



Striding Towards  
the Intelligent World  
White Paper

# Data Communication

Connecting Ubiquitous  
Computing Power and  
Intelligent Living



# Foreword

---

We are currently at a historical juncture on our journey towards an intelligent world, which needs to be built through digital and intelligent transformation.

The digital and intelligent wave has also set off a new round of transformation for global enterprises. Facing increasingly complex internal and external environments, diversified customer requirements, and new service scenarios, enterprise IT urgently needs digital products with low costs, high agility and scalability, and strong support for service and technology innovation. From a global perspective, enterprise IT has undergone the following major changes:

- 1. Multi-cloud becoming a consensus among enterprises:** The multi-cloud architecture integrates private and public clouds. This architecture enables enterprises to flexibly allocate hosting policies based on service and security requirements changing with time and space. This way, multi-cloud features such as economies of scale and high flexibility and scalability are brought into full play, ultimately cutting costs and improving efficiency.
- 2. Increasing IoT deployment scale:** IoT technologies play an increasingly important strategic role in various scenarios, be it efficient and convenient offices, efficient and secure industrial production, busy public transportation, air and ground logistics systems, or buildings for countless industries. As an extension of communications networks and the Internet, IoT uses sensing technologies and intelligent devices to enable enterprises and individuals to control

the physical world in real time, accurately manage it, and make science-based decisions through digital means.

- 3. Hybrid office becoming the new normal:** Since the pandemic, working remotely has become commonplace. Currently, more than 80% of employees want their employers to continue to support remote work. However, such a working mode brings data security risks. Indeed, data leakage caused by phishing attacks and ransomware has become the biggest security risk for enterprises. To cope with an onslaught of such challenges, enterprises want to integrate security products into multi-functional solutions.
- 4. Increasing IT O&M difficulty:** Driven by new technologies such as mobility, big data, cloud computing, and AI, there is an explosion in the numbers of NEs, technology stacks, services, and more involved in the enterprise IT architecture. Currently, service experience is being severely affected by inefficient service fault locating resulting from insufficient O&M manpower, lack of network visualization methods, and numerous false alarms. Enterprises' IT systems urgently need digitalization technologies.

These changes drive the transformation of the enterprise data communication network architecture. Looking back at the development of data communication networks, we can see they have gone through five phases: academic research, explosive World Wide Web application, social media and multi-service transport, short-form video and mobile Internet, and

cloud era and industry digitalization. Indeed, the world of the future will be a digital world featuring connectivity of everything, intelligent connectivity of everything, and connected intelligent twins. IP networks support more and more application scenarios. We believe that networks will soon enter the era of 5.5G, which focuses on the continuous advancement of key trends such as multi-cloud synergy, ubiquitous IoT, hyper-automation, deterministic experience, network security as a service, and hyper-converged data center. Based on the challenges brought by service changes to networks and intergenerational changes of network technologies, this document provides suggestions on building networks oriented to the digital era.

In addition, this document outlines the future development of data communication networks on their journey to the Net5.5G era. This helps enterprises quickly adapt to industry trends and changes, streamline data sharing channels inside and outside organizations through digital means, implement data sharing and integration, and efficiently mine data value to take the lead in the ever-changing market.

**Kevin Hu**  
**President of Huawei's Data Communication**  
**Product Line**



## Executive Summary

01

## Trend 1

04

Flexible Multi-Cloud Networks Become the Key to Enterprise IT Cloudification Success

## Trend 2

12

IoT Evolves from Simple Services Oriented to Lightweight Data Collection to Complex Services Featuring High-Density Collection + Control Collaboration

## Trend 3

21

Cloud-based Network Security Service Solutions Become Increasingly Mature

## Trend 4

28

Data Center Networks Are Evolving to All-Ethernet

## Trend 5

36

AI-based Hyper-Automation Is Changing the Network Management Mode

## Trend 6

44

Industrial Networks Are Moving Towards IT/OT Convergence, Enabling Intelligent Industrial Upgrade

## Prospects

49

Striding Towards Net5.5G Together, Connecting Ubiquitous Computing Power and Intelligent Living

