li>● HVPN+ (H-VPN and HoVPN)</li> <li>● Popgo action on an IPv4 public network</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	VPN Features	EVPN	<p>Ethernet virtual private network (EVPN) is used for Layer 2 internetworking. EVPN is similar to BGP/MPLS IP VPN. Using extended BGP reachability information, EVPN implements MAC address learning and advertisement between Layer 2 networks at different sites on the control plane instead of on the data plane.</p> <p>EVPN offers the following benefits:</p> <ul style="list-style-type: none"> <li>● Improved link usage and transmission efficiency: EVPN supports load balancing, fully utilizing network resources and reducing network congestion.</li> <li>● Reduced network resource consumption: By deploying RRs on the public network, EVPN decreases the number of logical connections required between PEs on the public network. In addition, EVPN enables PEs to use locally stored MAC addresses to respond to ARP Request messages from connected sites, minimizing the number of broadcast ARP Request messages.</li> </ul> <p>Supported EVPN functions:</p> <p>The following deployment models are supported:</p> <ul style="list-style-type: none"> <li>● EVPN E-Line</li> <li>● EVPN E-LAN</li> <li>● EVPN E-Tree (local AC isolation)</li> <li>● Access to EVPN through VLL</li> <li>● VPLS through EVPN</li> <li>● Access to EVPN through VXLAN</li> <li>● PBB EVPN</li> <li>● EVPN L3VPN</li> <li>● EVPN L3VPNv6</li> </ul> <p>The following basic functions are supported:</p> <ul style="list-style-type: none"> <li>● Unicast traffic forwarding</li> <li>● BUM traffic forwarding</li> <li>● Unicast traffic load-balancing</li> <li>● Inter-AS VPN Option B</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	VPN Features	L2TPv3	<p>L2TPv3 over IPv6 establishes an IPv6-based L2TPv3 tunnel that transparently transmits Layer 2 user packets to remote ends over an IPv6 network. L2TPv3 over IPv6, which establishes tunnels based on static configurations, does not require dynamic negotiation for tunnel establishment or teardown.</p> <ul style="list-style-type: none"> <li>• Users can access an L2TPv3 tunnel in whole-interface mode.</li> <li>• Users can access an L2TPv3 tunnel in C-tag termination mode.</li> <li>• Users can access an L2TPv3 tunnel in S-tag termination mode.</li> <li>• Users can access an L2TPv3 tunnel in S-tag+C-tag termination mode.</li> <li>• Local packet switching is supported.</li> <li>• Packet injection is supported.</li> </ul>
Service Features	VPN Features	IP Hard Pipe	<p>IP hard pipe is an end-to-end bandwidth guarantee solution that divides the network bandwidth into two parts, one for the hard pipe and the other for the soft pipe. The hard and soft pipes are isolated and cannot preempt the bandwidth of each other. This guarantees bandwidth and low delay for traffic entering the hard pipe. Currently, only static PW services can be transmitted through the hard pipe.</p> <p>The following functions are supported:</p> <ul style="list-style-type: none"> <li>• Point-to-point IP hard pipe (VLL IP hard pipe)</li> <li>• Point-to-multipoint IP hard pipe (VPLS IP hard pipe)</li> </ul>
Service Features	QoS	DiffServ Model	<p>Multiple service flows can be aggregated into a behavior aggregate (BA) and then processed based on the same per-hop behavior (PHB). This simplifies the processing and storage of services.</p> <p>On a core network that uses the DiffServ model, packet-specific QoS is provided. Therefore, signaling processing is not required.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	BA Classification	<p>BA classifies data packets into multiple priorities or service classes. If the IP precedence, the first three bits of the ToS field in the IP header, is used to mark packets, the packets can be classified into a maximum of eight classes. If the differentiated services code point (DSCP), the first six bits of the ToS field, is used to mark packets, the packets can be classified into a maximum of 64 classes. After the packets are classified, QoS features can be applied to different classifiers to implement classifier-based congestion management and traffic shaping.</p> <p>The network administrator can set BA policies for packets based on the IP preference or DSCP values of IP packets, EXP values of MPLS packets, and 802.1p priorities of VLAN packets.</p> <p>The NetEngine 8000 F1A supports BA classification on Ethernet interfaces, Ethernet sub-interfaces, Layer 2 Ethernet interfaces, Eth-Trunk interfaces, Eth-Trunk sub-interfaces, Layer 2 Eth-Trunk interfaces, QinQ VLAN tag termination sub-interfaces, dot1q VLAN tag termination sub-interfaces, QinQ stacking interfaces, VE interfaces, .</p> <ul style="list-style-type: none"> <li>● Layer 2 BA classification                     <p>The NetEngine 8000 F1A performs BA classification based on 802.1p priorities of VLAN packets. The ingress PE maps the 802.1p priority of a Layer 2 packet to an upper-layer priority value (such as the IP DSCP and MPLS EXP value) so that DiffServ is also implemented for the packet after it enters the backbone network. The egress PE then maps the upper-layer priority value back to the 802.1p priority.</p> </li> <li>● QinQ BA classification                     <p>QinQ requires the 802.1p priorities in both inner and outer VLAN tags to be detected. The NetEngine 8000 F1A can process the 802.1p priority as follows:</p> <ul style="list-style-type: none"> <li>- Ignore the 802.1p priority in the inner VLAN tag and set a new 802.1p value in the outer VLAN tag.</li> <li>- Copy the 802.1p priority in the inner VLAN tag to the outer VLAN tag.</li> <li>- Set a new 802.1p priority in the outer VLAN tag based on the 802.1p priority in the inner VLAN tag.</li> </ul> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>QinQ supports 802.1p re-marking in the following modes:</p> <ul style="list-style-type: none"> <li>- Specify a value.</li> <li>- Use the 802.1p priority in the inner VLAN tag.</li> <li>- Map the 802.1p priority in the inner VLAN tag to the 802.1p value in the outer VLAN tag. The 802.1p priorities in multiple inner VLAN tags of different packets can be mapped to the 802.1p value in one outer VLAN tag, whereas the 802.1p priority in one inner VLAN tag cannot be mapped to the 802.1p priorities in multiple outer VLAN tags of different packets.</li> </ul>
Service Features	QoS	MF Classification	<p>The device performs multi-field (MF) classification based on the following information:</p> <ul style="list-style-type: none"> <li>• Layer 2 and Layer 3 information carried in packets</li> <li>• Source MAC address, destination MAC address, link layer protocol number, and 802.1p priority (of tagged packets) in the Ethernet frame header; IP precedence/DSCP value/ToS value, source IP address prefix, destination IP address prefix, protocol number, fragmentation flag, TCP SYN flag, TCP/UDP source port number or port range, and TCP/UDP destination port number or port range of IPv4 packets</li> <li>• Information carried in MPLS packets</li> </ul> <p>The device supports MF classification on Ethernet interfaces, Ethernet sub-interfaces, Layer 2 Ethernet interfaces, Eth-Trunk interfaces, Eth-Trunk sub-interfaces, Layer 2 Eth-Trunk interfaces, QinQ VLAN tag termination sub-interfaces, dot1q VLAN tag termination sub-interfaces, VE interfaces, and QinQ stacking sub-interfaces.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	Traffic Policing	<p>Traffic policing controls the rate of incoming packets to ensure that network resources are properly allocated. Committed access rate (CAR) is a traffic policing technique that uses token buckets to measure data flows. Only data flows assigned tokens within a specified period are permitted to pass through. Only data flows assigned tokens within a specified period are permitted to pass through. In addition, the rate of specific types of data flows can be limited based on information, such as the IP address, interface number, and priority. Rate limiting is not performed on data flows that do not meet the specified conditions, and these data flows are forwarded at the original interface rate.</p> <p>CAR is implemented at the network edge to ensure data processing on core devices. The NetEngine 8000 F1A supports CAR for both incoming and outgoing traffic.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	Traffic Shaping	<p>Traffic shaping uses generic traffic shaping (GTS) to shape traffic that is irregular or does not conform to preset traffic features to ensure that traffic is transmitted at an even rate. This improves the allocation of bandwidth resources between the upstream and downstream networks.</p> <p>The NetEngine 8000 F1A supports traffic shaping only on the outbound interface.</p> <ul style="list-style-type: none"> <li>• Different shaping parameters can be configured for packets based on service classes (EF, AF1, AF2, AF3, AF4, BE, CS6, or CS7).</li> <li>• GTS queues can use priority queuing (PQ) or weighted fair queuing (WFQ) scheduling algorithm. Packets with different service levels in GTS queues have different default scheduling modes. <ul style="list-style-type: none"> <li>– For AF1 to AF4 queues and BE queues, WFQ scheduling is configured by default. Bandwidth is allocated based on the configured weight values.</li> <li>– For EF, CS6, and CS7 queues, PQ scheduling is configured by default. PQ scheduling is performed based on priorities, and therefore is applicable to delay-sensitive services.</li> </ul> </li> <li>• When GTS queues use WFQ scheduling, weight values can be configured for services of different priorities in WFQ queues or the bandwidth ratio for each type of flow can be configured.</li> <li>• Shaping values can be configured on interfaces. A shaping value is the rate at which tokens enter the token bucket. If the packet rate exceeds the shaping value, the packets are cached in the GTS queue.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	Queue Scheduling	<p>The NetEngine 8000 F1A supports PQ, WFQ, and LPQ for queue scheduling on interfaces.</p> <p>The NetEngine 8000 F1A maps packets with different priorities to different queues and uses the round robin (RR) algorithm for queue scheduling on each interface.</p> <p>PQ schedules packets in descending order of priority. When packets leave queues, the queue with the highest priority is served first until it is empty, then the queues with lower priorities are served in sequence. PQ provides absolute preferential treatment to high priority traffic, ensuring that mission-critical service traffic gets priority treatment. When the network is idle, non-critical service traffic is transmitted. This implementation ensures that the quality of key services is guaranteed, and the network resources are fully utilized.</p> <p>WFQ is a complex queuing process, which ensures that services with the same priority are fairly treated and services with different priorities are weighted. WFQ ensures fairness (bandwidth and delay) and provides weights. The weights are configurable. The value of this parameter depends on the value of (precedence) in the IP packet header. WFQ dynamically classifies packets based on the quintuple information (or ToS field value). Packets with the same source IP address, destination IP address, source port number, destination port number, protocol number, and ToS value belong to the same flow. Each flow is assigned to a queue. This process is called hash. WFQ uses the hash algorithm to automatically add flows to different queues. When a flow leaves a queue, WFQ allocates the egress bandwidth to the flow based on the flow priority (precedence). The smaller the value of the priority, the less the bandwidth is allocated. A larger value indicates a higher bandwidth. In this way, the fairness between services of the same priority is ensured, and the weight between services of different priorities is reflected.