IP Network eBook Series

SD-WAN Solution

Author : Ting Leng

Information Digitalization and Experience Assurance (IDEA) Department

HUAWEI

Copyright

Author: Ting Leng

Key Contributors: Cheng Sheng, Hanlin Zhao, Jun Hu, Yongbo Wang, Qiaoqiao Liu, and Heng Ding

Release Date: 2024-9-10

Issue: 08

Copyright © Huawei Technologies Co., Ltd. 2024. 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.

Preface

Author Introduction

Ting Leng: Serves as documentation engineer for Huawei Software-Defined Wide Area Network (SD-WAN) Solution. Ms. Leng joined Huawei in 2005 and took responsibility for network product software design and development for six years. Since then, she has been dedicated to development and design of documentation for network products such as Huawei's iMaster NCE, eSight, and SD-WAN Solution. She has made significant contributions to developing the book *Software-Defined Wide Area Network Architectures and Technologies*.

About This Book

Since its emergence, SD-WAN has been developing dramatically both in standards and application.

This book starts with the challenges faced by traditional Wide Area Networks (WANs) and then moves on to the standards, advantages and benefits, solution architecture, and key technologies of SD-WAN. This book also outlines the typical networking, device model selection, and typical applications of Huawei's SD-WAN Solution across industries.

Intended Audience

This book is intended for information and communications technology (ICT) practitioners, such as network engineers with a basic knowledge of data communication and operation experience. It is also recommended for anyone with SD-WAN service requirements or with a general interest in SD-WAN.

Symbol Conventions

Note **Supplements important information in the main text. Note is used to address information not related to personal injury, equipment damage, or environment deterioration.**

Table of Contents

Chapter 1 SD-WAN Overview 1

1.1 WAN Trends and Challenges 1

1.2 SD-WAN Emergence and Industry Standards 3

1.3 Pain Points Resolved by SD-WAN 6

1.4 Huawei's SD-WAN Solution 7

Chapter 2 Key Differentiators 9

2.1 Flexible Cloud Access: On-demand Interconnection 9

2.2 Intelligent Traffic Steering: Optimal Experience 12

2.3 Intelligent O&M: Simplified Deployment 13

Chapter 3 Overall Architecture 16

Chapter 4 Key Technologies 20

4.1 Diverse System Channels: Enhancing Reliability and Security . 20

4.2 Multiple ZTP Modes: Plug-and-Play Devices 22

4.3 Flexible Networking: Meeting Diversified Networking Requirements

..... 23

4.4 Application-based Intelligent Traffic Steering: Guaranteeing Key Applications and Maximizing Bandwidth Utilization 27

4.5 WAN Optimization: Delivering Optimal Application Experience 32

4.6 Intelligent Policy Recommendation: Facilitating WAN Experience Assurance 37

4.7 Proactive Defense: Building E2E Security 39

4.8 Visualized O&M and Monitoring: Improving O&M Efficiency ... 43

Chapter 5 Typical SD-WAN Networking 47

5.1 Enterprise HQ + Branch (Hub-Spoke Networking) 47

5.2 Enterprise HQ + Branch (Full-Mesh Networking) 50

5.3 Enterprise HQ + Regional Center + Branch (Hierarchical Networking) 52

5.4 Enterprise Multi-DC + Branch (Multi-Hub Networking) 54

5.5 Multi-Tenant IWG (POP Networking) 56

Chapter 6 Typical Applications 58

6.1 Finance Industry 58

6.2 Carrier/MSP Resale 61

Chapter 7 Product Portfolio 64

7.1 NetEngine AR Routers 64

7.2 iMaster NCE 66

A Acronyms and Abbreviations 68

Chapter 1
SD-WAN Overview

Abstract

This chapter describes the challenges faced by and requirements of traditional Wide Area Networks (WANs), industry standards, as well as key technologies and typical applications of Huawei's of Software- Defined Wide Area Network (SD-WAN) Solution.

1.1 WAN Trends and Challenges

Evolving Enterprise WANs

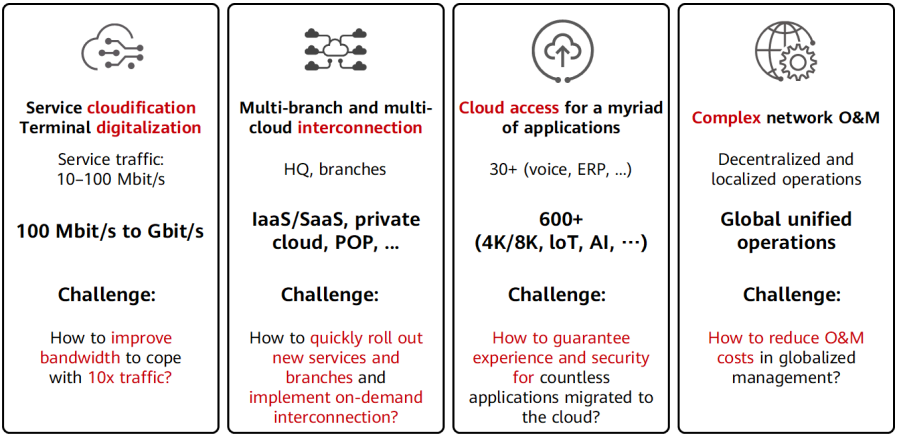
As its name suggests, a WAN is a wide area interconnection network used for long-distance communication between enterprises or organizations, and can span multiple countries, regions, or cities. With coverage often ranging from tens to thousands of kilometers, WANs enable information and resource sharing over vast distances. Due to costs and construction difficulties, WANs are generally provided by carriers. Most enterprises set up their own WANs by leasing WAN private lines from carriers.

With the rapid development of enterprise IT digitalization and economic globalization, enterprises are now stepping into the cloud era. More and more enterprises are choosing to build their IT systems on the public cloud in order to reduce construction costs. They are also choosing to move their traditional applications to the cloud. In most cases, enterprises are using WANs to access Software as a Service (SaaS) applications, such as office software and databases.

Challenges Facing Enterprise WANs

Service changes drive enterprise WANs into today's cloud era. Figure 1-1 illustrates the new challenges faced by traditional enterprise WANs in this era, as a result of the cloudification of enterprise services.

Figure 1-1 Challenges facing enterprise WANs



- **Difficult multi-cloud interconnection due to closed architectures**

  Cloudification is an inevitable trend, with most enterprises expected to move their services onto clouds in the next few years. To access cloud applications, enterprise WANs need to interconnect with public clouds, private clouds, and SaaS clouds. This is currently beyond the reach of traditional WANs due to their closed architectures, not to mention the mounting burden of explosive cloud application traffic on traditional WANs after enterprises move services to clouds.

- **Increasingly diverse interconnection requirements with more flexible networking**

  Amid the trend of globalization, branches are becoming more widely distributed. The branches may have varying requirements on networks in different regions, for example, hierarchical networking by one branch and flattened networking by another; multiple uplinks (> 5) by one branch and multiple hub sites (> 4) by another. Such varying and complex interconnection requirements cannot be satisfied with traditional WANs.

- **Poor experience of key applications**

  In the era of cloud and digitalization, cloud computing fuels the explosive growth of enterprise applications, both in quantity and type. These applications, including voice, video, file transfer, email, and SaaS, have varying requirements on link quality. Traditional enterprise private lines cannot differentiate services, and the newly deployed Internet links cannot guarantee service quality. As such, when any traffic congestion occurs or link quality deteriorates, the experience of key services cannot be guaranteed.

- **Difficult network O&M and error-prone manual configuration**

  On traditional WANs, service configuration, network operations and maintenance (O&M), and fault locating need to be manually performed onsite, resulting in inefficient but costly service provisioning and network O&M. Against the backdrop of digitalization and globalization, enterprise WANs have a growing number of branches that are more widely distributed and carry more complex services, which means more difficult O&M. Traditional manual configuration and O&M hold back rapid service development.

1.2 SD-WAN Emergence and Industry Standards

Facing such unprecedented challenges, how can enterprise WANs move forward? This is where SD-WAN comes in.

What Is SD-WAN?

SD-WAN was first proposed by the Open Networking User Group (ONUG) at a conference in 2014. It is a type of network service that applies software defined networking (SDN) technology to the interconnection of WANs in enterprises.

Leveraging the SDN controller — a centralized network control system — this type of network service delivers automated configuration for WANs, centralized control and management, and high openness and programmability.

Building on the initial definition of SD-WAN made by ONUG, many other standards organizations have actively participated in enriching SD-WAN with additional characteristics and technical standards. The definitions proposed by Gartner and Metro Ethernet Forum (MEF) are now widely accepted.

SD-WAN Defined by Gartner

As the world's most authoritative IT research and advisory company, Gartner's research scope covers all IT industries, including IT research, development, evaluation, application, and markets. It is noted for providing objective, fair demonstrations and market surveys for its customers.

Gartner defines SD-WAN as follows: SD-WAN solutions provide a replacement for traditional WAN routers and are agnostic to WAN transport technologies. SD- WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

According to Gartner, SD-WAN has three major characteristics: hybrid links, dynamic path selection, and additional services.

SD-WAN Defined by MEF

MEF is a non-profit organization that focuses on resolving technical issues of metro Ethernet and dedicates itself to promoting the implementation of existing and new network standards, Ethernet service definitions, test procedures, and technical specifications.

MEF has published the industry's first global standard defining an SD-WAN service and its service attributes: MEF 70. Table 1-1 presents a brief description of the SD-WAN characteristics defined by MEF.

Table 1-1 SD-WAN characteristics defined by MEF

No.	Description
1	Secure, IP-based overlay network
2	Independent underlay network that operates over any type of wired or wireless access networks
3	Service assurance of each SD-WAN tunnel
4	Application-based traffic steering and forwarding
5	Hybrid access using multiple types of WAN links, featuring high reliability
6	Policy-based packet forwarding
7	Automated service provisioning through centralized management, control, and orchestration, such as Zero Touch Provisioning (ZTP)
8	WAN optimization

Although different standards organizations have different approaches to defining and interpreting the functions of SD-WAN, there seems to be a consensus on SD- WAN fundamentals, illustrated as follows:

- SD-WAN shall implement rapid deployment and rollout of branches through ZTP, improving service deployment efficiency.
- SD-WAN shall dynamically adjust traffic paths by application type, achieving flexible, convenient traffic scheduling.
- SD-WAN shall implement centralized network management and control, network-wide status visualization, and automated, intelligent network O&M.
- SD-WAN shall support plenty of value-added services (VASs) which exemplify WAN optimization and security to deliver optimal service experience.

In summary, the industry has high expectations for SD-WAN to facilitate fast deployment, robust flexibility, high scalability, and intelligent O&M.

1.3 Pain Points Resolved by SD-WAN

SD-WAN deeply integrates conventional enterprise WAN technologies, such as routing, Quality of Service (QoS), security, and WAN acceleration, as well as future-proof brand-new technologies, including SDN, Network Functions Virtualization (NFV), and service orchestration. Powered by the SD-WAN network controller, SD-WAN achieves centralized orchestration, control, and management of WAN interconnections, resolving many pain points faced by enterprises and carriers.

- **Flexible cloud connectivity**

  In the cloud era, enterprise WANs need to connect to various cloud resources, which are abstracted into a cloud site. A cloud site also requires a virtual gateway device to connect enterprise branches and the public cloud. Such a device must reside on the cloud and be created quickly. To this end, the network controller remotely schedules public cloud application programming interfaces (APIs) and resources, and automatically enables cloud devices to facilitate seamless communication between branch sites and the public cloud.

- **Lower interconnection costs**

  In recent years, the Internet improved drastically in terms of coverage and performance, and Internet links are now able to offer network quality closer to that of private lines. As such, Internet links are becoming a new choice for WAN interconnections. With SD-WAN, in addition to the MPLS private lines provided by carriers, enterprises can also use Internet links to connect WAN branches. This achieves hybrid interconnections and slashes deployment costs for enterprise WANs.

- **Improved application experience**

  The introduction of hybrid WANs enables enterprise service traffic to be transmitted over a variety of WAN links. The network quality varies according to WAN link. For example, MPLS private lines can provide guaranteed link quality, though they are expensive; even though Internet links can support bandwidth-hungry applications, they are still prone to large latency and packet loss. SD-WAN supports application-based traffic steering,

which enables high-value applications to be preferentially transmitted over high-quality WAN links. This delivers optimal user experience for such high- value applications.

- **Faster service rollout**

  The provisioning of private lines is time-consuming and labor-intensive, and is unable to support fast service deployment. SD-WAN makes devices plug- and-play, enabling fast provisioning of new branch networks and service rollout. SD-WAN shortens the provisioning time of branch networks from days or even months to hours, greatly improving the service provisioning efficiency.

- **Higher O&M efficiency**

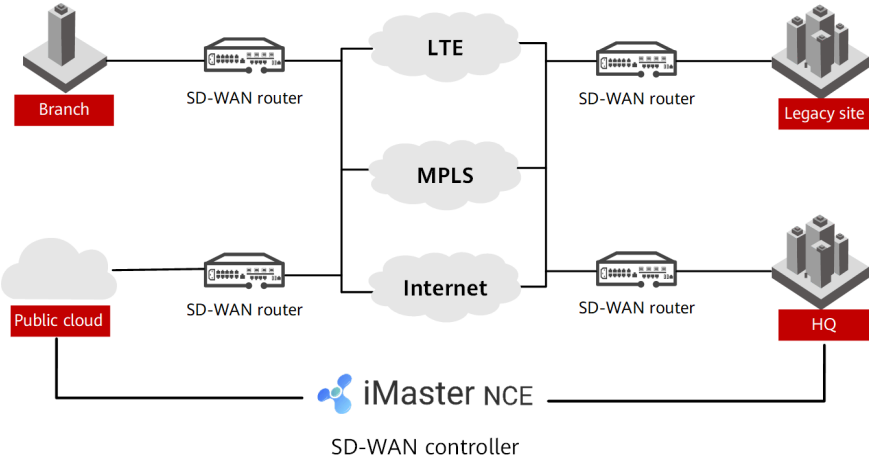
  Due to the large number of widely distributed enterprise branches, enterprise WANs are in urgent need of a system capable of centralized management and control as well as O&M to improve efficiency. SD-WAN is such a viable solution.