# Executive Summary

## 1 Multi-Cloud Network

A growing number of enterprises are further integrating cloud computing into their operations as the value of the technology becomes ever more apparent. As digital transformation gains momentum, many enterprises choose to incorporate the multi-cloud strategy into their long-term plans and hope to maximize the value of cloud services through multi-cloud resource collaboration. However, there is a disparity between the technology stacks and management tools provided by different cloud service providers, and enterprises lack unified heterogeneous multi-cloud management capabilities. This means that multi-cloud adoption aggravates the silos between enterprise networks, lowers the operational efficiency of IT teams, and hampers efficient collaboration among multi-cloud resources.

To address these issues, enterprises can adopt a hierarchical network architecture to overcome differences between heterogeneous networks in the upward direction and provide O&M of physical network connections in the downward direction. This architecture enables networks to provide seamless connections and service assurance between clouds, as well as between devices deployed on and off the clouds from the service perspective. Doing so unifies operations, unifies resource scheduling, and unifies service quality assurance for multi-cloud networks.

## 2 IoT

IoT is an important connector between the digital and physical worlds and is needed for enterprises to collect data. Driven by technological development and a maturing ecosystem, IoT now not only offers lightweight data collection for simple services, but also high-density data collection and control collaboration for complex services. However, traditional IoT systems are constructed independently, resulting in communication interfaces and protocols of IoT terminals varying from vendor to vendor. Plus, IT and OT networks are separated, preventing data from being exchanged between systems, which in turn hinders effective collaboration.

Against this backdrop, it is vital to unify IoT technologies, enable communication between different IoT systems, and achieve ubiquitous connectivity and efficient communication for digital information, all with the goal of maximizing the value of data.

## 3 Network Security

The multi-cloud strategy and large-scale IoT application are reshaping the scope of enterprise networks and further expanding the boundaries of network security. Traditionally, security products are deployed locally for network protection, falling short of meeting enterprises' network security requirements in the digital era.

Network security protection is a contest between a myriad of attack and defense techniques. To have a plurality of defense techniques, enterprises or organizations must understand attacks in all phases of their lifecycle, evaluate attack techniques in each phase of attack, and formulate defense measures accordingly. Nowadays, enterprises are raising higher requirements on network security, and manageable security service modes are becoming increasingly mature. Against this backdrop, the traditional O&M mode of "security products + local onsite O&M" has shifted to the cloud service-based mode, and providing network security protection capabilities in the form of cloud delivery is becoming a common choice for network security investment. In addition, the increasing popularity of cloud services makes enterprises more willing to embrace security solutions delivered in the cloud.

#### **4 All-Ethernet Data Center Network**

Data centers, as the rendezvous points of computing power and data, play a pivotal role for traffic and services in the digital economy era. Traditional data center networks include general-purpose Ethernet networks, centralized storage-oriented fiber channel (FC) networks, and high-performance-computing-oriented InfiniBand networks. As global data centers continue to expand in scale, the traffic and service complexity of data center networks also increases, complicating network management and operations.

The all-Ethernet reconstruction of data center networks enables general-purpose computing, storage, and high-performance computing networks to be carried on the open and standard Ethernet technology stack. Unifying networking protocols and using a mix of TCP and RoCE data flows for transmission help overcome the limitations of traditional distributed architecture. In addition, automation is achieved throughout the lifecycle based on big data, AI, and other means. These meet future data centers' service requirements for ultra-high computing power and ultra-large data throughput (400G/800G).

#### **5 Network O&M**

Driven by new technologies such as mobility, big data, cloud computing, and AI, the number of NEs, technology stacks, and services involved in enterprise IT architecture has increased exponentially, yet the workforce of enterprise O&M department remains unchanged. This puts great pressure on network O&M. Traditional device-centric O&M cannot meet the service agility requirements of the digital era. Enterprises urgently need to go digital and intelligent and replace manual labor with machines.