</p> <p>Low priority queuing (LPQ) is performed after PQ and WFQ scheduling is complete. LPQ also schedules packets based on priorities in descending order.</p>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	Congestion Avoidance	<p>Congestion avoidance is a flow control technique used to relieve network overload. By monitoring the usage of network resources for queues or memory buffers, the device automatically drops packets on interfaces that show signs of traffic congestion.</p> <p>Random early detection (RED) and weighted random early detection (WRED) algorithms are frequently used to avoid congestion.</p> <p>RED sets the upper and lower limits for each queue and specifies the following rules:</p> <ul style="list-style-type: none"> <li>• When a queue length is below the lower limit, no incoming packets are discarded.</li> <li>• When a queue length exceeds the upper limit, all incoming packets are discarded.</li> <li>• When a queue length is between the lower and upper limits, incoming packets are discarded randomly. A random number is assigned to each received packet, and the random number is compared with the drop probability of the current queue. If the random number assigned to the packet is greater than the drop probability, the packet is discarded. The longer the queue, the higher the drop probability. The drop probability, however, has an upper limit.</li> </ul> <p>Unlike RED, the random number in WRED is based on the IP precedence of packets. WRED uses a lower drop probability for packets with higher IP precedence.</p> <p>RED and WRED employ the random packet drop policy to avoid global TCP synchronization. The NetEngine 8000 F1A uses WRED to implement congestion avoidance.</p> <p>The NetEngine 8000 F1A supports congestion avoidance in both inbound and outbound directions of an interface. The WRED template is applied in the outbound direction; the default scheduling policy of the system is applied in the inbound direction. In addition, the NetEngine 8000 F1A supports WRED application to the multicast tunnel interface (MTI) bound to the distributed multicast VPN on the device.</p> <p>The NetEngine 8000 F1A supports service-based congestion avoidance and reserves eight service queues on each interface: BE, AF1, AF2, AF3, AF4, EF, CS6, and CS7. The NetEngine 8000 F1A colors packets red, yellow, or green to indicate their drop priorities.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	QoS	HQoS	<p>The NetEngine 8000 F1A supports the following HQoS functions:</p> <ul style="list-style-type: none"> <li>• Provides four scheduling levels to ensure diverse services.</li> <li>• Sets flow queue parameters, such as the maximum queue length, WRED, low delay, SP/WRR, CBS, PBS, and statistics function.</li> <li>• Sets parameters, such as the CIR, PIR, and queue scheduling algorithm, for each user.</li> <li>• Provides the traffic statistics function, which allows users to query the bandwidth usage of services and accordingly distribute bandwidth properly after traffic analysis.</li> <li>• Supports interface-based HQoS in VPLS, L3VPN, VLL, and TE scenarios.</li> <li>• Supports interface-based, VLAN-based, user-based, and service-based HQoS.</li> </ul>
Service Features	QoS	MPLS QoS	<p>MPLS HQoS is a complete L2VPN/L3VPN QoS solution that uses various QoS techniques to meet the diversified and fine-granular QoS demands of VPN users. MPLS HQoS provides relative QoS on MPLS DiffServ networks and end-to-end QoS on MPLS TE networks. Select any of the following based on your networking requirements:</p> <ul style="list-style-type: none"> <li>• MPLS DiffServ: applies to an L2VPN/L3VPN.</li> <li>• MPLS TE: applies to an L2VPN/L3VPN.</li> <li>• VLL HQoS: implements priority-based scheduling and rate limit management for services in a VLL and traffic bandwidth management for the entire VLL.</li> </ul>
Service Features	Load Balancing	Equal-cost load balancing	<p>The NetEngine 8000 F1A can implement equal-cost load balancing on traffic transmitted through trunk member links. When multiple equal-cost routes are available to a destination, the NetEngine 8000 F1A can evenly balance traffic among these routes.</p> <p>The NetEngine 8000 F1A supports per-flow load balancing.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Load Balancing	UCMP	<p>The NetEngine 8000 F1A supports the following UCMP modes:</p> <ul style="list-style-type: none"> <li>• Load balancing based on routes If direct routes have the same cost, a weight can be configured for each route for load balancing.</li> <li>• Load balancing based on interfaces A weight can be configured for each trunk member link for load balancing.</li> <li>• Load balancing based on link bandwidth for IGP: In this mode, unequal-cost session-by-session load balancing is performed on the outbound interfaces of paths. The proportion of traffic transmitted along each path is approximate to or equal to the proportion of bandwidth of each link. This mode fully considers the link bandwidth. In this manner, the case when links with low bandwidth are overloaded whereas links with high bandwidth are idle does not exist.</li> </ul> <p>The NetEngine 8000 F1A can balance traffic between physical interfaces or between physical and logical interfaces. In addition, the device can detect logical interface bandwidth changes that occur due to manual configuration of new member links or status changes of member links. When the bandwidth of a logical interface changes, traffic is automatically load-balanced based on the new bandwidth proportion.</p>
Service Features	Traffic Statistics	URPF Traffic Statistics	The NetEngine 8000 F1A can collect statistics about URPF-compliant traffic and URPF denied traffic that is discarded.
Service Features	Traffic Statistics	ACL Traffic Statistics	The NetEngine 8000 F1A supports ACL traffic statistics collection. When an ACL is created and applied to QoS and PBR, after the ACL traffic statistics collection is enabled, the NetEngine 8000 F1A collects statistics based on the ACL number. In addition, commands are provided to query the number of ACL matches and the number of matched packets and bytes.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Traffic Statistics	CAR Traffic Statistics	<p>The NetEngine 8000 F1A provides diverse QoS functions, such as traffic classification, traffic policing (using CAR), and queue scheduling. For these specific functions, the NetEngine 8000 F1A supports the following QoS traffic statistics functions:</p> <ul style="list-style-type: none"> <li>• In traffic classification, the device can collect statistics about the traffic that matches or does not match traffic classification rules.</li> <li>• The traffic statistics function for traffic policing is implemented in the following manners: <ul style="list-style-type: none"> <li>– Collects statistics about all traffic that matches CAR.</li> <li>– Collects statistics about traffic that is permitted or discarded by CAR.</li> <li>– Collects traffic statistics based on interfaces.</li> <li>– Collects CAR traffic statistics based on interfaces if the same traffic policy is applied to different interfaces.</li> </ul> </li> </ul>
Service Features	Traffic Statistics	HQoS Traffic Statistics	<ul style="list-style-type: none"> <li>• Number of forwarded packets, bytes, and discarded packets of a user queue, which includes eight flow queues (each with a different priority)</li> <li>• Number of forwarded packets, bytes, and discarded packets of a user group queue</li> <li>• Number of forwarded packets, bytes, and discarded packets of eight flow queues on an interface</li> </ul>
Service Features	Traffic Statistics	Interface Traffic Statistics	<p>Traffic statistics can be collected on all interfaces, including physical interfaces, sub-interfaces, loopback interfaces, null interfaces, logical channel interfaces, and virtual Ethernet interfaces.</p> <p>Statistics on all supported protocol packets can be collected, including MPLS, ARP, IGP, BGP, PIM, and DHCP packets.</p>
Service Features	Traffic Statistics	TE Tunnel Traffic Statistics	<p>When the NetEngine 8000 F1A functions as a PE on an MPLS TE network, it can collect statistics about incoming and outgoing traffic of a tunnel. When a VPN is statically bound to a TE tunnel, the device can collect statistics about the traffic of each VPN and all traffic carried over the TE tunnel.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	Security Authentication	<p>The NetEngine 8000 F1A supports the following features:</p> <ul style="list-style-type: none"> <li>• AAA</li> <li>• Simple text authentication and MD5 ciphertext authentication supported by routing protocols (RIPv2, OSPF, IS-IS, and BGP)</li> </ul> <p><b>NOTE</b> The encryption algorithm MD5 has a low security, which may bring security risks. If protocols allowed, using more secure encryption algorithms.</p> <ul style="list-style-type: none"> <li>• MD5 ciphertext authentication supported by LDP and RSVP</li> <li>• SNMPv3 encryption and authentication</li> </ul>
Service Features	Security	URPF	The device supports URPF for IPv4/IPv6 traffic.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	MAC Address Limit	<p>The NetEngine 8000 F1A supports the following MAC address limit functions:</p> <ul style="list-style-type: none"> <li>● Limit on the maximum number of MAC addresses that can be learned</li> <li>● Limit on the rate at which MAC addresses can be learned</li> <li>● Limit on interface-based MAC address learning</li> <li>● Limit on PW-based MAC address learning</li> <li>● Limit on VLAN+interface-based MAC address learning</li> <li>● Limit on interface+VSI-based MAC address learning</li> <li>● Limit on QinQ-based MAC address learning</li> </ul> <p>MAC entries in a MAC address table are categorized into three types.</p> <ul style="list-style-type: none"> <li>● Dynamic entries Dynamic entries are learned by interfaces and stored in of the device. Dynamic entries can age and will be lost when the system is reset.</li> <li>● Static entries Static entries are manually configured and delivered to the device. Static entries do not age. After static entries are configured and saved, they are not lost when the system is reset.</li> <li>● Black hole entries Black hole entries are also manually configured and delivered to the device. They are used to filter out data frames with specific destination MAC addresses. Black-hole entries do not age. After black-hole entries are configured and saved, they are not lost when the system is reset.</li> </ul>
Service Features	Security	MAC Entry Deletion	<p>The NetEngine 8000 F1A supports the following MAC entry deletion functions:</p> <ul style="list-style-type: none"> <li>● Interface+VSI-based MAC entry deletion</li> <li>● Interface+VLAN-based MAC entry deletion</li> <li>● Trunk-based MAC entry deletion</li> <li>● Outbound QinQ interface-based MAC entry deletion</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	Unknown Traffic Limit	<p>The NetEngine 8000 F1A provides unknown traffic limits to implement the following functions on a VPLS or Layer 2 network:</p> <ul style="list-style-type: none"> <li>• User traffic management</li> <li>• User-specific bandwidth allocation</li> </ul> <p>This function maximizes network bandwidth usage and ensures network security.</p>