  - Centralized management and control: SD-WAN supports remote management of devices at branch sites, ZTP, and centralized policy provisioning.
  - O&M: SD-WAN supports visualized, intelligent O&M, and real-time monitoring of alarms and logs, greatly improving O&M efficiency.

1.4 Huawei's SD-WAN Solution

Huawei's SD-WAN Solution complies with both MEF's SD-WAN standards and Gartner's definition of SD-WAN. In addition to integration and enhancements on traditional WAN technologies, this future-proof solution fully utilizes hybrid links for interconnection between enterprise branches, headquarters (HQ), and clouds, and implements SDN-based network orchestration, management, and control. In this way, it implements networking automation, visualized monitoring, centralized management, and optimized application experience. Figure 1-2 shows the implementation of Huawei's SD-WAN Solution.

Figure 1-2 Huawei's SD-WAN Solution



For details about the components and products of Huawei SD-WAN Solution, see Chapter 7.

Chapter 2
Key Differentiators

Abstract

This chapter describes the key differentiators of Huawei's SD-WAN Solution: flexible cloud access, intelligent traffic steering, and intelligent O&M.

2.1 Flexible Cloud Access: On-demand Interconnection

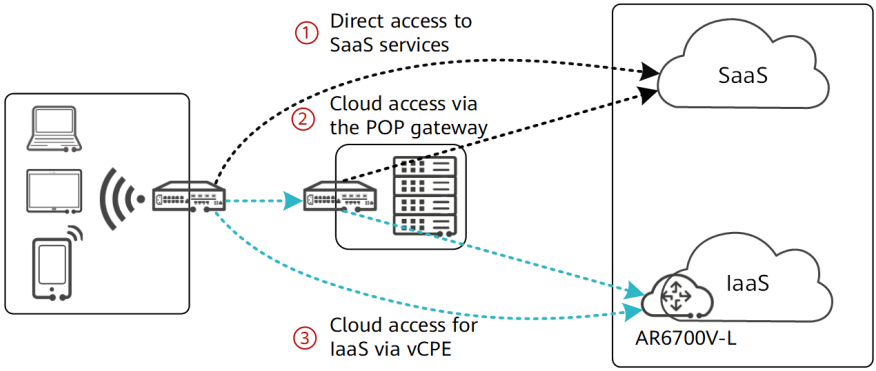
A growing number of enterprises are deploying their services on the cloud. How can enterprise WANs enable fast cloud access in multi-cloud interconnection scenarios involving SaaS, public, and private clouds? Flexible networking and 5G gigabit wireless links make on-demand interconnection of enterprise services a reality.

Flexible Networking, On-demand Interconnection

Huawei's SD-WAN Solution supports diverse networking models, such as hub- spoke networking, full-mesh networking, partial-mesh networking, multi-hub networking, MPLS interworking networking, and access through the optimal MSP Point of Presence (POP) node. In addition, this solution maintains compatibility with the legacy network to implement smooth migration. Such robust networking flexibility enables on-demand interconnection.

As shown in Figure 2-1, Huawei's SD-WAN Solution also allows one network to connect to multiple clouds, such as SaaS and infrastructure as a service (IaaS) clouds, enabling pervasive access to enterprise services.

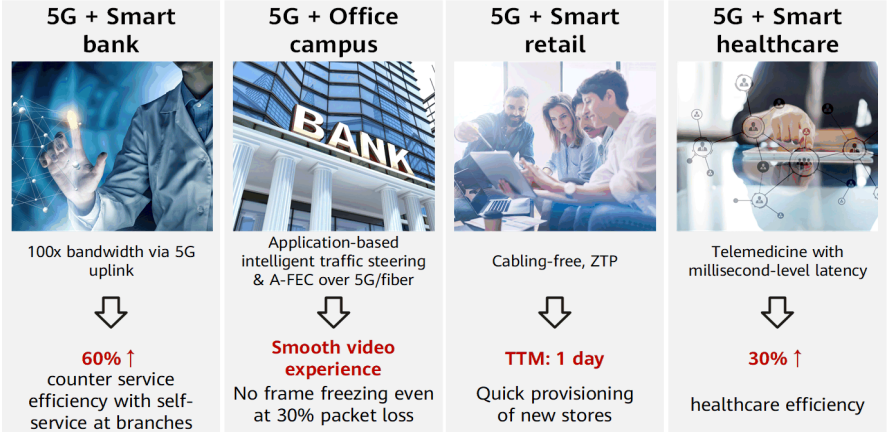
Figure 2-1 Connecting one network to multiple clouds via Huawei's SD-WAN Solution



5G Gigabit Wireless access, Enabling Service Access Anytime and Anywhere

5G networks stand out with high bandwidth, short latency, wide coverage, and low costs. As such, 5G gigabit wireless links have become another ideal choice. Leveraging 5G gigabit wireless links, services can be provisioned within minutes at any site. The use of 5G gigabit wireless links also gives birth to a wide set of innovative applications, such as smart banking, smart retail, smart healthcare, and office campus, as shown in Figure 2-2.

Figure 2-2 Innovative applications powered by 5G and SD-WAN



Now, let's look at two typical applications of 5G and SD-WAN in the finance industry.

- **Provisioning of unstaffed banks**

  Huawei's SD-WAN Solution incorporating diverse WAN links such as the Internet, while 5G offers more choices to the finance industry. Powered by 5G and SD-WAN, unstaffed banks not only slash link costs but also simplify network deployment and O&M. The network controller centrally manages all devices in each branch, without the need of professionals at the site.

- **Fast interconnection between smart branches**

  5G WAN links can quickly interconnect smart branches. The combination of 5G and SD-WAN has several advantages over traditional private lines, including: zero cabling, short provisioning period, and low maintenance costs. Meanwhile, with application-based intelligent traffic steering and WAN optimization, SD-WAN ensures uninterrupted services of key banking applications.

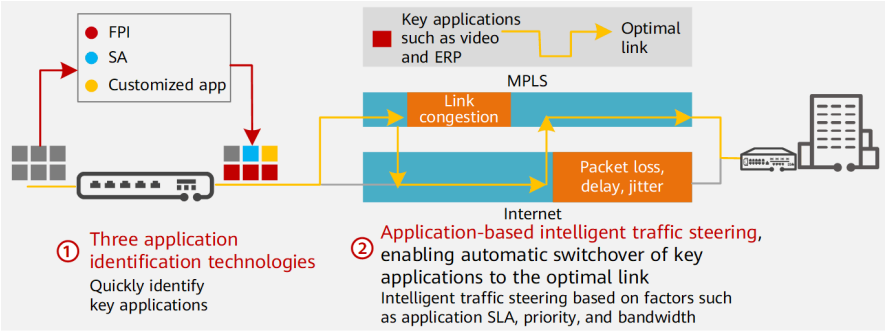
2.2 Intelligent Traffic Steering: Optimal Experience

Huawei's SD-WAN Solution adopts intelligent traffic steering and Adaptive Forward Error Correction (A-FEC) to deliver an optimal user experience. Application-based intelligent traffic steering ensures user experience of key applications, and A-FEC ensures smooth audio and video experience even if the packet loss rate reaches 30%.

Application-based Intelligent Traffic steering

Huawei's SD-WAN Solution supports application-based intelligent traffic steering, which detects the Service Level Agreement (SLA), including the packet loss rate, delay, and jitter, of each available path in real time. Based on the SLA, key applications are preferentially transmitted over high-quality WAN links, ensuring user experience of key applications. Figure 2-3 illustrates the implementation of application-based intelligent traffic steering.

Figure 2-3 Application-based intelligent traffic steering



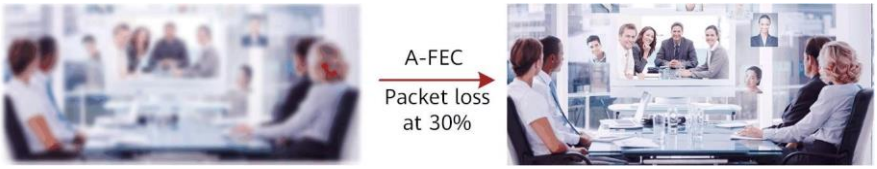
A-FEC

Instant messaging applications, such as voice calls, video conferences, and live streaming, have stringent requirements on delay and packet loss. When packet

loss occurs on the network, artifacts or even frame freezing occurs, and voice transmission is intermittent, severely affecting user experience. In most cases, when the packet loss rate reaches 1%, user services are slightly affected; when the packet loss rate reaches 10%, applications are almost unavailable.

Huawei's SD-WAN Solution uses A-FEC to mitigate packet loss. A-FEC identifies specific data flows through traffic classification, adds redundant packets that carry check information to the original packets, and decodes the received packets at the receive end to restore the lost packets. A-FEC ensures smooth video experience even if the packet loss rate reaches 30%, as shown in Figure 2-4.

Figure 2-4 Smooth video experience powered by A-FEC



2.3 Intelligent O&M: Simplified Deployment

Compared with traditional deployment and O&M systems, Huawei's SD-WAN Solution builds a simpler, smarter, and more visualized SD-WAN deployment and O&M system, enabling simplified deployment and visualized O&M.

Simplified Deployment

Rapid deployment and rollout of branch services are crucial to an enterprise's competitiveness. Through ZTP, SD-WAN implements plug-and-play and simplified deployment, greatly improving deployment efficiency.

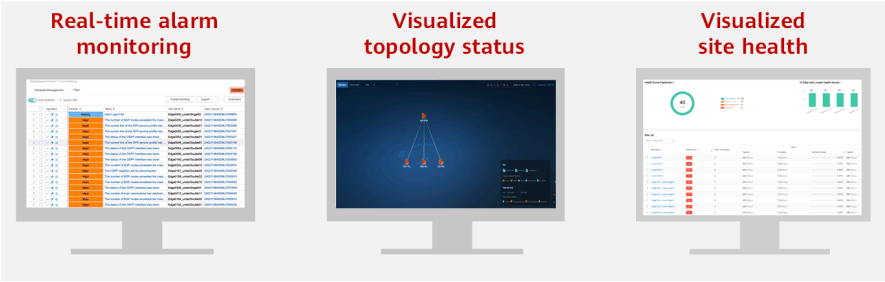
Before deployment, the network administrator preconfigures devices at the site on the SD-WAN network controller and sends an email containing the device configuration information to deployment personnel. The deployment personnel then connect cables, power on the devices, and click the URL in the email for

one-click deployment. The devices automatically register with the SD-WAN network controller and go online, implementing fast service provisioning.

Visualized O&M

In Huawei's SD-WAN Solution, the SD-WAN O&M system can display the WAN network topology and monitor alarms, logs, and other key events of devices at each branch site in real time. This enables the network administrator to centrally manage, control, and maintain a large number of devices at widely distributed sites. The SD-WAN O&M system can also graphically display key network performance data and application experience health. As shown in Figure 2-5, SD- WAN visualized O&M covers topology visualization, site health visualization, link status visualization, application quality visualization, and alarm and log information monitoring.

Figure 2-5 Visualized O&M



Intelligent O&M

In addition to visualization, the SD-WAN O&M system also provides intelligent O&M capabilities for fault locating and prevention. The SD-WAN O&M system leverages telemetry technology to collect network data in real time, and uses big data analytics and machine learning algorithms to learn network behavior and identify fault patterns.

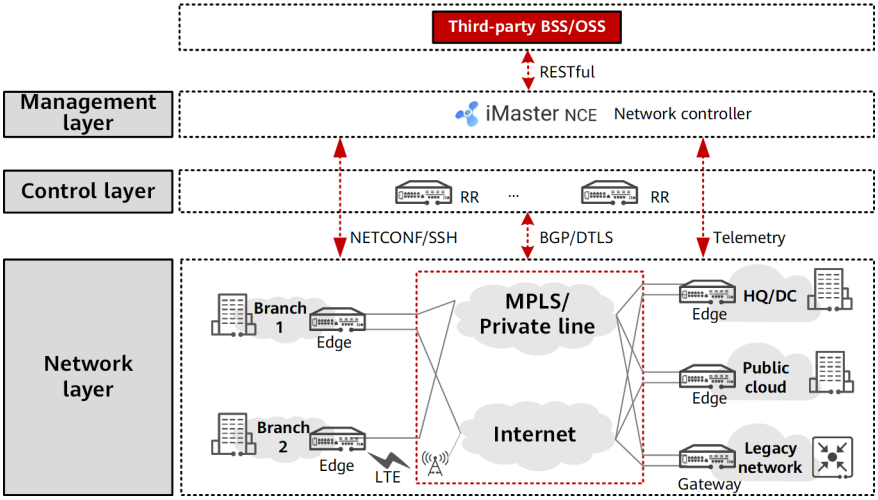
The SD-WAN O&M system can also collaborate with professional network analysis components to implement intelligent root cause analysis, predict faults and events on the network, and provide warnings or troubleshooting suggestions.

The SD-WAN intelligent O&M system helps O&M personnel proactively detect 80% of all network problems, greatly improving O&M efficiency.

Chapter 3
Overall Architecture

Figure 3-1 shows the overall architecture of Huawei's SD-WAN Solution, which consists of the management layer, control layer, and network layer. Each layer has specific core components and provides different functions.

Figure 3-1 Overall architecture of Huawei's SD-WAN Solution



Third-party Business Support System (BSS)/Operations Support System (OSS) is a support system for integration and information resource sharing of telecommunication carriers. Leveraging the open northbound API capabilities of the SD-WAN network controller, carriers or enterprise customers can incorporate the end-to-end (E2E) service process of SD-WAN into the existing third-party service orchestration systems such as BSS/OSS. This implements integration of Huawei's SD-WAN Solution and flexible GUI customization.

Management Layer

The network controller is the core component of the management layer and the smart brain of Huawei's SD-WAN Solution. It provides abundant network orchestration and management capabilities for E2E SD-WAN service processing.