With data processing capabilities on edge network devices, enterprises can use a myriad of distributed nodes to process and analyze data, eliminating the need to send a large amount of data to the management and control center and thereby saving computing resources. In addition, technologies such as big data and AI help enterprises achieve network-wide intelligent traffic optimization and prediction.

## 6 Advanced Industrial Network

Data is essential to the industrial Internet, and data collection therefore plays a pivotal role. Currently, the online rate of industrial terminals is still low, and a large amount of data is accumulated on siloed networks. Bringing industrial devices online enables these devices to communicate with industrial application systems for data collection or control through the enterprise intranet or extranet.

Networks are the basis of the industrial Internet and the foundation for collecting data needed by Man, Machine, Material, Method, Environment, and Measurement (5M1E) analysis and device interconnection. They allow enterprises to build advanced industrial networks for intelligent connectivity of everything and facilitate data and computing power access. IP-based industrial networks are the basis for end-to-end communication and convergence of IT and OT networks.

## 7 Net5.5G

Clearly, future networks promise tremendous potential and uncertainties. The entire industry needs to work together to explore these new technologies, move towards Net5.5G, build ubiquitous intelligent IP networks, and connect ubiquitous computing power and smart terminals.



# 01

## **Flexible Multi-Cloud Networks Become the Key to Enterprise IT Cloudification Success**







## Trend

As enterprises cope with increasingly complex internal and external environment changes, customer requirements, and new service scenarios, they are being driven by factors such as diversification, personalization, and efficiency to select digital products with low costs, high agility and elasticity, and strong support for service and technology innovation. As the cloud computing industry matures, most enterprises choose to incorporate the multi-cloud strategy into their long-term plans. Against this backdrop, more and more IT departments are adopting public clouds and on-premises private clouds. According to *Flexera 2021 State of the Cloud Report*, 92% of surveyed

enterprises around the world have adopted the multi-cloud strategy. These enterprises each use 5.3 clouds on average, while 82% use hybrid clouds. However, the transformation of large-scale enterprise applications from the hybrid-cloud architecture to the multi-cloud architecture is not as simple as expected. The key capability of the multi-cloud architecture is heterogeneous multi-cloud management, and the biggest challenge facing this architecture is network interconnection management between clouds. The multi-cloud-native network architecture must meet the usability, reliability, and security requirements in multi-cloud environments.

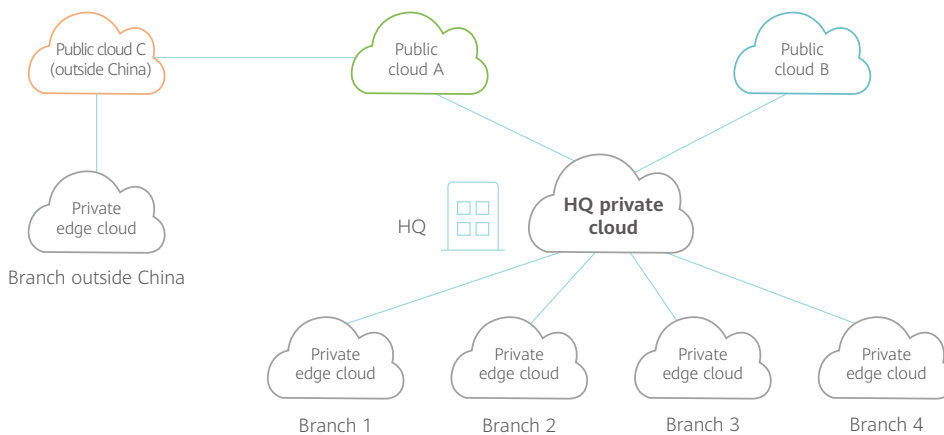


Figure 1-1 Typical multi-cloud networking of an enterprise



## Challenges

### Network Issues Brought by Multi-Cloud Deployment

**1. Fragmented networks lead to poor service experience.** The multi-cloud architecture replaces the classic LAN/DCN/WAN architecture as well as related knowledge and experience, and introduces virtual networks between different clouds. However, different cloud service providers provide varying virtual network technology stacks, such as VXLAN, GRE, and L2TP. As a result, cross-cloud network management requires multiple tools and protocols. The existing IT system cannot unify the management, configuration, monitoring, and O&M for different networks. If complaints are made about service experience, IT system engineers have to work long hours to locate the root causes on siloed networks.