Service Features	Security	IGMP Snooping	The NetEngine 8000 F1A supports IGMP snooping on Layer 2 interfaces and VPLS PWs.
Service Features	Security	MLD Snooping	The NetEngine 8000 F1A supports MLD snooping on Layer 2 interfaces and VPLS PWs.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	Local Attack Defense	<p>The NetEngine 8000 F1A provides a local attack defense module to manage and maintain the attack defense policies of the entire system, offering an all-around attack defense solution.</p> <p>The NetEngine 8000 F1A supports the following features:</p> <ul style="list-style-type: none"> <li>● Whitelist</li> <li>● Blacklist</li> <li>● CPU total CAR</li> <li>● User-defined flow</li> <li>● Active link protection (ALP)</li> </ul> <p>The NetEngine 8000 F1A uses the whitelist to protect TCP-based application-layer session data.</p> <ul style="list-style-type: none"> <li>● Uniform configuration of CAR parameters</li> </ul> <p>The NetEngine 8000 F1A supports the following methods for configuring CAR parameters:</p> <ul style="list-style-type: none"> <li>- Uniform configuration GUI for users</li> <li>- Configuration of protocol-specific CAR parameters, making the GUI more user-friendly</li> </ul> <ul style="list-style-type: none"> <li>● Smallest packet compensation</li> </ul> <p>The NetEngine 8000 F1A provides the smallest packet compensation function to effectively defend against network attacks using small packets. After the device receives packets to be sent to the CPU, it checks the packet length.</p> <ul style="list-style-type: none"> <li>- If the packet length is smaller than the preset minimum packet length, the device calculates the packet transmission rate based on the preset minimum length.</li> <li>- If the packet length is greater than the preset minimum packet length, the device calculates the packet transmission rate based on the actual packet length.</li> </ul> <ul style="list-style-type: none"> <li>● Association between the application layer and lower layers</li> <li>● Interface URPF</li> <li>● Management and service plane protection</li> <li>● Discarding and rate limit based on the TTL range</li> <li>● TCP/IP packet attack defense</li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>The NetEngine 8000 F1A defends against attacks by sending the following types of packets on TCP/IP networks:</p> <ul style="list-style-type: none"> <li>- Malformed packets Malformed packets include IGMP null payload packets, packets with invalid TCP flag bits, LAND attack packets, IP null payload packets, and Smurf attack packets.</li> <li>- Fragmented packets Fragmented packet attacks can be launched by a large number of fragments, packets that have a large offset value, or repetitive fragmented packets. Fragmented packet attacks include Tear Drop, syndrop, nesta, fawx, bonk, NewTear, Rose, ping of death, and Jolt attacks.</li> <li>- TCP SYN packets</li> <li>- UDP flood packets</li> <li>● Attack source tracing When the NetEngine 8000 F1A is attacked, it obtains and stores suspicious packets and then displays the packets in a certain format using command lines or offline tools. This makes locating the attack source easier. When attacks occur, the system automatically removes the data encapsulated at upper layers of the transmission layer and then caches the packets in memory. When a specified number of packets are cached, the earliest cached packets are overwritten when more packets are cached.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	GTSM	<p>Attackers forge valid packets to attack routers, which overloads the routers and consumes limited resources, such as CPU resources. For example, an attacker forges BGP protocol packets and continuously sends them to a router. After the forwarding plane of the router receives the packets, it finds that the packets are destined for itself and then sends the packets directly to the BGP processing module on the main control board without checking the validity of the packets. As a result, the system is busy processing these forged valid packets, and the CPU usage increases rapidly.</p> <p>To prevent the preceding attacks, the NetEngine 8000 F1A provides the GTSM mechanism. GTSM protects services above the IP layer by checking whether the time to live (TTL) value in the IP header is within a predefined range. In actual applications, GTSM is mainly used to protect the TCP/IP-based control plane (routing protocol) against CPU-utilization attacks, such as CPU overload.</p> <p>The NetEngine 8000 F1A supports BGP GTSM, OSPF GTSM, and LDP GTSM.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	ARP Attack Defense	<p>The NetEngine 8000 F1A supports the following features:</p> <ul style="list-style-type: none"> <li>● Interface-based ARP entry limit</li> <li>● Timestamp suppression based on the source and destination IP addresses of ARP packets</li> <li>● Destination IP address check for ARP packets</li> </ul> <p>The system checks the destination IP addresses of received ARP packets. If the destination IP address of a packet is correct, the system sends it to the CPU; otherwise, the system discards the packet.</p> <ul style="list-style-type: none"> <li>● ARP bidirectional isolation</li> <li>● ARP packet filtering</li> </ul> <p>The NetEngine 8000 F1A filters out the following types of ARP packets:</p> <ul style="list-style-type: none"> <li>- Invalid ARP packets</li> </ul> <p>Invalid ARP packets include ARP request packets with destination MAC addresses as unicast addresses, ARP request packets with source MAC addresses as non-unicast addresses, and ARP reply packets with destination MAC addresses as non-unicast addresses.</p> <ul style="list-style-type: none"> <li>- Gratuitous ARP packets</li> <li>- ARP request packets with non-null destination MAC addresses</li> </ul> <p>The preceding types of packets can be filtered out simultaneously.</p>
Service Features	Security	Local Mirroring	<p>Local mirroring allows to have a physical observing port, multiple logical observing ports, and multiple mirrored ports configured.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	Netstream	<p><b>NOTE</b></p> <p>The NetStream feature may be used to analyze the communication information of terminal customers for network traffic statistics and management purposes. Before enabling the NetStream feature, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.</p> <p>NetStream supports the following functions:</p> <ul style="list-style-type: none"> <li>• Accounting</li> <li>• Network planning and analysis</li> <li>• Network monitoring</li> <li>• Application monitoring and analysis</li> <li>• Abnormal traffic detection</li> </ul> <p>NetStream involves three devices: NetStream Data Exporter (NDE), NetStream Collector (NSC), and NetStream Data Analyzer (NDA). The NetEngine 8000 F1A functions as an NDE to sample packets and aggregate and output flows.</p> <p>The NetEngine 8000 F1A supports the following sampling functions:</p> <ul style="list-style-type: none"> <li>• Sampling on inbound and outbound interfaces</li> <li>• Sampling of IPv4 unicast/multicast packets, fragmented packets, MPLS packets, MPLS L3VPN packets, and IPv6 packets</li> <li>• Regular packet sampling, random packet sampling, sampling at regular time, and sampling at random time</li> <li>• Sampling on various types of physical and logical interfaces, including Ethernet interfaces, VLAN sub-interfaces, and trunk interfaces</li> </ul> <p>The device supports the following aggregation and output functions:</p> <ul style="list-style-type: none"> <li>• IPv4 packets can be aggregated based on the AS number, AS-ToS, protocol-port, protocol-port-ToS, source-prefix, source-prefix-ToS, destination-prefix, destination-prefix-ToS, prefix, and prefix-ToS.</li> <li>• MPLS packets can be aggregated based on Layer 3 labels.</li> <li>• The generated statistics can be output in v5, v8, or v9 format with 16-bit or 32-bit AS numbers (set using commands). When packets are output in v9</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			format, both 16-bit and 32-bit interface indexes are supported and can be set.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Security	IPFIX	<p><b>NOTE</b></p> <p>Internet Protocol Flow Information Export (IPFIX) is compliant with the IETF RFC 7011, RFC 7012, RFC 7013, and RFC 7015 standards. For details about security risks, see relevant descriptions in these standards. This function can be used to analyze communication contents of specific target users for maintenance and operation purposes. Strictly observe the local law when using this function. When collecting and storing communication contents of specific users, ensure that the contents are profoundly protected.</p> <p>IPFIX supports the following functions:</p> <ul style="list-style-type: none"> <li>● Accounting</li> <li>● Network planning and analysis</li> <li>● Network monitoring</li> <li>● Application monitoring and analysis</li> <li>● Detection of unusual traffic</li> </ul> <p>The device supports the following sampling functions:</p> <ul style="list-style-type: none"> <li>● Packet sampling on inbound and outbound interfaces (some boards support packet sampling on inbound interface only)</li> <li>● Interface-based sampling and traffic-classifier-based sampling</li> <li>● Sampling of IPv4 unicast/multicast packets, fragmented packets, MPLS packets, MPLS L3VPN packets, and IPv6 packets</li> <li>● Fixed packet sampling, random packet sampling, and fixed interval sampling</li> <li>● Sampling on various physical and logical interfaces, such as Ethernet interfaces, VLAN sub-interfaces, and trunk interfaces.</li> </ul> <p>The device supports the following flow aggregation and output functions:</p> <ul style="list-style-type: none"> <li>● IPv4 packets can be aggregated based on the AS number, AS-ToS, protocol-port, protocol-port-ToS, source-prefix, source-prefix-ToS, destination-prefix, destination-prefix-ToS, prefix, and prefix-ToS.</li> <li>● IPv6 packets can be aggregated based on the AS number, AS-ToS, protocol-port, protocol-port-ToS, source-prefix, source-prefix-ToS, destination-prefix, destination-prefix-ToS, prefix, and prefix-ToS.</li> <li>● MPLS packets can be aggregated based on Layer 3 labels.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<ul style="list-style-type: none"> <li>Each type of aggregated flow can be output to a maximum of eight NMS servers.</li> </ul>
Service Features	Security	SSHv2	The NetEngine 8000 F1A supports the STelnet client and server and the SFTP client and server. Both SSHv1 (SSH1.5) and SSHv2 (SSH2.0) are supported.
Service Features	Security	Dynamic system integrity protection	<ul style="list-style-type: none"> <li>Digital signatures</li> <li>Trusted boot and secure boot</li> </ul>