- **Network orchestration: The network controller abstracts service-oriented SD-WAN network models, orchestrates services related to enterprise WAN networking and network policies, and automatically provisions service configurations. It also abstracts and defines the network model of enterprise WANs, and shields technical details about SD-WAN deployment and implementation, implementing simplified and flexible WAN configuration and service provisioning.**
- **Network management: The network controller implements network management and O&M functions for enterprise WANs, including but not limited to the following: collection of fault information such as alarms and logs of NEs; collection, statistics, and analysis of performance data based on links, applications, and networks; collection and display of multi-dimensional O&M information such as network topologies, alarms, and performance data.**

Control Layer

An SD-WAN Route Reflector (RR) is a core component at the control layer and is responsible for centralized control of route forwarding and topology definition at the SD-WAN network layer. The RR distributes and filters VPN routes of SD-WAN tenants, creates and modifies VPN topologies, and creates and maintains overlay tunnels between sites.

In contrast with the distributed control mode of traditional networks, this centralized control mode separates the control plane from the forwarding plane

of enterprise WANs. This simplifies network O&M operations, reduces network configuration errors, and improves the O&M efficiency of enterprise WANs.

In actual deployments, an RR can be deployed independently or combined with an existing edge site.

Network Layer

From the perspective of services, enterprise sites include enterprise branches, HQ, data centers (DCs), and cloud-based IT infrastructure. The network layer consists of two parts: network devices used for WAN interconnection at different sites and the intermediate WANs.

According to network functions, an enterprise's SD-WAN network can be divided into the underlay network and overlay network.

- Underlay network: a physical network, which is a WAN created by connecting network devices such as routers via physical lines provided by carriers. Examples of such a network include an MSTP network, MPLS network, and the Internet.
- Overlay network: one or more virtual networks, which are constructed on the same physical network through IP and software technologies. Although different virtual networks share devices and lines on a physical network, services are decoupled from physical networking and interconnection technologies on the physical network. As the core networking technology at the SD-WAN network layer, multi-instance virtual networks can serve different services (such as multiple departments) of the same tenant or different tenants.

From the perspective of network device functionality, the network layer of SD-WAN is mainly constructed using two types of devices: edge and gateway.

- Edge: egress customer-premises equipment (CPE) of an enterprise's SD-WAN site. In essence, an edge is the start point or termination point of an SD-WAN tunnel and can be considered as the boundary of an SD-WAN network. Overlay tunnels between edges can be established over any wired or wireless underlay WAN.
- Gateway: a device that connects an SD-WAN site and other networks (for example, legacy VPNs). The gateway enables an SD-WAN network to

communicate with an enterprise's legacy networks and public cloud networks.

Chapter 4
Key Technologies

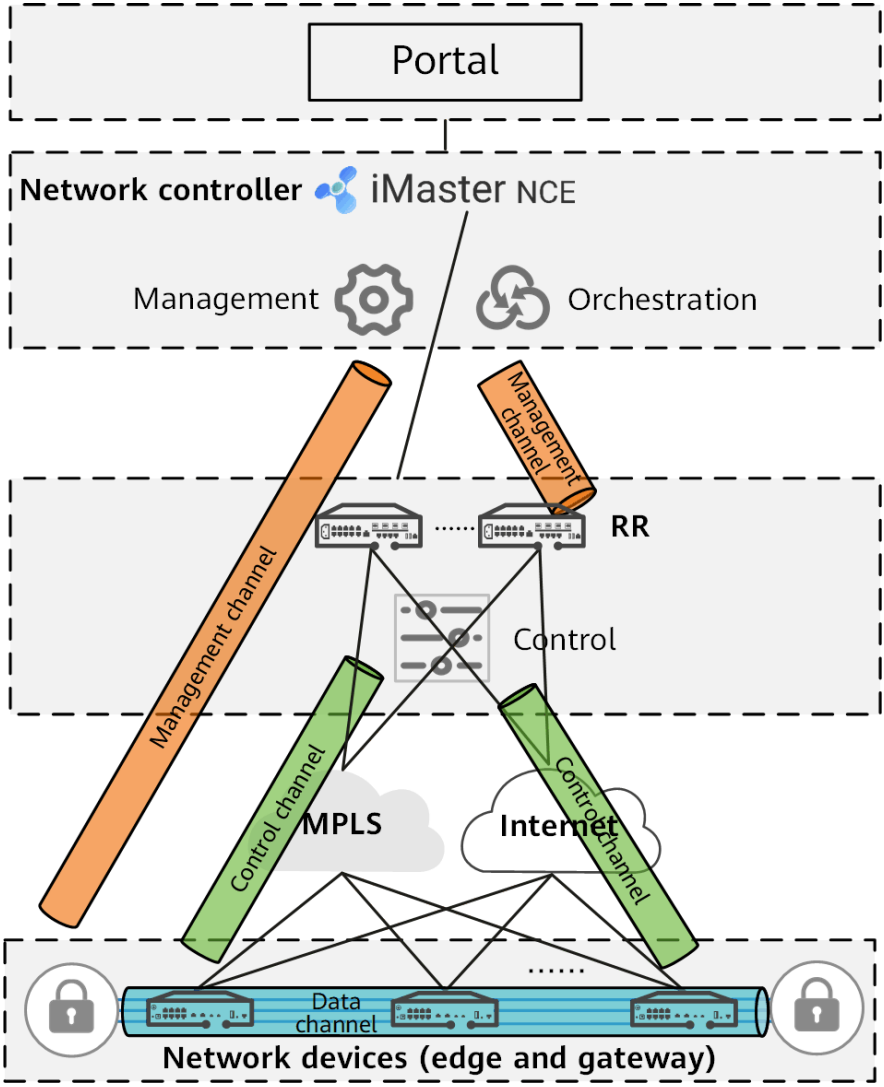
Abstract

This chapter describes the key technologies of Huawei's SD-WAN Solution: diverse system channels, multiple ZTP modes, flexible networking, intelligent traffic steering, WAN optimization, security, and O&M and monitoring.

4.1 Diverse System Channels: Enhancing Reliability and Security

Components in Huawei's SD-WAN Solution collaborate with each other to provide many functions. As shown in Figure 4-1, three system channels can be abstracted logically, between which data is isolated, ensuring that services do not affect each other.

Figure 4-1 System channels of Huawei's SD-WAN Solution



- **Management channel: used for network configuration and O&M between the network controller and network devices, such as edges, gateways, and RRs.**
- **Control channel: used to distribute forwarding information such as routes and tunnels between an RR and an edge node or between an RR and a gateway. This channel uses BGP EVPN.**
- **Data channel: used to transmit data between the edge and gateway at the network layer. Data channels are established based on IP overlay tunneling technology. As data needs to traverse a WAN, data channels generally use Internet Protocol Security (IPsec) for encryption.**

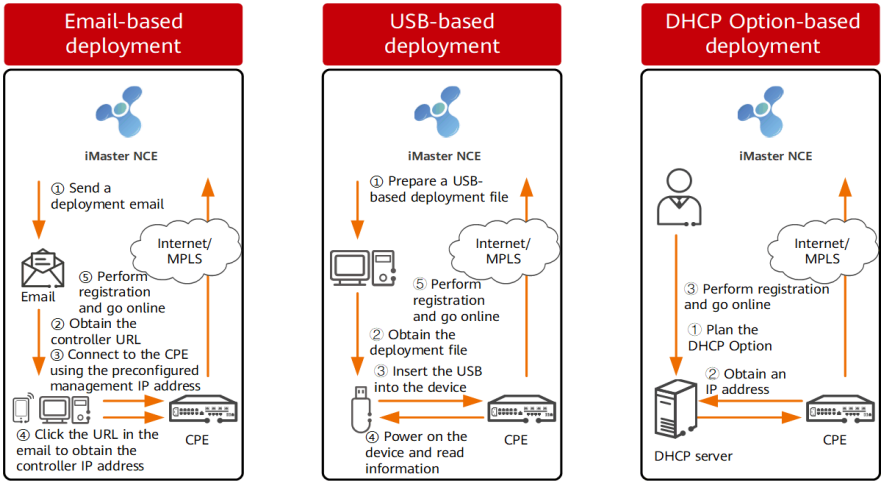
4.2 Multiple ZTP Modes: Plug-and-Play Devices

Traditional branch network deployment has high technical requirements, is error-prone, and is time-consuming. Huawei's SD-WAN Solution provides diverse ZTP modes for deployment in various scenarios. Table 4-1 lists the ZTP modes supported by Huawei's SD-WAN Solution, and Figure 4-2 shows the deployment process.

Table 4-1 ZTP modes

ZTP Mode	Application Scenario
Email-based deployment	This mode is applicable to onsite deployment. The network administrator sends a deployment email to the specified email address. After receiving the email, a deployment engineer clicks the URL in the email to automatically complete the deployment.
USB-based deployment	This mode is applicable to batch deployment in warehouses. The device administrator imports the CPE configuration in the warehouse, and a deployment engineer only needs to connect cables, insert a USB flash drive, and power on the device.
DHCP option-based deployment	This mode is applicable only to the scenario where CPEs are connected to the network through Dynamic Host Configuration Protocol (DHCP). A site deployment engineer only needs to connect cables and power on the CPE.

Figure 4-2 ZTP process



4.3 **Flexible Networking: Meeting Diversified Networking Requirements**

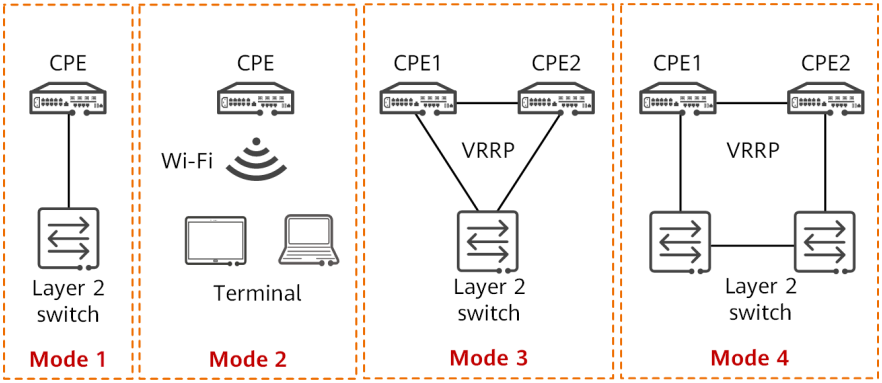
LAN-side Networking

Huawei's SD-WAN Solution provides a broad range of interfaces, such as FE, GE, XGE, and Eth-Trunk interfaces, for LAN-side interconnection and supports Layer 2 and Layer 3 interconnection scenarios.

LAN-side Layer 2 interconnection

At small sites with a simple intranet structure, CPEs typically connect to the intranet of the site at Layer 2. Figure 4-3 shows the four networking modes for LAN-side Layer 2 interconnection.

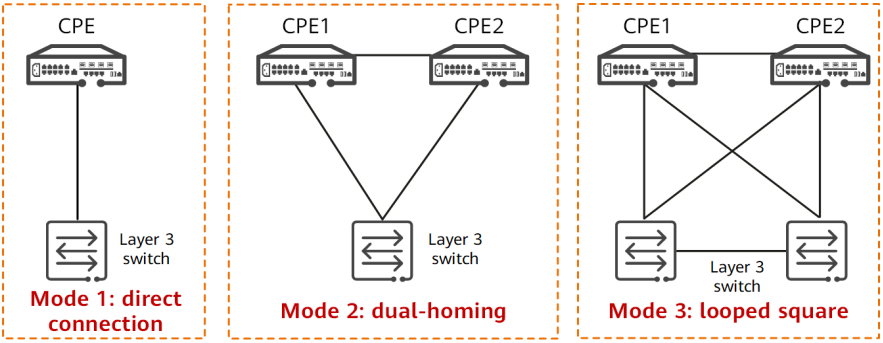
Figure 4-3 LAN-side Layer 2 networking



LAN-side Layer 3 interconnection

A large enterprise site has a complex network structure and facilities (such as a large number of routers and switches) and often involves a hierarchical, multi- network design. SD-WAN routers can establish Layer 3 connections with the LAN side through static, BGP, and OSPF routes using three networking modes, as shown in Figure 4-4.

Figure 4-4 LAN-side Layer 3 networking



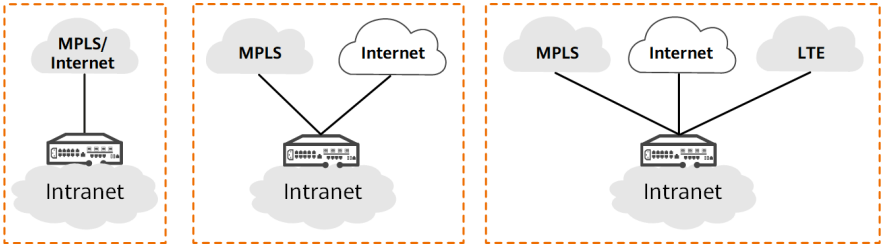
WAN-side Networking

Huawei's SD-WAN Solution provides a wide set of WAN interfaces, such as Ethernet, LTE/5G, and xDSL interfaces. Multiple networking modes are available, depending on the number of CPEs deployed at SD-WAN sites and the number of WAN links connected to the CPEs.

Single-CPE networking

A single CPE is deployed at a small site. Figure 4-5 illustrates the single-CPE networking.

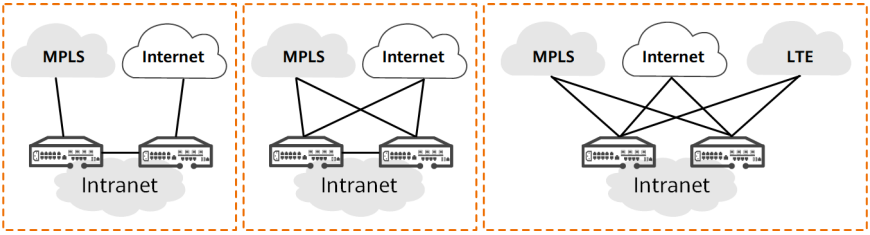
Figure 4-5 Single-CPE networking



Dual-CPE networking

Dual CPEs are deployed at sites requiring high reliability to provide device-level redundancy. Figure 4-6 illustrates the dual-CPE networking.