- 2. The network operational efficiency is threatened.** Nowadays, clouds are typically interconnected through cloud APIs. These APIs and related parameters, however, vary greatly from cloud to cloud, making it difficult for enterprises to use unified interfaces for cloud interconnection. This results in a steep learning curve for IT teams as they have to understand the characteristics of multi-cloud networks before determining their own solutions. What's worse, they have to frequently upgrade their IT systems in line with the technical changes from cloud service providers. These challenges drive up IT operational costs.
- 3. Network security and compliance are more complex.** Adopting multiple clouds increases the exposure surface and, as a result, the attack surface. It also makes centralized access control and permission management impossible. As such, heavier data governance tasks are required to prevent data leakage and abuse. Enterprises need to ensure that traditional security policies and customized security architectures hosted by private clouds are inherited and implemented in a unified manner across these clouds.
- 4. Network connection costs rise constantly.** As data flows expand from on-premises private IT infrastructure to multiple clouds, it is imperative to establish long-distance and high-bandwidth network connections. Relying solely on carriers' private lines significantly drives up transmission costs. Enterprises urgently need to make full use of the higher Internet bandwidth at lower costs.



## Recommendations

### Hierarchize the Network Architecture and Overcome Operational Differences of Networks for Different Clouds to Unify Network Operations

1. **Hierarchize network connections:** Divide the network into the heterogeneous infrastructure network layer, multi-cloud virtual network layer, and tenant-perspective service connection layer. This helps to provide OAM of physical network connections in the downward direction and overcomes the implementation differences between heterogeneous networks in the upward direction. The latter enables the network to provide seamless network connections and service assurance between clouds, as well as between devices deployed on and off the cloud from the service perspective.
2. **Unify network operations:** Overcome the operational differences of networks for different clouds. Provide unified and full-lifecycle network orchestration and policy management for clouds and sites, fault recovery and high availability, and visualized monitoring of configurations and running status. Further to this, implement on-demand automated provisioning of inter-cloud connections, bandwidth, and applications based on service intents.
3. **Provide security anywhere:** Provide cloud-native SD-WAN/SASE capabilities and unified identity, analysis, and security policies. Incorporate security into the network architecture to provide security control for E2E data flow behavior.

#### 4. Efficiently utilize network resources:

Optimize inter-cloud resource scheduling to ensure service experience and maximize resource utilization. Also, visualize costs through refined service quality awareness, full-dimensional fine-grained telemetry, and real-time awareness in collaboration with the controller.

#### 5. Provide quality assurance for service applications:

Identify applications and data flows and provide differentiated network services based on applications. These services include data acceleration, deterministic lossless experience assurance, fast resource call, application traffic governance, and high network/application/data reliability.

#### 6. Provide open and easy operations:

Provide multi-tenant services, application-level single-flow operations, open hierarchical network services, and intelligent recommendations.



## Solution

### Huawei's iMaster NCE-Fabric Solution for Hybrid Clouds

To enable flexible multi-cloud network orchestration and ensure security compliance, Huawei launched the iMaster NCE-Fabric Solution for Hybrid Clouds, which can be logically divided into the following layers: service orchestration layer, control layer, and infrastructure layer.