Service Features	IP RAN Features	Plug and play	<p>Plug-and-Play (PnP) use DHCP to automatically configure and commission devices remotely.</p> <p>On an IP RAN deployed with a large number of devices, the device deployment costs, especially on-site software commissioning, are high. This greatly affects profits. To address this issue, Huawei launches a PnP solution for IP RANs.</p> <p>PnP effectively reduces the on-site software commissioning time and frees engineers from working in bad outdoor environments, which accelerates the project progress and improves the project quality.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	IP RAN Features	DCN	<p>The data communication network (DCN) refers to the network on which network elements (NEs) exchange Operation, Administration and Maintenance (OAM) information with the network management system (NMS). It is constructed for communication between managing and managed devices.</p> <p>The DCN technique offers a mechanism to implement plug-and-play. After an NE is installed and started, an IP address (NEIP address) mapped to the NEID of the NE is automatically generated. Each NE adds its NEID and NEIP address to a link state advertisement (LSA). Then, Open Shortest Path First (OSPF) advertises all Type-10 LSAs to construct a core routing table that contains mappings between NEIP addresses and NEIDs on each NE. After detecting a new NE, the GNE reports the NE to the NMS. The NMS accesses the NE using the IP address of the GNE and ID of the NE. To commission NEs, the NMS can use the GNE to remotely manage the NEs on the network.</p> <p>Data communication network (DCN) automatically discover NEs and manage NEs using service channels provided by the managed NEs. No additional devices are required, reducing operation costs.</p>
Service Features	IP RAN Features	Y.1731	<p>Y.1731 supports the following functions:</p> <ul style="list-style-type: none"> <li>● Single-ended frame loss measurement</li> <li>● Dual-ended frame loss measurement</li> <li>● One-way frame delay measurement</li> <li>● Two-way frame delay measurement</li> <li>● One-way jitter</li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Network Reliability	FRR	<p>The NetEngine 8000 F1A provides multiple fast reroute (FRR) features, which can be deployed as required to improve network reliability.</p> <ul style="list-style-type: none"> <li>● IP FRR                     <p>IP FRR switching can be completed in 50 ms, minimizing data loss when network failures occur.</p> <p>The NetEngine 8000 F1A supports IP FRR, enabling the system to monitor and save the status of boards and interfaces in real time and to check the interface status during packet forwarding. If a fault occurs on an interface, the NetEngine 8000 F1A can rapidly switch traffic to another preset route. In this manner, the mean time between failures (MTBF) is prolonged and the packet loss rate is reduced.</p> </li> <li>● LDP FRR                     <p>LDP FRR switching can be completed in 50 ms.</p> <p>LDP remote LFA: calculates a remote LFA route using a routing protocol and establishes a remote LDP session over the route and an LSP over the session so that an FRR protection path can be established. LDP remote LFA switching is performed within 50 ms.</p> </li> <li>● TE FRR                     <p>TE FRR is an MPLS TE technology that protects local networks. Only interfaces with transmission rates of over 100 Mbit/s support TE FRR. TE FRR switching can be completed in 50 ms, which minimizes data loss if network failures occur.</p> <p>TE FRR only temporarily protects traffic. When the protected LSP becomes normal or a new LSP is established, traffic switches back to the original protected LSP or the new LSP.</p> <p>After TE FRR is configured for an LSP, if a link or node on the LSP fails, traffic is switched to the protection link, and the ingress on the LSP attempts to establish a new LSP.</p> <p>TE FRR is classified into the following types:</p> <ul style="list-style-type: none"> <li>- Link protection</li> <li>- Node protection</li> </ul> </li> <li>● Auto FRR                     <p>Auto FRR extends MPLS TE FRR working in facility backup mode. It automatically creates a bypass</p> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			<p>tunnel that meets the requirements for the LSP by configuring the attributes of the bypass tunnel, global auto FRR attributes, and interface-based auto FRR attributes on the interface of the primary tunnel. When the primary tunnel changes to another path, the previous bypass tunnel is automatically deleted. Then a bypass tunnel that meets the requirements is set up.</p> <ul style="list-style-type: none"> <li>● VPN FRR VPN FRR is a technique that allows a device to fast switch VPN routes by presetting and using master and backup forwarding entries on the remote PE (which correspond to the master and backup PEs, respectively), combined with fast detection of PE failures. VPN FRR prevents the issue where E2E service convergence caused by a PE failure lasts more than 1 second and the issue where the service restoration time for a faulty PE relies on the number of VPN routes in the routing table of the PE on an MPLS VPN where a CE is dual-homed to PEs. After VPN FRR is configured on the PEs, E2E service convergence takes less than 1 second in the event of a PE failure. VPN FRR provides fast service convergence after a node on a tunnel fails, irrespective of the number of VPN routes in the routing table of the node. In addition, VPN FRR is simple, reliable, and easy to deploy. Except for fast detection of PE failures, VPN FRR does not require assistance of adjacent devices.</li> <li>● VLL FRR VLL FRR switching can be completed in 50 ms.</li> <li>● Multicast FRR</li> </ul>
Service Features	Network Reliability	Dual-System Hot Backup	The NetEngine 8000 F1A supports ARP dual-system 1+1 or 1:1 hot backup.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Network Reliability	Transmission Alarm Customization and Suppression	<p>Transmission alarm suppression can efficiently filter and suppress alarms, preventing frequent interface flapping. In addition, transmission alarm customization allows the system to effectively control the impact of alarms on the interface status.</p> <p>Transmission alarm suppression and customization implement the following functions:</p> <ul style="list-style-type: none"> <li>• Customizes alarms by specifying the alarms that can cause interface status changes.</li> <li>• Suppresses alarms to filter out the burr and prevent frequent network flapping.</li> </ul>
Service Features	Network Reliability	Ethernet OAM Fault Management	<p>Ethernet OAM fault management includes the following functions:</p> <ul style="list-style-type: none"> <li>• Ethernet in the First Mile OAM (EFM OAM) NetEngine 8000 F1A EFM OAM is a point-to-point Ethernet fault management technique defined in IEEE 802.3ah for detecting faults in the last mile of the direct link on the user side of the Ethernet. The NetEngine 8000 F1A supports EFM OAM functions, including OAM discovery, link monitoring, remote fault notification, and remote loopback.</li> <li>• CFM OAM is an end-to-end Ethernet fault management technique defined in IEEE 802.1ag for fault detection and location. CFM OAM supports hierarchical MDs. Each MD has a level that ranges from 0 to 7. The greater the value, the higher the level. 802.1ag packets from a low-level MD are discarded in a high-level MD. 802.1ag packets from a high-level MD can be transmitted through a low-level MD.</li> </ul>
Service Features	Network Reliability	VRRP	<p>VRRP dynamically associates a virtual router with a physical router that carries services. If the physical router fails, another router is elected to take over services. The failover is transparent to users, and therefore the internal and external networks can communicate without interruption.</p> <p>The NetEngine 8000 F1A supports the following VRRP functions:</p> <ul style="list-style-type: none"> <li>• mVRRP</li> <li>• E-VRRP</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Network Reliability	GR	<p>Graceful restart (GR) is a key technology used to implement high availability (HA). It is designed based on NSF.</p> <p>The NetEngine 8000 F1A supports system-level GR and protocol-level GR. Protocol-level GR includes:</p> <p>Protocol-level GR includes:</p> <ul style="list-style-type: none"> <li>• BGP GR helper</li> <li>• OSPF GR helper</li> <li>• IS-IS GR helper</li> <li>• MPLS LDP GR helper</li> <li>• Martini VLL GR helper</li> <li>• Martini VPLS GR helper</li> <li>• L3VPN GR helper</li> <li>• RSVP GR helper</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Network Reliability	BFD	<p>BFD is a detection mechanism used to monitor and rapidly detect the connectivity of network-wide links or IP routes.</p> <p>BFD sends detection packets simultaneously from both ends of a bidirectional link to check the link status in both directions. BFD can detect link faults within milliseconds. The device supports single-hop and multi-hop BFD.</p> <p>The NetEngine 8000 F1A supports the following BFD applications:</p> <ul style="list-style-type: none"> <li>● BFD for VRRP                     <p>The system uses BFD to detect and monitor the connectivity of links or IP routes on a network, triggering fast VRRP switchover.</p> </li> <li>● BFD for FRR                     <ul style="list-style-type: none"> <li>– BFD for LDP FRR                             <p>LDP FRR switchover is triggered after BFD detects faults on protected interfaces.</p> </li> <li>– BFD for IP FRR and BFD for VPN FRR                             <p>IP FRR and VPN FRR are triggered after BFD detects faults on the NetEngine 8000 F1A and reports fault information to upper layer applications.</p> </li> </ul> </li> <li>● BFD for static routes</li> <li>● BFD for IS-IS                     <p>The NetEngine 8000 F1A can use static BFD sessions to detect IS-IS neighbor relationships. BFD detects the fault of the link between the adjacent IS-IS nodes and rapidly reports the fault to the IS-IS module. Thus fast convergence of IS-IS routes is performed.</p> </li> <li>● BFD for OSPF/BGP                     <p>The device supports OSPF and BGP for dynamically setting up and deleting BFD sessions.</p> </li> <li>● BFD for PIM</li> <li>● BFD for trunk                     <p>The NetEngine 8000 F1A can use BFD to monitor the connectivity of a trunk interface and its member links separately.</p> </li> <li>● BFD for LSP                     <p>BFD for LSP performs fast fault detection of LSPs, TE tunnels, and PWs, and subsequently implements</p> </li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
			fast switchover of MPLS services, such as VPN FRR, TE FRR, and VLL FRR. <ul style="list-style-type: none"> <li>● BFD for dot1q sub-interfaces</li> <li>● BFD for mVSI</li> <li>● Multi-hop BFD</li> <li>● BFD for VPLS PW</li> <li>● BFD for VPLS/VLL PW</li> <li>● VPLS over LDP FRR/FW unicast</li> <li>● BFD protocol packet authentication</li> </ul>
Service Features	Network Reliability	BFD Bit-Error-Triggered Protection Switching	If a bit error occurs on a traditional transmission network, services are dually fed and selectively received. Packets on links with low bit error rates are selectively received.  If a bit error occurs on an IP RAN, traditional detection mechanisms cannot trigger protection switching, and the base stations may go out of service. Bit-error-triggered protection switching can be configured to resolve this problem. Bit error-triggered protection switching uses BFD sessions to transmit bit errors of a link, triggering protection switching.
Service Features	Clock	Ethernet Clock Synchronization	Ethernet interfaces on the NetEngine 8000 F1A provide Ethernet clock synchronization to ensure clock quality and stratum on the network.