Figure 4-6 Dual-CPE networking

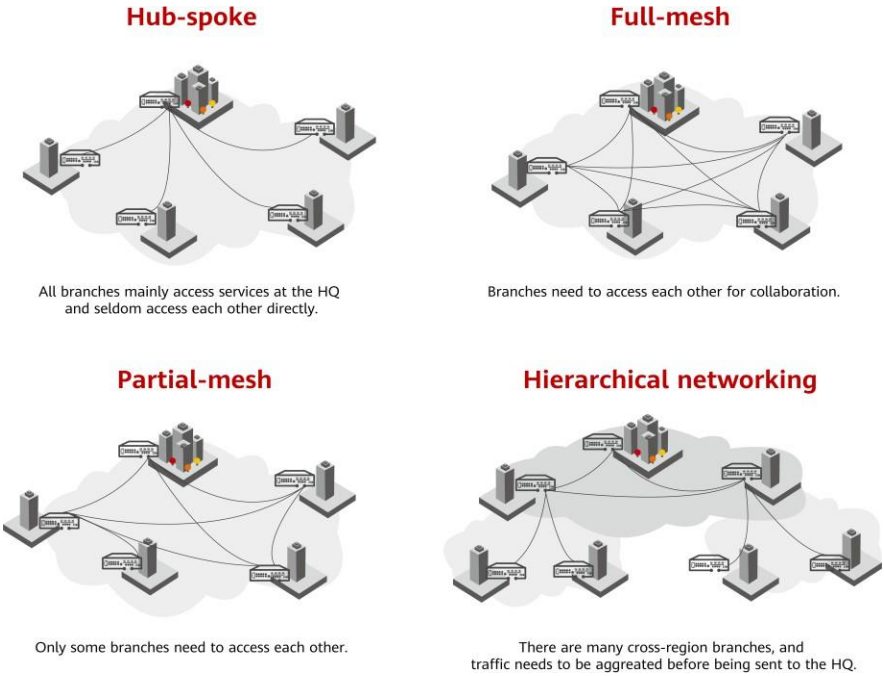


On-demand Overlay Tunnel Setup

Overlay tunnels are established on the underlay network to implement communication between SD-WAN sites. Multiple topology models are available for WAN communication. Based on the actual service access requirements, you can configure the VPN topology on the network controller and specify key topology roles (such as the hub and spoke). The network controller then automatically converts the topology model into a standard routing policy and delivers it to an RR. The RR controls the route sending and receiving of different sites based on the routing policy delivered by the network controller to implement communication between sites.

Enterprise WAN topology models typically fall into two types: single-layer network model and hierarchical network model. The former can be further classified into hub-spoke, full-mesh, and partial-mesh, as illustrated in Figure 4-7.

Figure 4-7 Enterprise WAN topology models



4.4 Application-based Intelligent Traffic Steering: Guaranteeing Key Applications and Maximizing Bandwidth Utilization

Application-based intelligent traffic steering is an important feature of Huawei's SD-WAN Solution. With this feature enabled, the network quality is monitored in real time; an SLA-compliant WAN link is dynamically and automatically selected among multiple WAN links with varying network quality, with the overall WAN network utilization maximized.

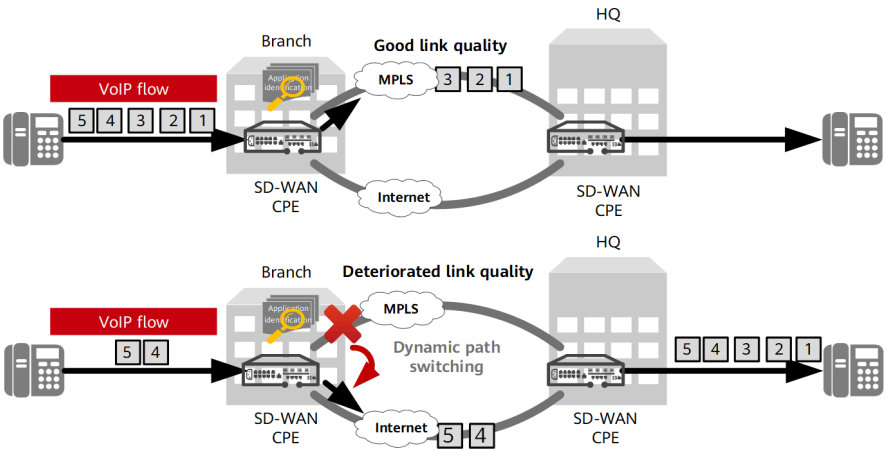
Huawei's SD-WAN Solution adopts multiple intelligent traffic steering algorithms, including: link quality-, load balancing-, application priority-, as well as bandwidth utilization-based load balancing.

Link Quality-based Traffic Steering

Applications have varying requirements on link quality. For example, voice and video services have a low tolerance for delay (under 150 ms) and packet loss rate (under 1%). You can select an MPLS link with good quality as the primary link for the voice and video services and an Internet link as the secondary link. In addition, you need to configure the SLA requirements of the services for traffic steering based on the link SLA.

As shown in Figure 4-8, when the MPLS link or network is not congested, the MPLS link delivers good quality, over which the voice flow (VoIP flow) is transmitted. The CPE monitors the link quality in real time. If the MPLS link quality deteriorates due to congestion and the voice service SLA cannot be met, the CPE switches the voice traffic to the Internet link as it has a light load while meeting the SLA requirements. In addition, SD-WAN CPEs can detect link faults in real time. When detecting a fault on the MPLS link, the CPE dynamically migrates all services on the MPLS link to the Internet link to prevent services from being impacted.

Figure 4-8 Link quality-based traffic steering

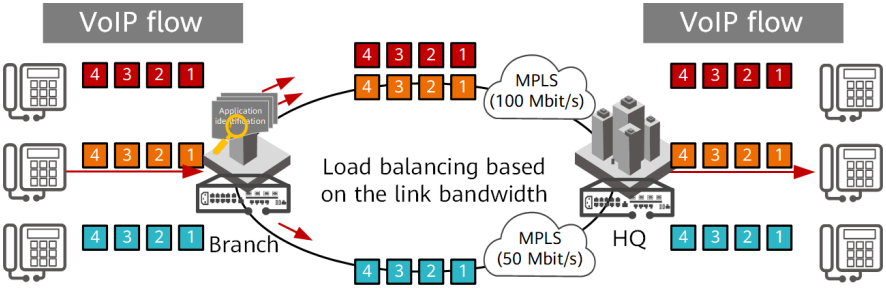


Load Balancing-based Traffic Steering

If an enterprise with multiple links wants to fully utilize the link bandwidth, you can configure load balancing-based traffic steering.

As shown in Figure 4-9, an enterprise purchases two MPLS links from different carriers: 100 Mbit/s MPLS link from carrier A and 50 Mbit/s MPLS link from carrier B, which are used as the primary links for the voice service. If the quality of both links meets the SLA requirements of the voice service, voice flows can be carried over the two MPLS links in load balancing mode, fully utilizing bandwidth resources.

Figure 4-9 Load balancing-based traffic steering

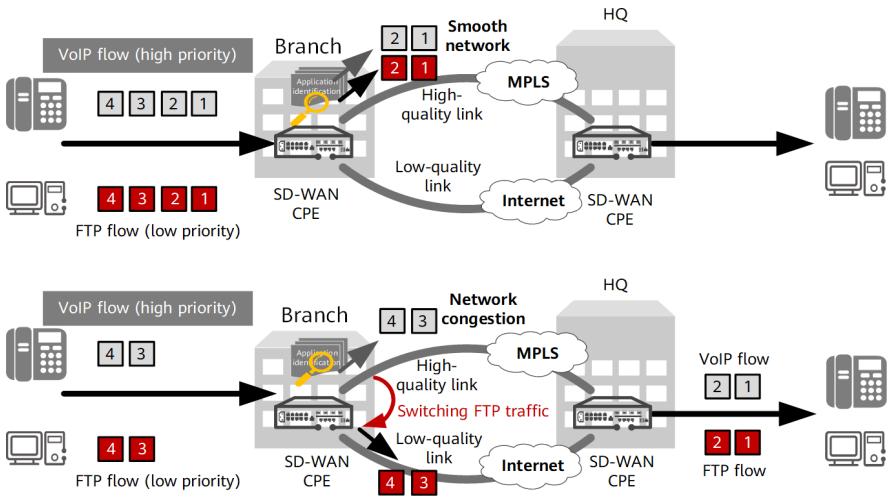


Application Priority-based Traffic Steering

If multiple types of service packets are transmitted on the same link, traffic of high-priority applications is preferentially processed when congestion occurs, ensuring user experience of high-priority applications. In this case, application priority-based traffic steering can be used. For example, voice, video, and file transfer services are carried on an MPLS link. If the link bandwidth is insufficient, the experience of the voice and video services is preferentially guaranteed.

As shown in Figure 4-10, the MPLS link offers better quality than the Internet link and is configured as the primary link for both the voice and FTP services, with the Internet link being the secondary link. The voice service takes precedence over the FTP service. As the traffic volume of the voice and FTP services increases, the MPLS link becomes congested. To ensure voice service experience, FTP service traffic is gradually migrated to the Internet link until MPLS congestion is relieved. To fully utilize the MPLS link bandwidth, FTP service traffic is gradually switched back to the MPLS link when the MPLS link recovers.

Figure 4-10 Application priority-based traffic steering



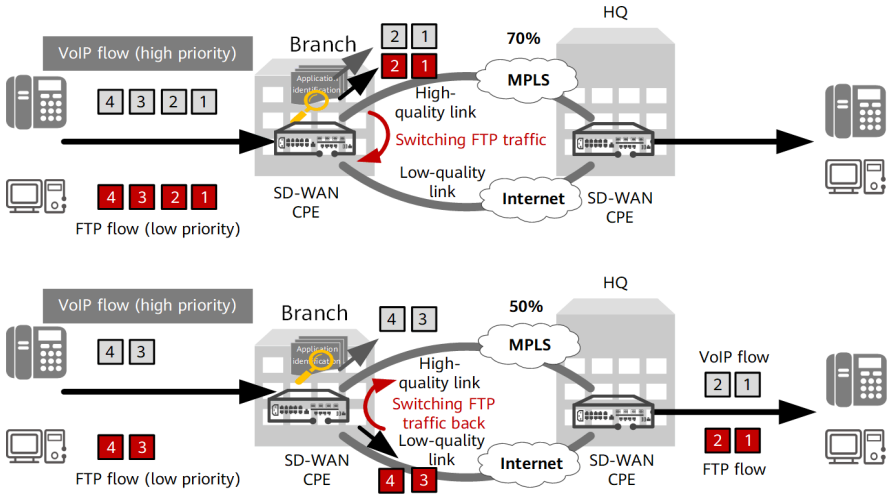
Bandwidth Utilization-based Traffic Steering

If multiple types of service packets are transmitted on the same link, to preferentially ensure experience of high-priority applications upon congestion, low-priority applications can be migrated to other SLA-compliant links when the link bandwidth utilization reaches a certain threshold. In this case, bandwidth utilization-based traffic steering can be used. For example, if both the voice and FTP services are carried over the MPLS link and the bandwidth utilization of the MPLS link reaches the upper threshold, FTP service traffic can be migrated to preferentially ensure the voice service.

As shown in Figure 4-11, the MPLS link offers better quality than the Internet link and is configured as the primary link for both the voice and FTP services, with the Internet link being the secondary link. The voice service takes precedence over the FTP service, and the upper threshold for switching traffic and lower threshold for switching traffic back are set to 70% and 50%, respectively, for the MPLS link. As the traffic volume of the voice and FTP services increases, the MPLS link becomes congested. To ensure voice service experience, FTP service traffic is gradually migrated to the Internet link once the

bandwidth utilization of the MPLS link exceeds 70%. When the bandwidth utilization of the MPLS link falls below 50%, FTP service traffic is gradually switched back to the MPLS link. This maximizes the bandwidth utilization for the MPLS link.

Figure 4-11 Bandwidth utilization-based traffic steering



4.5 WAN Optimization: Delivering Optimal Application Experience

Audio and video conferencing and video surveillance technologies are becoming more and more pervasive, posing higher requirements on bandwidth and delay. As such, the proportion of WAN-side enterprise data traffic increases explosively, which greatly increases the cost of enterprise leased lines. The unsatisfying Internet link quality brings enterprise application experience problems. To solve these problems, enterprise networks need to introduce WAN optimization technologies to optimize application access experience and reduce bandwidth costs.

FEC

FEC mitigates packet loss by applying traffic policies. It classifies traffic, obtains specific data streams, adds redundant packets that contain check information, and verifies packets at the receive end. If a packet is lost or damaged on the network, the redundant packet can be used to recover it. Figure 4-12 shows the FEC process.

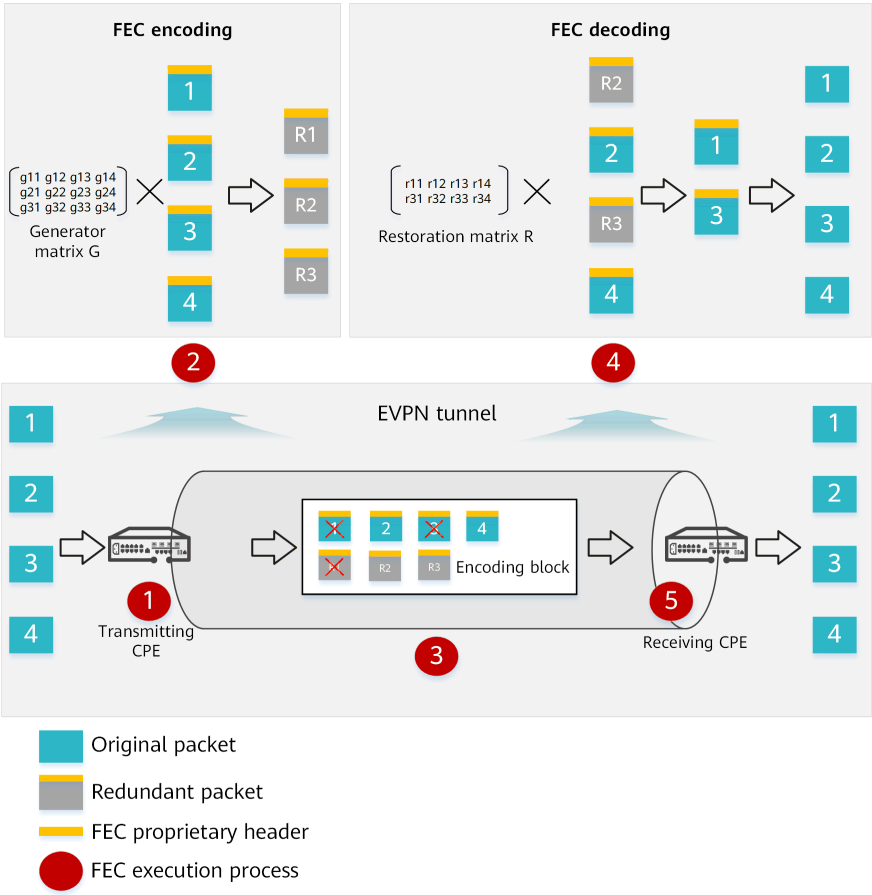
Note

FEC supports the following algorithms for generating redundant packets:

Determined FEC (D-FEC): Redundant packets are generated at a fixed redundancy rate.