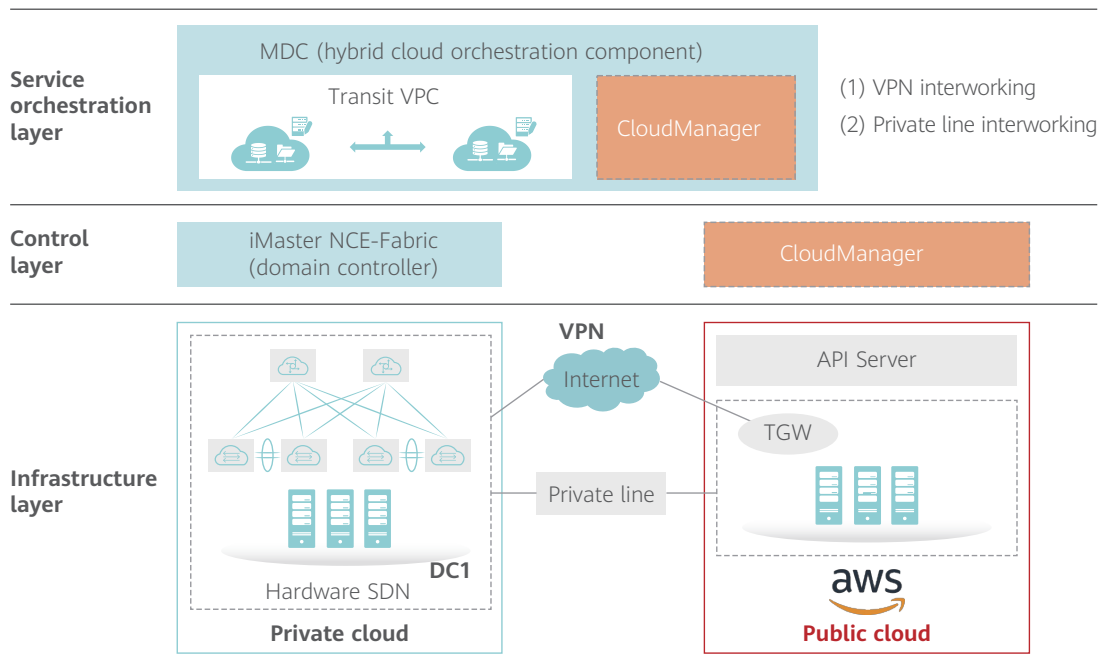


Figure 1-2 Layers of Huawei's iMaster NCE-Fabric Solution for Hybrid Clouds

**1. Service orchestration layer:** The Multi-Datacenter Controller (MDC) is a hybrid cloud orchestration component that overcomes the differences and complexity between heterogeneous clouds. It enables service departments to focus on service system connectivity as well as service interworking, network orchestration, security isolation, and compliance requirements of public and private clouds.

- MDC: implements cross-fabric service orchestration of private clouds, service orchestration between private and public clouds, and flexible security policy control.

**2. Control layer:** orchestrates intra-domain networks of public and private clouds, automatically delivers configurations, and performs unified O&M.

- iMaster NCE-Fabric: private cloud domain controller. In the southbound direction, it manages physical devices in a single

or multiple fabrics on the private cloud, and orchestrates and delivers the logical network in a fabric.

- CloudManager: orchestrates the public cloud network. It remotely invokes open APIs of the public cloud in the southbound direction to deliver configurations to the public cloud network.

**3. Infrastructure layer:** includes one or more intra-cloud networks, provides overlay gateways for communication between heterogeneous clouds, and connects to the public cloud through private lines or VPNs.



## Customer Benefits

The iMaster NCE-Fabric Solution for Hybrid Clouds provides the following benefits:

- 1. Simple deployment:** In the private cloud, public cloud APIs are remotely invoked to provision configurations and monitor the status of the public cloud. In this case, there is no need to deploy cloud-based controllers or virtualized NEs in the public cloud or create separate public cloud management accounts. This decouples the networking architecture for multiple clouds and minimizes public cloud usage costs.
- 2. Flexible orchestration:** The unified orchestration UI for interworking between public and private clouds enables logical network orchestration through simple drag-and-drop operations and a visualized logical topology. This single-pane-of-glass interface eliminates the need to switch between orchestration pages, improving orchestration efficiency.
- 3. Network visualization:** The logical topology is restored based on public cloud network configurations that have been delivered. This visualizes the public cloud

network topology, giving you a clear view of the association between network resource objects.