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Clock	1588v2	<p>The 1588v2 features are described as follows:</p> <ul style="list-style-type: none"> <li>• Supports input and output of externally synchronized time.</li> <li>• Supports OC, BC, E2ETC, P2PTC, E2ETCOC, P2PTCOC, and TCandBC.</li> <li>• Allows the device to function as a GrandMaster.</li> <li>• Supports slave-only mode when the device functions as an OC.</li> <li>• Supports the dynamic BMC algorithm.</li> <li>• Supports two delay measurement methods: Delay and PDelay</li> <li>• Supports one-step and two-step modes in which 1588v2 packets used by 1588v2 devices to perform time synchronization are timestamped.</li> <li>• Supports multicast MAC encapsulation (The VLAN ID and 802.1p priority are configurable).</li> <li>• Supports multicast UDP encapsulation (The source IP address, VLAN ID, and DSCP priority are configurable).</li> <li>• Supports unicast MAC encapsulation (The destination MAC address, VLAN ID, and 802.1p priority are configurable).</li> <li>• Supports unicast UDP encapsulation (The source IP address, destination IP address, destination MAC address, VLAN ID, and DSCP priority are configurable).</li> <li>• Uses the clock recovered using the Precision Time Protocol (PTP) as the clock source and supports the dynamic clock source selection algorithm (based on the clock priority and stratum).</li> <li>• Supports performance monitoring of passive ports on a 1588v2 device.</li> <li>• Implements back-to-back clock recovery in compliance with G.813 specifications.</li> <li>• Implements back-to-back clock recovery within 30 ns.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Clock	1588 ACR	<ul style="list-style-type: none"> <li>● Supports only frequency synchronization.</li> <li>● Supports clock source switching.</li> <li>● Supports unicast UDP encapsulation (with DSCP values).</li> <li>● Supports service modeling and networking in compliance with Recommendation G.8261 and performs clock recovery with G.823-compliant accuracy.</li> <li>● Supports the 1588 ACR server functionality.</li> <li>● Supports two-way frequency recovery mode.</li> </ul>



Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Clock	Network Time Protocol (NTP) clock	<p>The NetEngine 8000 F1A supports the following NTP working modes:</p> <ul style="list-style-type: none"> <li>• Client/server mode</li> <li>• Peer mode</li> <li>• Broadcast mode</li> <li>• Multicast mode</li> </ul> <p>The NetEngine 8000 F1A supports two NTP security mechanisms:</p> <ul style="list-style-type: none"> <li>• Access authority</li> </ul> <p>The NetEngine 8000 F1A provides four access control levels. After receiving an NTP access request packet, the device matches the packet against the access control list from the lowest access control level to the highest access control level. The first successfully matched access control level takes effect. The matching order is as follows:</p> <p>peer: minimum access control. The remote end can send a time request and a control query to the local end. The local clock can also be synchronized with the clock of the remote server.</p> <p>server: The remote end can send a time request and a control query to the local end. The local clock, however, is not synchronized with the clock of the remote server.</p> <p>synchronization: The remote end can only send a time request to the local end.</p> <p>query: maximum access control. The remote end can only send a control query to the local end.</p> <ul style="list-style-type: none"> <li>• Authentication</li> </ul> <p>When configuring NTP authentication, note the following rules:</p> <p>NTP authentication must be configured on both the client and server; otherwise, authentication does not take effect. If NTP authentication is enabled, keys must be configured and declared reliable.</p> <p>The client and server must have the same key configured.</p>
Service Features	Clock	Internal Clock	<p>The NetEngine 8000 F1A provides internal clocks. Clock information can be extracted from the . The precision is 4.6 ppm (0.00002s).</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Service Features	Clock	Extended SSM	<p>The NetEngine 8000 F1A supports the following extended SSM functions:</p> <ul style="list-style-type: none"> <li>• Sends and receives SSM information carrying clock IDs.</li> <li>• Configures a clock ID for a clock source.</li> <li>• Supports clock source selection based on extended SSM.</li> </ul>
Operation and Maintenance	Two-Phase Validation Mode	-	<p>In two-phase validation mode, the system configuration process is divided into two phases.</p> <ul style="list-style-type: none"> <li>• In the first phase, a user enters configuration commands. The system checks the data type, user level, and configuration object, and checks whether there are repeated configurations. If syntax or semantic errors are found in the command line, the system displays a message on the terminal to inform the user of the error and cause.</li> <li>• In the second phase, the user commits the configuration. The system then enters the configuration commitment phase and commits the configuration in the candidate database to the running database.</li> </ul>
Operation and Maintenance	System Configuration Modes	-	<p>The NetEngine 8000 F1A supports command line configuration.</p> <p>Command line configuration can be performed using either of the following:</p> <ul style="list-style-type: none"> <li>• Console interface</li> <li>• Telnet</li> </ul> <p>The console interface can be used as a command input interface to send command lines to the control plane.</p> <p>The console interface can also be used as a debugging interface to receive debugging information from the control and data planes and to deliver debugging and control commands.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	System Management and Maintenance	-	<p>The NetEngine 8000 F1A supports the following system management and maintenance functions:</p> <ul style="list-style-type: none"> <li>● Plug-and-play</li> <li>● Watchdog, board reset, RUN indicator control, fan and power supply control, system debugging, and version query</li> <li>● Local and remote software upgrading and data loading, version rollback, and data backup, saving, and clearing</li> <li>● Hierarchical user authority management, operation log management, command online help, and command comments</li> <li>● Three user authentication modes: local authentication, RADIUS authentication, and HWTACACS authentication, which authenticate and authorize users using commands and an SNMP-based NMS.</li> <li>● Multi-user operations</li> <li>● Layer 2 and Layer 3 interface information queries</li> <li>● Hierarchical alarm management, alarm classification, and alarm filtering</li> <li>● Support for the <b>shutdown</b> and <b>undo shutdown</b> commands on interfaces and optical modules</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	Device Running Status Monitoring	-	<p>The running status of the NetEngine 8000 F1A can be monitored through the information center. Syslog is a sub-function of the information center. Syslog uses UDP port 514 to output logs to log hosts.</p> <p>The information center can receive and process the following information:</p> <ul style="list-style-type: none"> <li>• Logs</li> <li>• Debugging information</li> <li>• Traps</li> </ul> <p>The information center supports 10 channels, of which channels 0 through 5 each have a default channel name. By default, the six channels correspond to six directions in which information is output. The log information on the CF card is output to log files through channel 9 by default. This means that a total of seven default output directions are supported.</p> <p>When multiple log hosts are available, you can configure log information to be output to different log hosts through one or more channels. For example, you can configure certain log information to be output to a log host through channel 2 (loghost), and certain log information to a log host through channel 6. In addition, you can change the name of channel 6 to facilitate channel management.</p> <p>The NetEngine 8000 F1A stores all traps in a log file and provides the CF card to store the log file. The number of logs determines the time these logs can be stored. Generally, logs can be stored for months.</p>
Operation and Maintenance	System Service and Status Tracking	-	<p>The NetEngine 8000 F1A provides the following functions for tracking system services and status:</p> <ul style="list-style-type: none"> <li>• Monitors the changes of routing protocol state machines.</li> <li>• Monitors the changes of MPLS LDP state machines.</li> <li>• Monitors the changes of VPN state machines.</li> <li>• Monitors the types of protocol packets sent by the forwarding engine to the control plane and displays detailed packet information by enabling debugging.</li> <li>• Monitors abnormal packets and collects statistics.</li> <li>• Displays a notification when the abnormality process starts.</li> <li>• Collects statistics about the resources used by each feature.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	System Test and Diagnosis	-	<p>The NetEngine 8000 F1A supports the debugging of running services, including online recording of key events, packet processing, packet parsing, and status switching of services at specified time, which serves as powerful support for device commissioning and networking. Debugging can be enabled or disabled through the console interface for specific services (for example, a routing protocol) or specific interfaces (for example, a routing protocol on a specific interface).</p> <p>The NetEngine 8000 F1A provides the system-based trace function to detect and diagnose running software, online recording of important events, such as task switchover, interrupt, queue reading and writing, and system abnormalities. If the system is restarted after a fault occurs, the device can read trace information to facilitate fault locating. The trace function can be enabled or disabled using commands on the console interface.</p> <p>In addition, the NetEngine 8000 F1A supports the real-time query of the CPU usage.</p> <p>Debugging and trace information provided by the NetEngine 8000 F1A is classified into different levels. Sensitive information assigned different levels can be output to different destinations as configured. For example, specific information can be output to the console interface, Syslog server, or SNMP agent to trigger traps.</p>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	NQA	-	<p>The NetEngine 8000 F1A supports Network Quality Analysis (NQA). NQA measures the performance of different protocols running on a network to obtain network operation indicators, such as the total HTTP delay, TCP connection delay, file transfer rate, FTP connection delay, Domain Name System (DNS) resolution delay, and DNS resolution error ratio. Based on these indexes, operators can provide differentiated network services and charge differently. NQA is also an efficient tool for diagnosing and locating network faults. NQA supports the following functions:</p> <ul style="list-style-type: none"> <li>• PWE3 tracer</li> <li>• Multicast ping</li> <li>• Multicast tracer</li> <li>• Tracer using the DISMAN-TRACEROUTE-MIB</li> <li>• Ping/UDP/TCP/SNMP tests using the DISMAN-PING-MIB</li> <li>• CE-ping (ping the host from a VPLS PE)</li> <li>• LSP ping, LSP traceroute, and MPLS LSP jitter</li> <li>• DNS verification using the DISMAN-NSLOOKUP-MIB</li> <li>• Transmission of consecutive 3000 simulated voice packets in one test</li> <li>• Minimum transmission intervals at 10 ms</li> <li>• NQA for multiple next hops in packet redirection</li> </ul>
Operation and Maintenance	VS	-	<p>A virtual system (VS) is classified as an admin VS or a common VS.</p> <ul style="list-style-type: none"> <li>• Common VS: The network administrator uses hardware-level and software-level emulation to partition a physical system (PS) into VSs. Each interface works only for one VS, and each VS runs individual routing tasks. VSs share software and hardware resources.</li> <li>• Admin VS: Each PS has a default VS named admin VS. All unallocated interfaces belong to this VS. The admin VS can process services in the same way as a common VS. In addition, the PS administrator can use the admin VS to manage VSs.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	In-Service Debugging	-	The NetEngine 8000 F1A provides port mirroring to map specific traffic to a monitoring interface. In this case, in-service debugging can be performed for advanced maintenance engineers to debug and analyze the network operating status.
Operation and Maintenance	Upgrade	-	<ul style="list-style-type: none"> <li>One-command system upgrade The NetEngine 8000 F1A provides an optimized upgrade process. A progress bar is displayed to show the upgrade progress. After the upgrade is complete, the upgrade result is displayed.</li> <li>Software version rollback If the new system software cannot start the system after an upgrade, the system can roll back to the previous version instead. NetEngine 8000 F1A protects services against system upgrade failures.</li> </ul>
Operation and Maintenance	License	-	<p>As the NetEngine 8000 F1A's software functions become increasingly diversified and software costs occupy an increasing proportion of the total costs, the traditional service model is insufficient to meet the following carrier requirements:</p> <ul style="list-style-type: none"> <li>Lower purchasing costs</li> <li>Effective control over the capacities and functions of devices during system upgrades and capacity expansion</li> </ul> <p>To meet different customer requirements, the NetEngine 8000 F1A implements flexible authorization of service modules. The NetEngine 8000 F1A provides a license authorization management platform called the global trotter license (GTL). The GTL allows you to:</p> <ul style="list-style-type: none"> <li>Purchase only required service functional modules, reducing purchasing costs.</li> <li>Extend device functions and expand device capacities by purchasing new licenses.</li> </ul>