A-FEC: Redundant packets are dynamically generated based on the packet loss information returned by the decoder. A-FEC is an improvement over D-FEC, and solves the problems of D-FEC, such as bandwidth waste and occasional failures to recover lost packets.

Figure 4-12 FEC process



1. **The transmitting CPE receives packets from the LAN side and implements packet loss mitigation on the traffic classified by a traffic classifier and transmitted over an EVPN tunnel.**
2. **The transmitting CPE performs FEC encoding on original packets.**
   a. **The transmitting CPE encapsulates original packets with a proprietary FEC header and sends the packets.**

b. The transmitting CPE accumulates multiple original packets as an encoding block, and encodes the original packets in the encoding block using FEC to generate FEC redundant packets. The encoding end can generate multiple redundant packets for multiple packets based on the generator matrix algorithm.

3. When packets are transmitted on the network, both original packets and redundant packets in the encoding block may be lost.
4. The receiving CPE performs FEC decoding on the received original packets and redundant packets.

   a. The receiving CPE receives packets from the network, detects packet loss information, and performs FEC decoding. It calculates a decoding matrix (restoration matrix) based on the encoding matrix and received packets, and recovers lost original packets (if any) based on the decoding matrix and received packets. The lost packets in an encoding block can be recovered as long as the lost packets are fewer than the redundant packets.

   b. After the receiving CPE completes decoding, it restores the lost packets and removes the proprietary header.

5. The receiving CPE sends packets to the LAN side at the receive end, and sends the restored packets to the receive end in sequence.

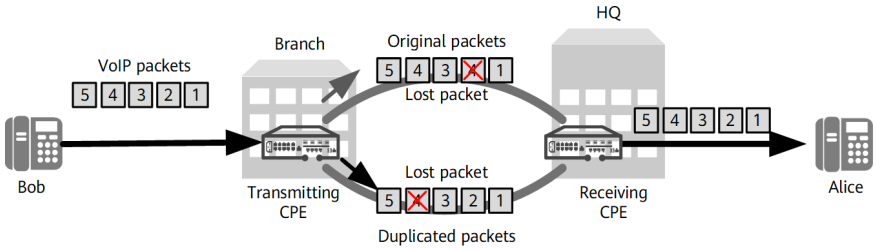
Multi-Path Packet Duplication

Multi-path packet duplication (dual-fed and selective receiving) mitigates packet loss. This feature enables the CPE at the transmit end to duplicate data packets and send the original and duplicated packets over two links. If packet loss occurs on one link, the CPE at the receive end uses the duplicated packet transmitted over the other link to restore the lost packet, requiring no retransmission. This feature is applicable to services with low traffic but requiring high reliability, for example, VoIP and payment services.

Figure 4-13 shows the multi-path packet duplication process. Leveraging multi- path packet duplication technology, the CPE at the transmit end makes a copy of data packets in a data flow and sends these data packets through multiple links. When combined with intelligent traffic steering, multi-path packet duplication selects two optimal links for transmission. The CPE at the receive end then

caches and deduplicates the received data packets to restore the original data flow.

Figure 4-13 Multi-path packet duplication

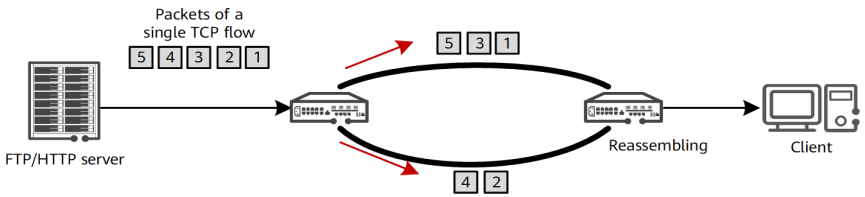


Per-Packet Load Balancing

On a network, elephant flows may exceed the bandwidth of a link, while other links are idle. In this case, per-packet load balancing can be used to distribute elephant flows to multiple links, improving link utilization. This feature significantly improves the transmission efficiency of large files at sites with multiple egress links and is suitable for applications such as FTP/HTTP large file download and data backup and replication.

Figure 4-14 shows the process of per-packet load balancing. The transmit end applies a traffic steering policy to traffic and implements per-packet load balancing on all available links that meet SLA requirements. The packet information to be encapsulated includes the packet sequence number, path number, path-based sequence number, and timestamp. The receive end resequences the out-of-order packets in the buffer to solve the packet disorder issue caused by the delay difference between different paths, and forwards data to devices in sequence.

Figure 4-14 Per-packet load balancing

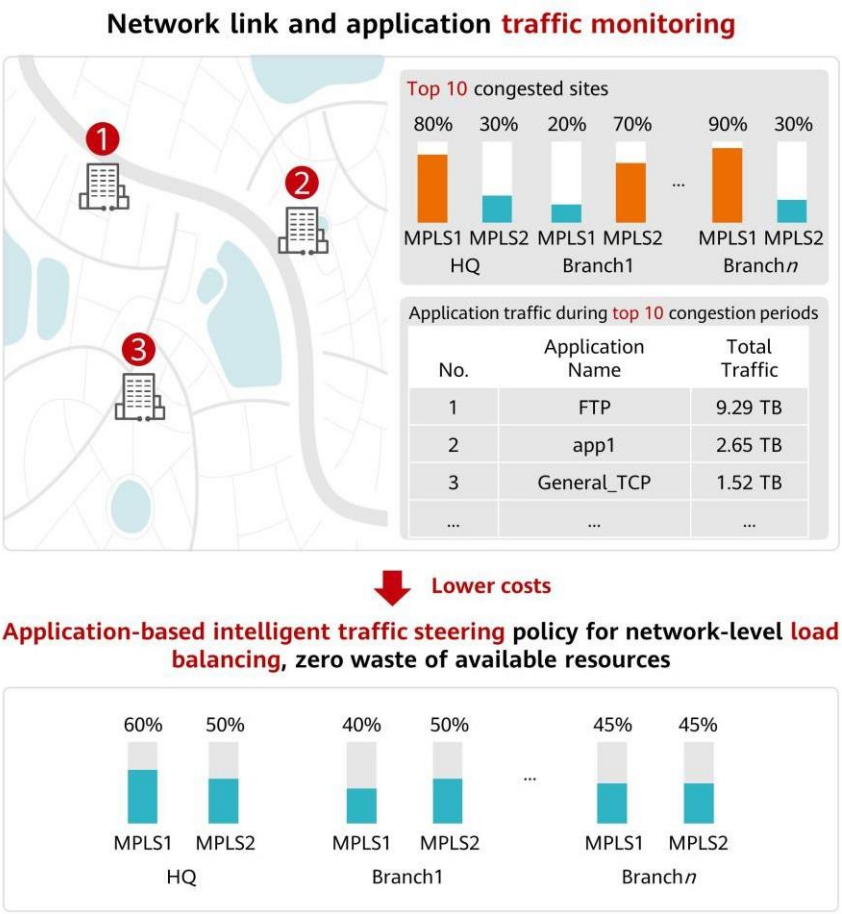


4.6 Intelligent Policy Recommendation: Facilitating WAN Experience Assurance

WANs are large in scale and consist of devices from multiple carriers. The traffic steering optimization of key applications relies on experience and per-site configuration, making it difficult to achieve proper load balancing. In addition, the link costs of enterprises are high. The purchased bandwidth usage cannot be detected, so there is no basis for expanding or reducing the link bandwidth. The SD-WAN Solution offers the intelligent policy recommendation function to improve network-wide bandwidth utilization and speed up the policy configuration.

Intelligent Traffic Steering Recommendation

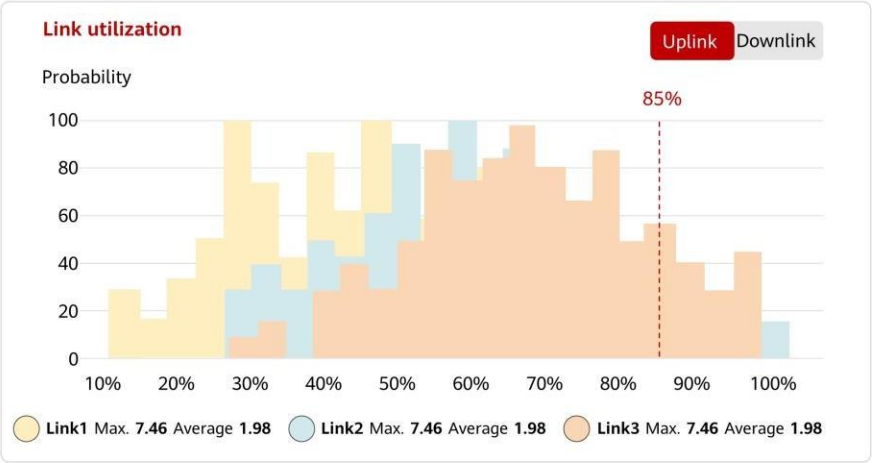
Intelligent traffic steering policy recommendation analyzes traffic data of network links and applications between the HQ and branches, generates global optimal traffic steering policies that achieve network-level load balancing for top congested sites and traffic-intensive applications, and displays simulation effects of service traffic after recommended policies are applied. Users can select the optimal traffic steering policy with one click after evaluation, automatically utilizing live-network resources optimally and achieving global optimal network balancing.



Bandwidth Analysis

The bandwidth analysis function models the link traffic, analyzes historical services and future trends, and provides global optimal bandwidth planning suggestions for enterprises and chain stores to purchase WAN bandwidth, by utilizing the live-network traffic model deduction capability of big data. This function maximizes link bandwidth utilization and improves economic benefits while ensuring lossless services.

Big-data-based live-network traffic model deduction

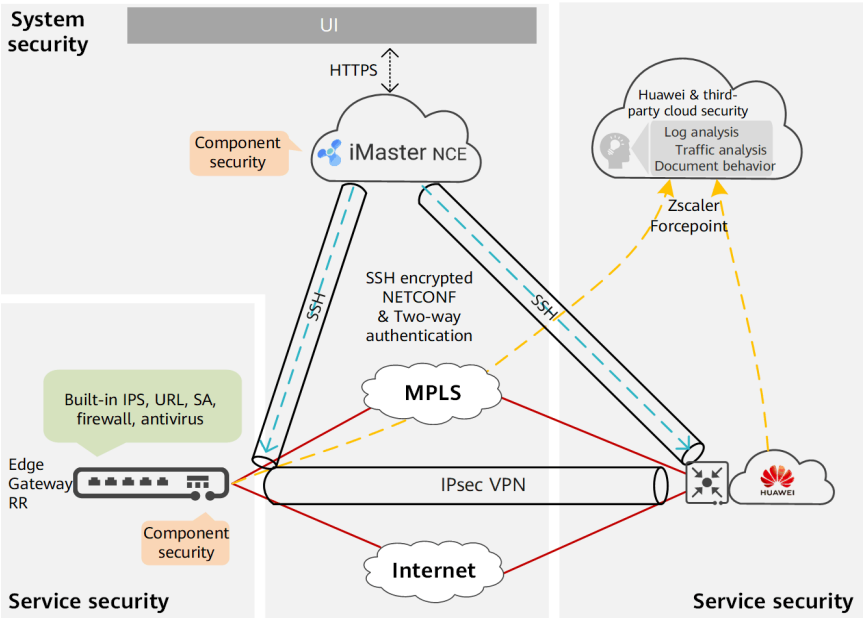


Global optimal bandwidth planning, one-click visualization of network-wide congestion, simplifying application experience O&M

4.7 Proactive Defense: Building E2E Security

Huawei's SD-WAN Solution ensures security from the aspects of system security, service security, and component security, as shown in Figure 4-15.

Figure 4-15 SD-WAN security



- **System security: basic security capabilities of Huawei's SD-WAN Solution, which ensure secure and reliable running of the SD-WAN Solution and are available upon system initialization.**
- **Service security: independently deployed security functions. Service security functions can be flexibly deployed based on the service security requirements of enterprises.**
- **Component security: security functions provided by iMaster NCE, CPEs, and RRs. Component security must be considered during component deployment.**

System Security

System security involves communication security between components of Huawei's SD-WAN Solution and multi-tenant security. Huawei's SD-WAN Solution consists of multiple components. The components and the

communication between them may encounter security threats. Therefore, security measures must be taken to ensure the security and reliability of Huawei's SD-WAN Solution. Specifically, system security covers:

- Inter-component communication security: Management channels, control channels, and data channels are established between components using secure communication protocols to ensure communication data security. Table 4-2 lists the inter-component communication security functions.

Table 4-2 Inter-component communication security functions

Type	Security Function
Management channel security	For the email-based deployment feature, the URL in the email is encrypted. CPEs/RRs and iMaster NCE authenticate each other through certificates. When a device registers with iMaster NCE and goes online, iMaster NCE verifies the equipment serial number (ESN) of the device. Unauthorized devices are not allowed to register with iMaster NCE. NETCONF over SSH is used to ensure security of key configuration data. HTTP/2 over SSL ensures security of reported performance data. The site isolation function isolates insecure devices from a network.
Control channel security	A CPE registers with an RR through DTLS. CPEs and RRs authenticate each other through certificates. IPsec is used to encrypt data transmitted between CPEs and RRs.
Data channel security	The IPsec ESP protocol, SHA2-256 and SM3 authentication algorithms, and AES-256, AES-128, and SM4 encryption algorithms are used between CPEs and between CPEs and gateways to ensure data confidentiality and integrity during transmission.