Level-1 Feature	Level-2 Feature	Level-3 Feature	Description
Operation and Maintenance	Other Operation and Maintenance Features	-	<ul style="list-style-type: none"> <li>• Hierarchical command authorization to prevent unauthorized access</li> <li>• Online help obtained by entering a question mark (?)</li> <li>• Rich and detailed debugging information for network fault diagnosis</li> <li>• DOSKEY-like function that allows specific historical commands to be run</li> <li>• Fuzzy matching of keywords using the command resolver, for example, "disp" for a <b>display</b> command</li> </ul>



# 6 Energy Conservation and Emission Reduction

---

## Regulation Compliance of the NetEngine 8000 F1A

The NetEngine 8000 F1A complies with the following energy conservation and emission reduction regulations:

- Directive 2011/65/EU & 2015/863/EU on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS)
- Regulation 2006/1907/EC concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH)
- Directive 2012/19/EC on waste electrical and electronic equipment (WEEE)
- ATIS-0600015.03.2016 Energy Efficiency for Telecommunications Equipment: Methodology for Measurement and Reporting for Router and Ethernet Switch Products
- Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast)

## Power Consumption Management of the NetEngine 8000 F1A

The NetEngine 8000 F1A provides the following power consumption management functions:

- Power supply management
- Device-based power consumption query
- Configuration and query of the energy conservation mode

## Power Consumption Reduction Designs of the NetEngine 8000 F1A

The NetEngine 8000 F1A has the following power consumption reduction designs:

- Allows fan modules to automatically adjust the fan speed based on environment temperature.
- Supports dynamic energy conservation for unused modules.

- Supports dynamic energy conservation based on service loads.

## **Energy Conservation Suggestions of the NetEngine 8000 F1A**

The energy conservation suggestions for the NetEngine 8000 F1A are as follows:

- Separate hot and cold air ducts in equipment rooms, place the air intake vent of the NetEngine 8000 F1A besides the cold air duct, and prevent hot air from entering the air intake vent.
- Cover unused slots with filler panels and cap unused interfaces with rubber plugs to ensure efficient heat dissipation.
- Enable the NetEngine 8000 F1A to work in energy conservation mode.

# 7 NMS

---

## NCE

The device supports the Network Cloud Engine (NCE). NCE is an innovative network cloudification engine of Huawei. Positioned as the brain of the future cloud-based network, NCE integrates functions such as network management, service control, and network analysis. It is the core enabling system that implements network resource pooling, network connection automation and self-optimization, and O&M automation.

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

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

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

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

NCE aims to build an intent-driven network (IDN) that is first automated, then self-adaptive, and finally autonomous:

**Automation:** Network deployment and maintenance are automated throughout the network lifecycle.

**Self-adaptation:** Service policies are automatically generated based on big data using the real-time analyzer to implement proactive maintenance and closed-loop optimization.

**Autonomy:** Artificial intelligence and machine learning are used to build an intelligent network that can automatically generate dynamic policies.

---

# 8 Acronyms and Abbreviations

---

<b>A</b>	
<b>AAA</b>	Authentication, Authorization and Accounting
<b>AAL5</b>	ATM Adaptation Layer 5
<b>AC</b>	Access Controller
<b>ACL</b>	Access Control List
<b>AF</b>	Assured Forwarding
<b>ANSI</b>	American National Standard Institute
<b>AP</b>	Access Point
<b>ARP</b>	Address Resolution Protocol
<b>ASBR</b>	Autonomous System Boundary Router
<b>ASIC</b>	Application Specific Integrated Circuit
<b>ATM</b>	Asynchronous Transfer Mode
<b>B</b>	
<b>BE</b>	Best-Effort
<b>BGP</b>	Border Gateway Protocol
<b>BGP4</b>	BGP Version 4
<b>C</b>	
<b>CAR</b>	Committed Access Rate
<b>CBR</b>	Constant Bit Rate
<b>CE</b>	Customer Edge
<b>CHAP</b>	Challenge Handshake Authentication Protocol
<b>CoS</b>	Class of Service

<b>CPU</b>	Center Processing Unit
<b>CR-LDP</b>	Constrained Route - Label Distribution Protocol
<b>D</b>	
<b>DC</b>	Direct Current
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name Server
<b>DS</b>	Differentiated Services
<b>E</b>	
<b>EACL</b>	Enhanced Access Control List
<b>EF</b>	Expedited Forwarding
<b>EMC</b>	ElectroMagnetic Compatibility
<b>F</b>	
<b>FE</b>	Fast Ethernet
<b>FEC</b>	Forwarding Equivalence Class
<b>FIB</b>	Forward Information Base
<b>FIFO</b>	First In First Out
<b>FTP</b>	File Transfer Protocol
<b>G</b>	
<b>GE</b>	Gigabit Ethernet
<b>GRE</b>	Generic Routing Encapsulation
<b>GTS</b>	Generic Traffic Shaping
<b>H</b>	
<b>HA</b>	High availability
<b>HTTP</b>	Hypertext Transport Protocol
<b>I</b>	
<b>ICMP</b>	Internet Control Message Protocol
<b>IDC</b>	Internet Data Center
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IETF</b>	Internet Engineering Task Force
<b>IGMP</b>	Internet Group Management Protocol

<b>IGP</b>	Interior Gateway Protocol
<b>IP</b>	Internet Protocol
<b>IPoA</b>	IP Over ATM
<b>IPTN</b>	IP Telephony Network
<b>IPTV</b>	Internet Protocol Television
<b>IPv4</b>	IP version 4
<b>IPv6</b>	IP version 6
<b>IPX</b>	Internet Packet Exchange
<b>IS-IS</b>	Intermedia System-Intermedia System;
<b>ISP</b>	Interim inter-switch Signaling Protocol
<b>ITU</b>	International Telecommunication Union - Telecommunication Standardization Sector
<b>L</b>	
<b>LAN</b>	Local Area Network
<b>LCD</b>	Liquid Crystal Display
<b>LCP</b>	Link Control Protocol
<b>LDP</b>	Label Distribution Protocol
<b>LER</b>	Label switching Edge Router
<b>LPU</b>	Line Processing Unit
<b>LSP</b>	Label Switched Path
<b>LSR</b>	Label Switch Router
<b>M</b>	
<b>MAC</b>	Media Access Control
<b>MBGP</b>	Multiprotocol Border Gateway Protocol
<b>MD5</b>	Message Digest 5
<b>MIB</b>	Management Information Base
<b>MP</b>	Multilink PPP
<b>MPLS</b>	Multi-protocol Label Switch;
<b>MSDP</b>	Multicast Source Discovery Protocol
<b>MSTP</b>	Multiple Spanning Tree Protocol
<b>MTBF</b>	Mean Time Between Failures
<b>MTTR</b>	Mean Time To Repair

<b>MTU</b>	Maximum Transmission Unit
<b>N</b>	
<b>NLS</b>	Network Layer Signaling
<b>NP</b>	Network Processor
<b>NTP</b>	Network Time Protocol
<b>NVRAM</b>	Non-Volatile Random Access Memory
<b>O</b>	
<b>OSPF</b>	Open Shortest Path First
<b>P</b>	
<b>PAP</b>	Password Authentication Protocol
<b>PE</b>	Provider Edge
<b>PFE</b>	Packet Forwarding Engine
<b>PIC</b>	Physical Interface Card
<b>PIM-SM</b>	Protocol Independent Multicast-Sparse Mode
<b>POP</b>	Point Of Presence
<b>PPP</b>	Point-to-Point Protocol
<b>PQ</b>	Priority Queue
<b>PT</b>	Protocol Transfer
<b>PVC</b>	Permanent Virtual Channel
<b>Q</b>	
<b>QoE</b>	Quality of Experience
<b>QoS</b>	Quality of Service
<b>R</b>	
<b>RADIUS</b>	Remote Authentication Dial in User Service
<b>RAM</b>	Random-Access Memory
<b>RED</b>	Random Early Detection
<b>RFC</b>	Request for Comments
<b>RH</b>	Relative Humidity
<b>RIP</b>	Routing Information Protocol
<b>ROM</b>	Read Only Memory

<b>RP</b>	Rendezvous Point
<b>RSVP</b>	Resource Reservation Protocol
<b>RSVP-TE</b>	RSVP-Traffic Engineering
<b>S</b>	
<b>SAP</b>	Service Advertising Protocol
<b>SCSR</b>	Self-Contained Standing Routing
<b>SDH</b>	Synchronous Digital Hierarchy
<b>SDRAM</b>	Synchronous Dynamic Random Access Memory
<b>SLA</b>	Service Level Agreement
<b>SNAP</b>	SubNet Attachment Point
<b>SNMP</b>	Simple Network Management Protocol
<b>SONET</b>	Synchronous Optical Network
<b>SP</b>	Strict Priority
<b>SPI4</b>	SDH Physical Interface
<b>SSH</b>	Secure Shell
<b>SVC</b>	Switching Virtual Connection
<b>T</b>	
<b>TCP</b>	Transfer Control Protocol
<b>TE</b>	Traffic Engineering
<b>TFTP</b>	Trivial File Transfer Protocol
<b>TM</b>	Traffic Manager
<b>ToS</b>	Type of Service
<b>TP</b>	Topology and Protection packet
<b>U</b>	
<b>UBR</b>	Unspecified Bit Rate
<b>UDP</b>	User Datagram Protocol
<b>UNI</b>	User Network Interface
<b>UTP</b>	Unshielded Twisted Pair
<b>V</b>	
<b>VBR-NRT</b>	Non-Real Time Variable Bit Rate
<b>VBR-RT</b>	Real Time Variable Bit Rate



<b>VC</b>	Virtual Circuit
<b>VCI</b>	Virtual Channel Identifier
<b>VDC</b>	Variable Dispersion Compensator
<b>VLAN</b>	Virtual Local Area Network
<b>VLL</b>	Virtual Leased Line
<b>VPI</b>	Virtual Path Identifier
<b>VPLS</b>	Virtual Private LAN Service
<b>VPN</b>	Virtual Private Network
<b>VRP</b>	Versatile Routing Platform
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>W</b>	
<b>WAN</b>	Wide Area Network
<b>WFQ</b>	Weighted Fair Queuing
<b>WRED</b>	Weighted Random Early Detection
<b>WRR</b>	Weighted Round Robin