- Management VPN: When a CPE accesses a third-party server through an overlay tunnel, an independent overlay VPN is created on the CPE to implement secure communication with the third-party server.
- Multi-tenant security: In the carrier/MSP resale scenario, carriers/MSPs need to provide SD-WAN services for many enterprises. iMaster

supports multi-tenancy and provides different management and control channels for tenants, implementing security isolation.

- Certificate management: To ensure security of the entire SD-WAN system, edges, gateways, RRs, and iMaster NCE use certificates for communication.

Service Security

Service security refers to security of services carried by Huawei's SD-WAN Solution. Based on the service model of an enterprise, service security covers the security of the inter-site access, Internet access, and cloud access services.

To ensure service security, Huawei's SD-WAN Solution takes the following measures to prevent attacks and intrusions from the Internet:

- CPEs provide a wealth of built-in security capabilities, including ACL-based packet filtering, 802.1X, firewall, intrusion prevention system (IPS), antivirus, and URL filtering, meeting service security requirements in different scenarios.
- Physical firewalls can be connected to CPEs in off-path mode to provide advanced security protection functions as VASs.
- When enterprises access the public cloud and SaaS, third-party cloud security gateways such as Zscaler and Forcepoint can be deployed to implement security detection on traffic and provide functions such as access control, threat prevention, and data protection.

Component Security

Component security covers security of each component, including:

- iMaster NCE

  As the brain of the entire network, iMaster NCE is prone to attacks. Its open APIs and southbound protocols face various security risks and challenges. iMaster NCE is deployed in an area protected by the firewall. Security hardening can be implemented on iMaster NCE in terms of authentication and permission control, data protection, security detection and response, privacy protection, security management, system protection, and security deployment, mitigating security risks.

- **Edge, gateway, and RR**

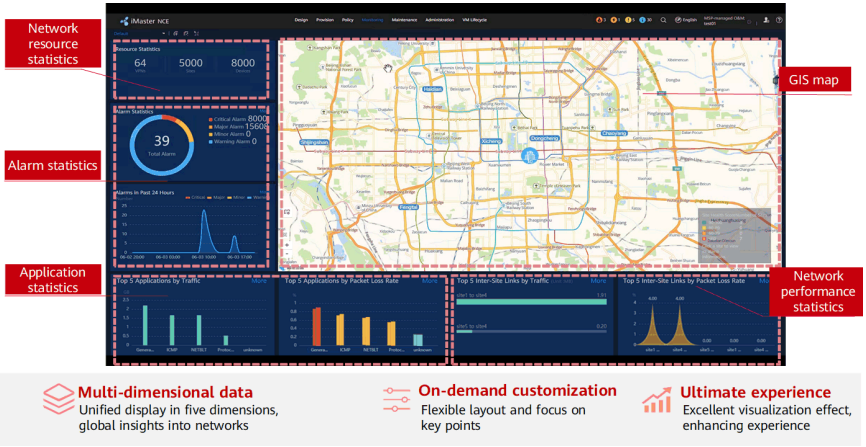
The system architecture of the edge, gateway, and RR complies with ITU-T X.805. Based on the three-layer and three-plane security isolation mechanism, the control plane, management plane, and forwarding plane are isolated from each other to ensure that the other planes are not affected when any plane is attacked. In addition, Huawei's SD-WAN Solution provides multiple security defense capabilities, such as physical security, data security, authentication, attack defense, and security audit.

4.8 Visualized O&M and Monitoring: Improving O&M Efficiency

Digital Dashboard: Integrated O&M Monitoring GUI

Huawei's SD-WAN Solution displays the network-wide status through the topology, geographic information system (GIS), and over 50 reports, as shown in Figure 4-16. This improves O&M efficiency and service experience.

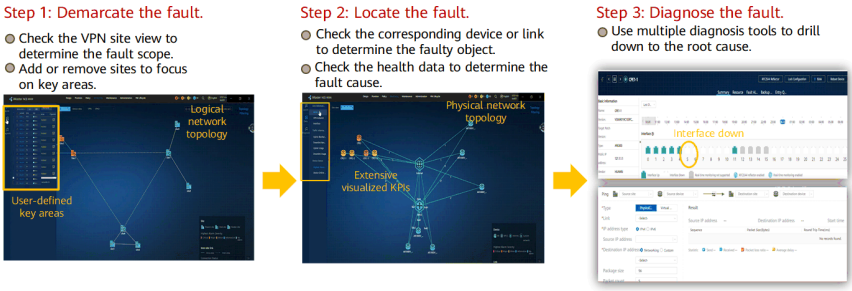
Figure 4-16 Digital dashboard



Topology-based One-stop O&M

Figure 4-17 illustrates the implementation of topology-based one-stop O&M, making the physical and logical networks visible to each other. In addition, common diagnosis tools are integrated to locate typical faults with one click.

Figure 4-17 Topology-based one-stop O&M



Agile Reports

Huawei's SD-WAN Solution flexibly displays data such as devices, links, network performance, and alarms, as shown in Figure 4-18. Through drag-and-drop operations and self-service analysis, agile reports provide a solid basis for service decision-making, as shown in Figure 4-19.

Figure 4-18 Site monitoring report

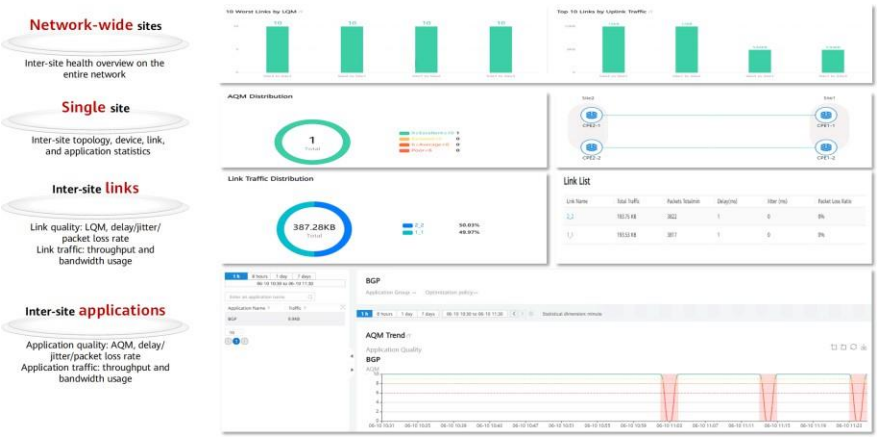
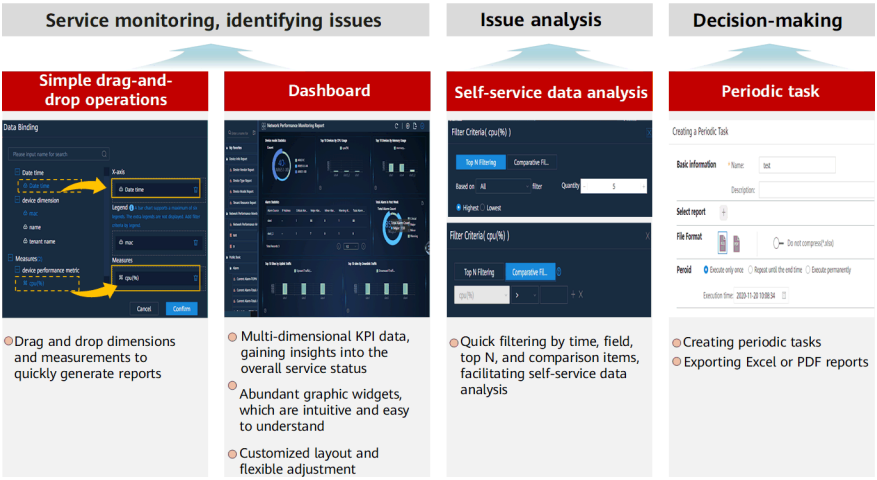


Figure 4-19 Agile report

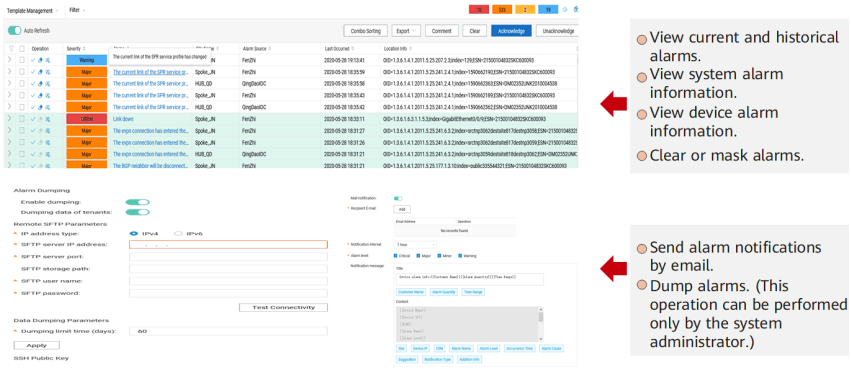


Precise Alarm Email Notifications

As shown in Figure 4-20, Huawei's SD-WAN Solution supports multiple alarm management methods, which help you understand the network health status in a timely manner.

- **Alarms generated by the controller and CPEs can be reported, including power-off, restart, and service interruption alarms.**
- **The fields contained in the alarm information and alarm dumping settings, such as the number of entries retained and retention period based on service requirements, can all be customized.**

Figure 4-20 Alarm management



Chapter 5
Typical SD-WAN Networking

Abstract

This chapter describes the application scenarios, topology, and device model selection of typical SD-WAN networking models.

5.1 Enterprise HQ + Branch (Hub-Spoke Networking)

Application Scenario

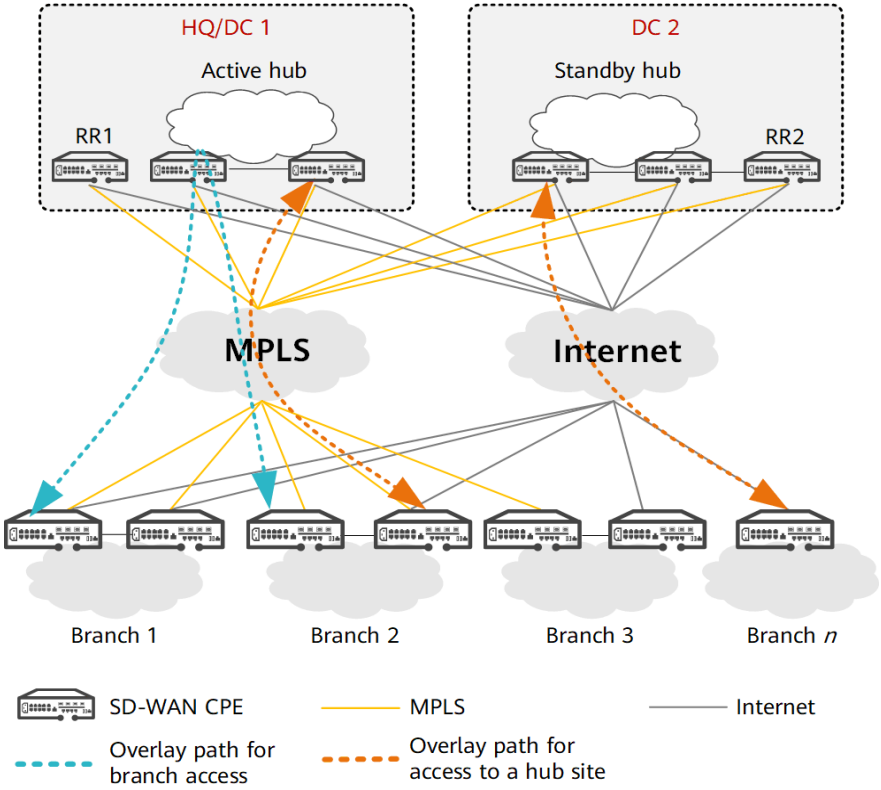
An enterprise has one or two DCs. Branches access services deployed in the HQ or DCs through the WAN. A small amount of traffic is transmitted between branches, or branches do not need to communicate with each other. Traffic between branches traverses the HQ or DCs.

Networking Topology

Networking: A flattened single-layer hub-spoke network is deployed between branches and the HQ, as shown in Figure 5-1. The enterprise HQ and DCs function as hub sites, and branches function as spoke sites.

O&M: Tenants manage all their SD-WAN sites and networks independently. Typically, one controller is deployed in the central equipment room for the entire network. If geographic redundancy is required, two controllers need to be deployed in active/standby mode in the active and standby equipment rooms and are interconnected with each other at Layer 3.

Figure 5-1 Networking diagram



Device Model Selection

Table 5-1 Device model selection

Site Type	Device Model
Hub site	AR8140, AR6710-H, AR6280, and AR6300 series
RR site	AR8140, AR6710-H, AR6280, and AR6300 series

Site Type	Device Model
Spoke site (branch site)	Large branches: AR8140, AR8700, AR6710-H, AR6280, and AR6300 series Midsize branches: AR6710-L, AR6120, and AR6140 series Small branches: AR5700, AR650, and AR610 series

5.2 Enterprise HQ + Branch (Full-Mesh Networking)

Application Scenario

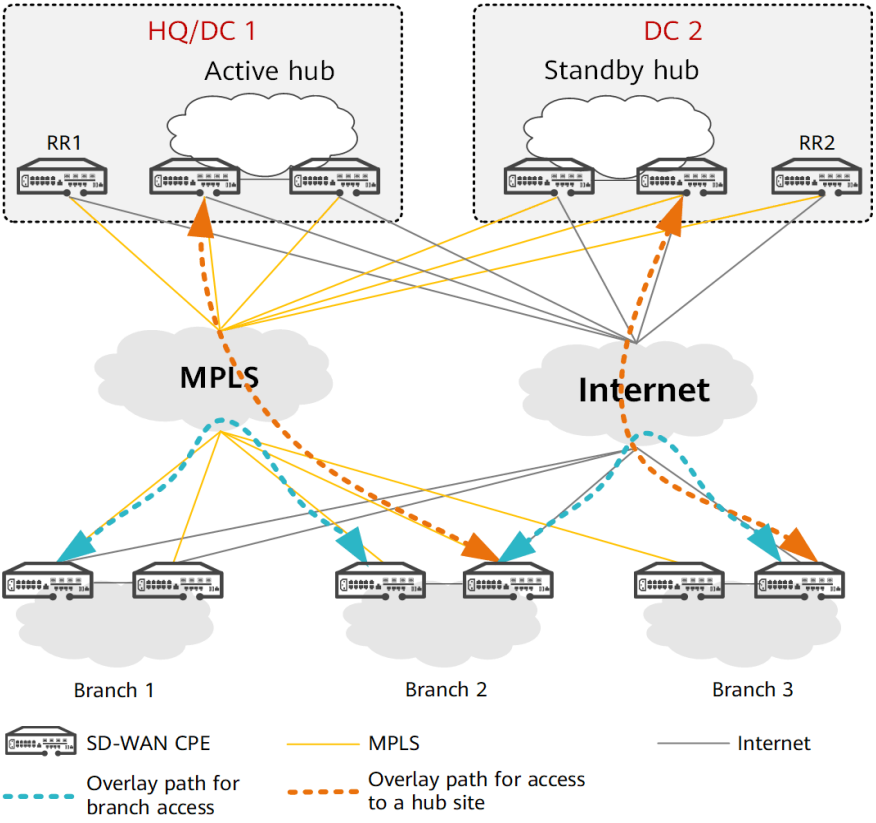
The full-mesh topology is applicable to small enterprises with a small number of sites or large enterprises whose branches need to collaborate with each other. Large enterprises' collaborative services, for example, high-value applications including VoIP and video conferencing, have stringent requirements on network performance such as the packet loss rate, delay, and jitter. To meet requirements of such services, branches are recommended to directly communicate with each other.

Networking Topology

Networking: In the full-mesh topology shown in Figure 5-2, branches can directly communicate with each other, without the need to divert traffic through intermediate nodes.

O&M: Tenants manage all their SD-WAN sites and networks independently. Typically, one controller is deployed in the central equipment room for the entire network. If geographic redundancy is required, two controllers need to be deployed in active/standby mode in the active and standby equipment rooms and are interconnected with each other at Layer 3.

Figure 5-2 Networking diagram



Device Model Selection

Table 5-2 Device model selection

Site Type	Device Model
RR site	AR8140, AR6300, and AR6280 series

Site Type	Device Model
HQ/Branch site	HQ/Large sites: AR8140, AR8700, AR6300, and AR6280 series Midsize sites: AR6700, AR6140, and AR6280 series Small sites: AR5700, AR6140, and AR6280 series

5.3 Enterprise HQ + Regional Center + Branch (Hierarchical Networking)

Application Scenario

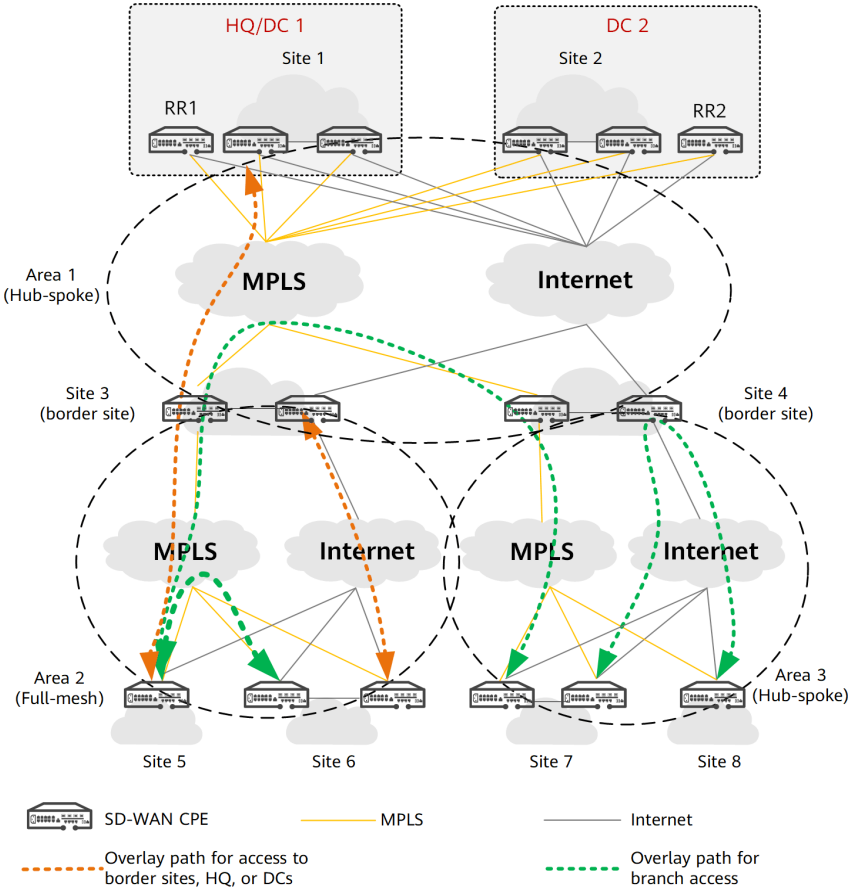
This networking features a clear network structure and excellent scalability and is therefore applicable to enterprises that have a large number of sites or multinational enterprises with sites widely distributed across countries or regions.

Networking Topology

Networking: This network model can be considered as the combination of single-layer network models. WANs are divided into multiple areas, which are interconnected through a centralized backbone area. This implements inter-area communication between a large number of sites. Figure 5-3 shows the networking.

O&M: Tenants manage all their SD-WAN sites and networks independently. Typically, one controller is deployed in the central equipment room for the entire network. If geographic redundancy is required, two controllers need to be deployed in active/standby mode in the active and standby equipment rooms and are interconnected with each other at Layer 3.

Figure 5-3 Networking diagram



Device Model Selection

Table 5-3 Device model selection

Site Type	Device Model
HQ/DC/Border site	AR8140, AR6280, and AR6300 series
RR site	AR8140, AR6280, and AR6300 series
Branch site	Large branches: AR8140, AR8700, AR6280, and AR6300 series Midsize branches: AR6700, AR6120, and AR6140 series Small branches: AR5700, AR650, and AR610 series

5.4 Enterprise Multi-DC + Branch (Multi-Hub Networking)

Application Scenario

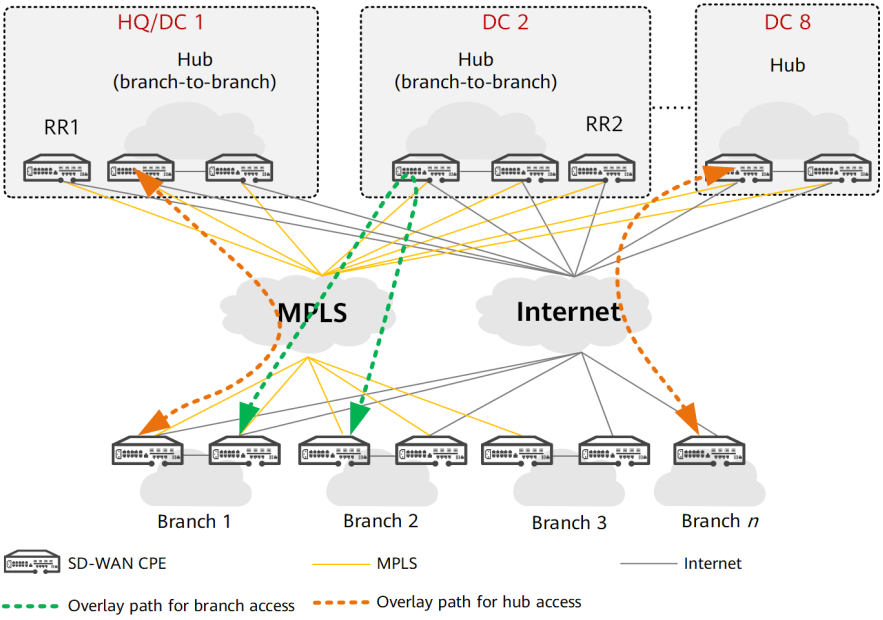
This networking is applicable to enterprises that have multiple DCs and deploy service servers in each DC to provide services for branches.

Networking Topology

Networking: The essence of this networking is the hub-spoke networking, in which up to eight hub sites can be deployed. Generally, multiple DCs of an enterprise function as hub sites to provide services for branches. When branches need to communicate with each other, you can enable the traffic diversion function on two hub sites for inter-branch service access. Figure 5-4 shows the networking.

O&M: Tenants manage all their SD-WAN sites and networks independently. Typically, one controller is deployed in the central equipment room for the entire network. If geographic redundancy is required, two controllers need to be deployed in active/standby mode in the active and standby equipment rooms and are interconnected with each other at Layer 3.

Figure 5-4 Networking diagram



Device Model Selection

Table 5-4 Device model selection

Site Type	Device Model
Hub site (DC)	**AR8140, AR6280, and AR6300 series**
RR site	**AR8140, AR6280, and AR6300 series**

Site Type	Device Model
Spoke site (branch site)	Large branches: AR8140, AR8700, AR6280, and AR6300 series Midsize branches: AR6700, AR6120, and AR6140 series Small branches: AR5700, AR650, and AR610 series

5.5 Multi-Tenant IWG (POP Networking)

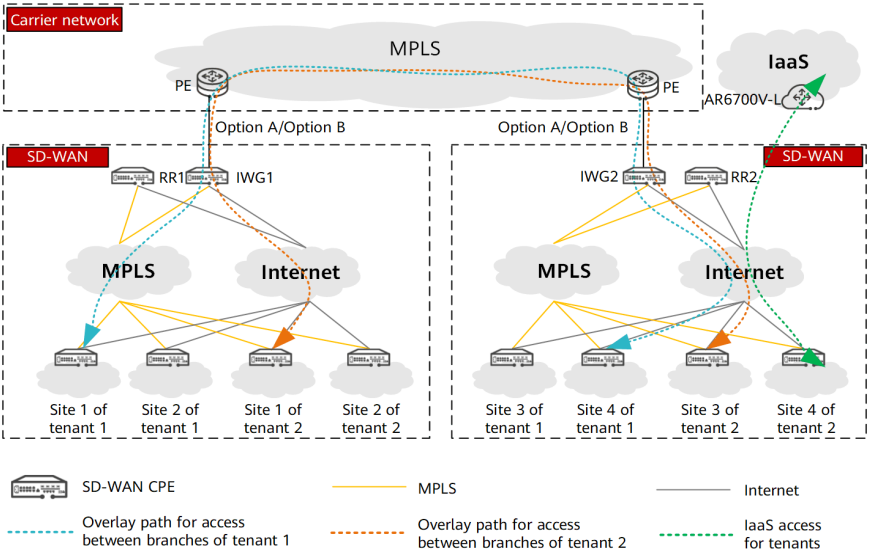
Application Scenario

When carriers or MSPs provide SD-WAN access services for enterprises, some enterprises may have both legacy branch sites and SD-WAN sites, which need to interwork with each other. This networking is applicable to such a scenario. The Interworking Gateway (IWG) can connect both SD-WAN sites and legacy MPLS VPN sites for multiple enterprise tenants.

Networking Topology

In the multi-tenant IWG networking, an IWG site needs to be deployed as the POP to connect to the legacy MPLS backbone network. Option A based on Layer 3 VLAN/Layer 3 VXLAN or inter-AS MPLS VPN Option B is used for interconnection, and an independent RR is deployed. Tenant sites and IWGs are deployed in hub-spoke networking. In addition, the AR6700V-L is deployed in the Virtual Private Cloud (VPC) of the public cloud to implement secure connection between branches and the IaaS. Figure 5-5 shows the networking.

Figure 5-5 Networking diagram



Device Model Selection

Table 5-5 Device model selection

Site Type	Device Model
IWG	AR8140 series, AR6300 series, AR6280 series, and AR6700V-L
RR site	AR8140 series, AR8700 series, AR6300 series, AR6280 series, and AR6700V-L
Branch site	Large branches: AR8140, AR8700, AR6300, and AR6280 series Midsize branches: AR6700, AR6120, and AR6140 series Small branches: AR5700, AR650, and AR610 series

Chapter 6
Typical Applications

Abstract

This chapter describes the typical applications of Huawei's SD-WAN Solution in the finance industry and carrier/MSP resale scenarios.

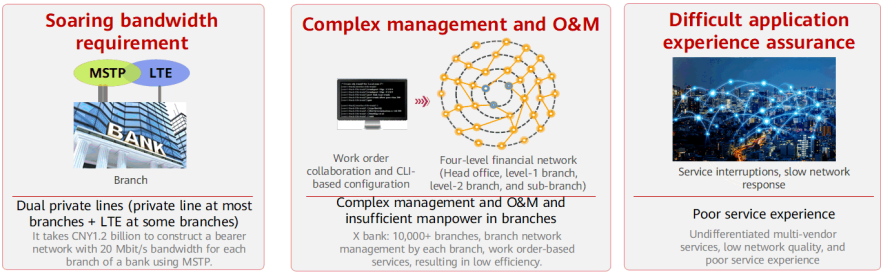
6.1 Finance Industry

Pain Points

The finance industry covers banking, insurance, and securities sectors. The traditional financial business model is transforming significantly as the development of social media and mobile technologies continues to boost Internet financial services, as shown in Figure 6-1. In addition to traditional transaction services, pan-financial services are growing rapidly, including online apps as well as diversified offline services, such as object recognition, big data, image, voice, artificial intelligence (AI), Virtual Teller Machine (VTM), and self- help services. This poses higher requirements on the bandwidth, delay, and service experience of the WAN. However, existing branch private lines offer low bandwidth, which is insufficient for diversified services. The construction of new

MPLS private lines is costly. For example, for 2000 sites each with 10 Mbit/s bandwidth, the annual private line cost is over CNY100 million. In addition, provisioning MPLS private lines takes a long time, severely affecting service provisioning efficiency.

Figure 6-1 Challenges faced by the finance industry

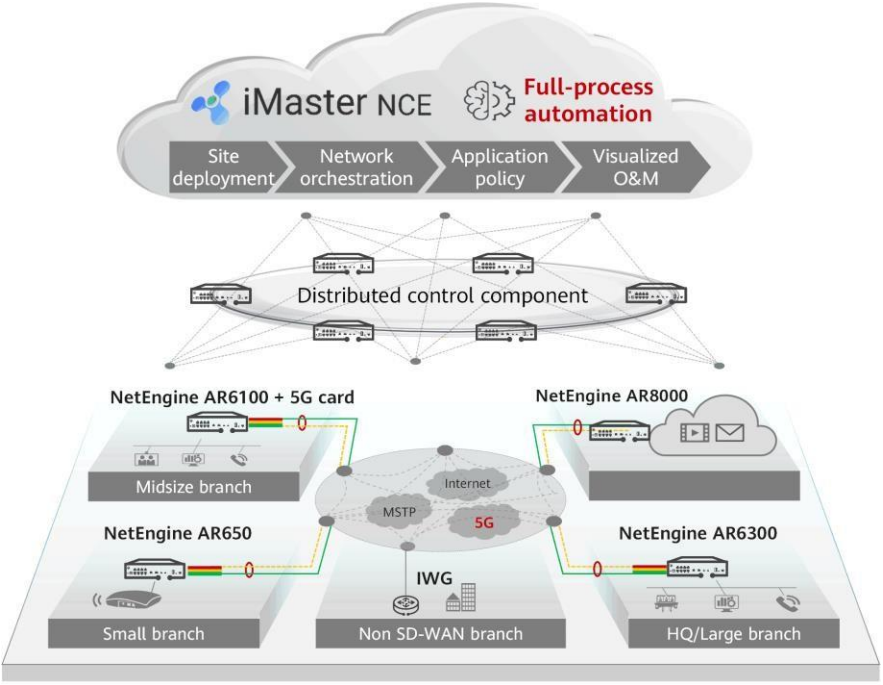


Networking Solution

To cope with the challenges faced by the finance industry, Huawei launches the SD-WAN Solution for the finance industry. The solution implements real-time synchronization between systems to ensure service continuity, efficiency, and stability of all branches, as well as data security.

Figure 6-2 shows the typical architecture of the SD-WAN Solution for the finance industry.

Figure 6-2 Typical architecture of the SD-WAN Solution for the finance industry



- **Multi-DC disaster recovery (DR)**

  DCs are built in multiple cities, and cloud-based interconnection between DCs is implemented through the core backbone network.

- **Layered and flattened networking, delivering an innovative experience**

  SD-WAN for the HQ and level-1 branches: covers the core backbone network between the HQ and level-1 branches.

  SD-WAN for branches: covers the WAN networking of level-1 branches, level-2 branches, and sub-branches.

  Built-in 5G cards provide the industry's optimal 5G network, allowing high bandwidth and low latency for innovative financial services.

- **Application-based intelligent traffic steering, ensuring experience of key applications**

- **Application-based intelligent traffic steering enables on-demand scheduling based on 5G and fibers.**
- **A-FEC ensures that no frame freezing or artifact occurs even at 30% packet loss.**

- **Full-process automation, multi-tenant hierarchical authorization, and domain-based independent O&M**
  - **Multiple ZTP modes, enabling branch networks to be deployed within minutes**
  - **Visibility of application, branch, device, and link status, enabling centralized management and simplifying O&M**
  - **Multi-tenant hierarchical authorization, enabling independent O&M for HQ, branches, and sub-branches**

Customer Benefits

- **High bandwidth and low latency for new virtual reality (VR)/augmented reality (AR) services in smart branches: High-speed Ethernet and 5G links, application-based intelligent traffic steering, and optimization ensure that traffic of key services such as securities is always transmitted over the optimal link, delivering an optimal service experience.**
- **Provisioning of branch networks within 30 minutes: Leveraging diverse ZTP modes, branch networks can be provisioned within 30 minutes, ensuring quick service rollout during branch construction, migration, and capacity expansion.**
- **Intelligent O&M and unified management: The status of the entire network, branch nodes, users, and applications is visualized, simplifying O&M, achieving a fully automated process, and reducing labor investment.**

6.2 **Carrier/MSP Resale**

Pain Points

A customer's legacy virtual private dial-up network (VPDN) carries services such as transaction, inventory management, and video surveillance across

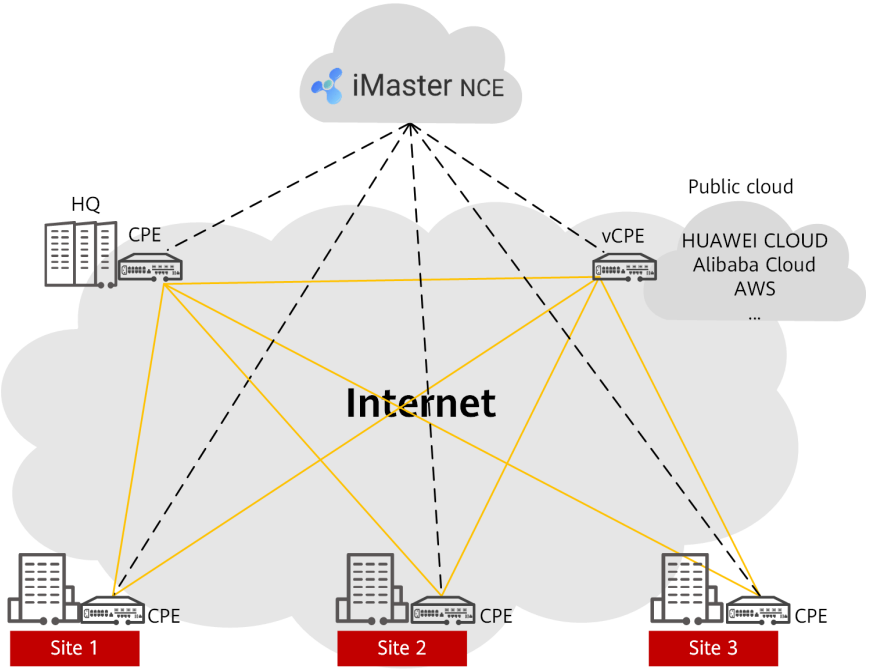
1,600 stores.

Due to outdated devices, the network cannot meet the customer's fast-growing application and service expansion requirements.

Networking Solution

As shown in Figure 6-3, a carrier/MSP combines the Internet and SD-WAN Solution to replace the legacy VPDN network and centrally manage all tenant networks in the country.

Figure 6-3 Networking diagram



Customer Benefits

- **50% lower private line costs: The Internet is introduced to replace or back up private lines, reducing WAN bandwidth costs and offering higher bandwidth.**
- **Fast service provisioning: ZTP enables devices to go online quickly, enabling fast service provisioning for stores.**
- **Simplified O&M: A visualized management platform and automatic O&M services are provided to simplify network O&M.**

Chapter 7
Product Portfolio

Abstract

This chapter describes the product portfolio of Huawei's SD-WAN Solution.

7.1 NetEngine AR Routers

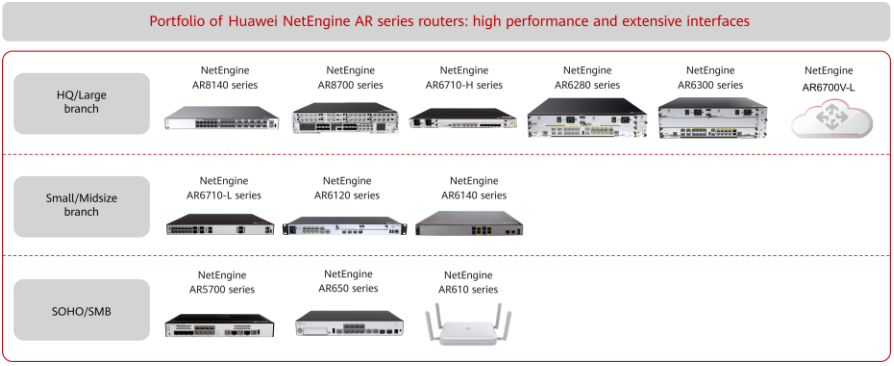
Huawei's NetEngine AR routers are core components at the network layer and control layer in Huawei's SD-WAN Solution. They can function as RRs, edge nodes, and gateways and are available in NetEngine AR series and NetEngine AR6700V-L.

NetEngine AR Series Routers

Designed for the cloud era, Huawei's NetEngine AR series routers integrate various service features such as SD-WAN, cloud management, VPN, MPLS, security, and voice. These feature-rich routers provide high performance to meet diversified service requirements of enterprise customers at all scales, including

SOHO/SMB, small/midsize branches, and HQ/DCs. Figure 7-1 shows the portfolio of NetEngine AR series routers.

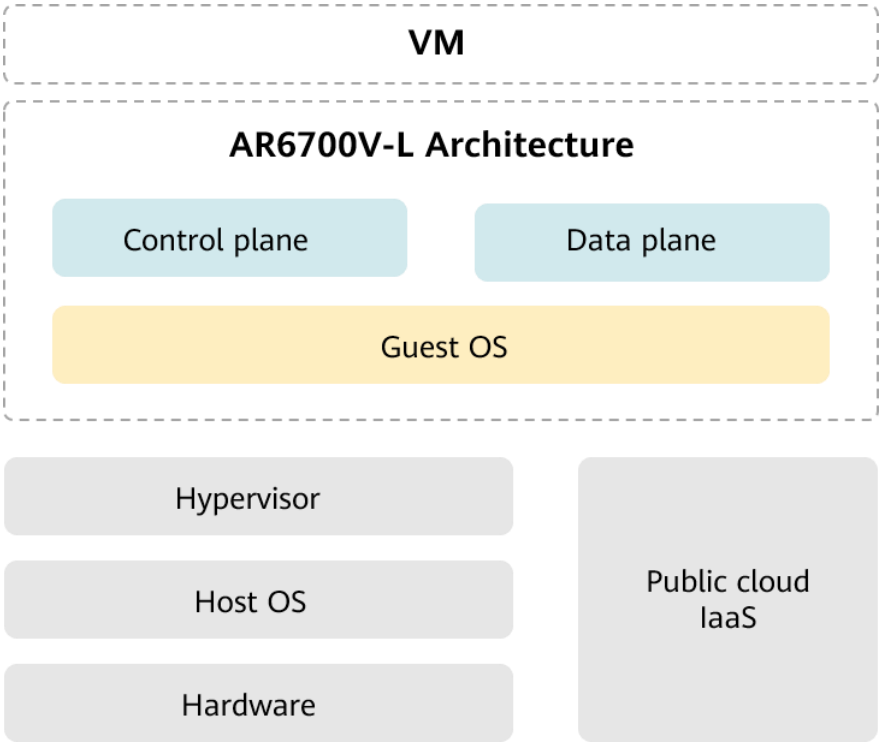
Figure 7-1 Portfolio of NetEngine AR series routers



NetEngine AR6700V-L

As shown in Figure 7-2, the NetEngine AR6700V-L is a next-generation virtual router developed by Huawei to meet various network requirements of enterprises in cloud scenarios. It can be flexibly deployed in virtualization and public cloud environments to function as a virtual customer-premises equipment (vCPE) or virtual gateway in Huawei SD-WAN Solution or function as a cloud access gateway.

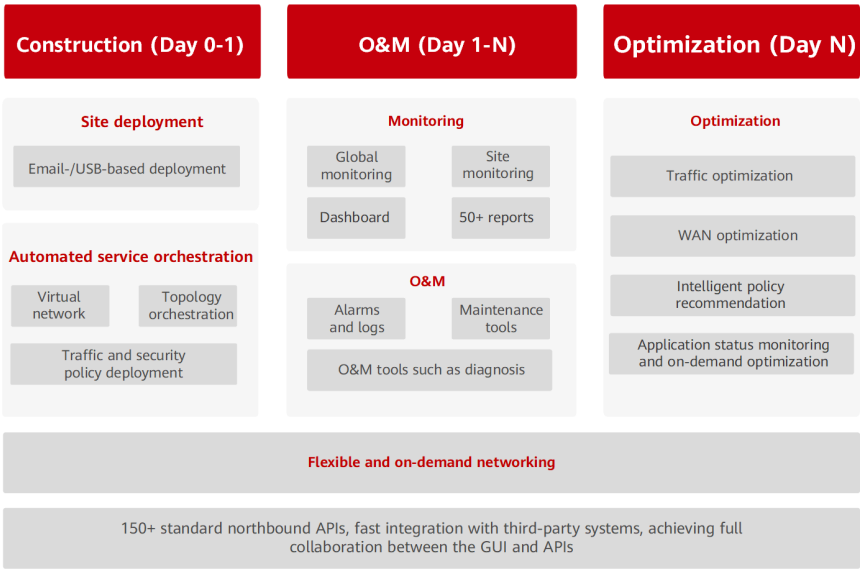
Figure 7-2 Huawei NetEngine AR6700V-L



7.2 iMaster NCE

As the network controller of Huawei's SD-WAN Solution, iMaster NCE is a core component at the management layer. It provides capabilities such as EVPN, fast service deployment, multi-network orchestration, application-based experience optimization, and intent-based monitoring and O&M, implementing automated and intelligent management across the full lifecycle of SD-WAN networks. Figure 7-3 shows the portfolio of iMaster NCE's network management and orchestration capabilities.

Figure 7-3 Portfolio of iMaster NCE's network management and orchestration capabilities



Note

In this document, Huawei iMaster NCE refers to iMaster NCE-Campus, which is an SD-WAN controller.

A Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
A-FEC	Adaptive FEC
D-FEC	Determined FEC
FEC	Forward Error Correction
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
IWG	Interworking Gateway
LTE	Long Term Evolution
MEF	Metro Ethernet Forum
MPLS	Multi-Protocol Label Switching
NFV	Network Functions Virtualization
ONUG	Open Networking User Group
POP	Point of Presence
QoS	Quality of Service
RR	Route Reflector

Acronym and Abbreviation	Full Name
SaaS	Software as a Service
SD	Software Defined
SD-WAN	Software Defined Wide Area Network
SDN	Software Defined Network
SLA	Service Level Agreement
WAN	Wide Area Network
WOC	WAN Optimization Controller
ZTP	Zero-Touch Provisioning

enquiries@aritofafrica.com, support@aritofafrica.com
www.aritofafrica,com

arit of africa ltd