 **Solution**

**Huawei's SD-WAN Solution with Multi-Cloud Enhancement**

Huawei has launched the SD-WAN Solution with Multi-Cloud Enhancement to meet enterprise requirements for all-scenario on-demand interconnection between branches, between branches and data centers, and between branches and clouds. The solution implements application-level intelligent traffic steering, intelligent acceleration, and intelligent O&M, providing better service experience and reshaping the full-process service experience for enterprise WAN interconnection. Huawei's SD-WAN Solution with Multi-Cloud Enhancement consists of the network layer and management layer.

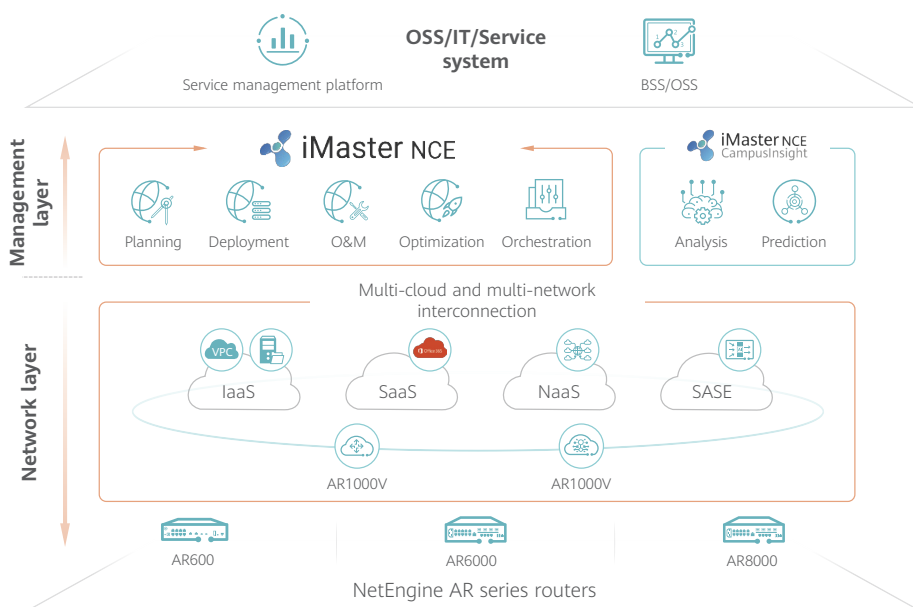


Figure 1-3 Layers of Huawei's SD-WAN Solution with Multi-Cloud Enhancement

## 1. Network layer

- Provides multiple wired and wireless interfaces and supports various networking models.
- Supports multi-tenancy and isolation of management and data planes.
- Provides cloud-native SASE capabilities and supports virtual gateway deployment on multiple clouds.
- Supports physical CPEs and vCPEs.

## 2. Management layer

- iMaster NCE controller: manages network devices in a centralized and automated manner. It uses NETCONF/YANG in the southbound direction to manage RRs/CPEs, and provides standard RESTful interfaces in the northbound direction to interconnect with third-party applications and cloud platforms.
- iMaster NCE CampusInsight: collects network indicators and uses machine learning technologies for fault locating and intelligent optimization.

solution can be deployed on many popular public clouds, such as Huawei Cloud, Alibaba Cloud, Tencent Cloud, AWS, e-Cloud, and Microsoft Azure, to implement interconnection between on-premises and public clouds, unified management, and unified policy orchestration.

**2. Intelligent traffic steering:** Optimal paths are selected based on factors such as the application SLA, application priority, and bandwidth utilization to ensure that key applications are running on the optimal link. The industry's first built-in A-FEC quality awareness ensures lossless experience of audio and video applications even at a 30% packet loss rate.

**3. Excellent performance:** Up to 10 Gbps SD-WAN performance is supported, meeting high-performance hub and IWG deployment requirements. Meanwhile, 5G mobile network uplinks and per-packet/per-flow load balancing are supported, improving network reliability.

**4. Expanded security:** Built-in Layer-7 application identification and control, firewall, IPS, URL filtering, and antivirus features are supported. Unified security policies for enterprise cloud migration are implemented without the need of additional devices. Advanced security functions, such as threat awareness, malicious file identification, and attack defense are supported.

**5. Intelligent O&M:** Powered by intelligent and big data analytics technologies, iMaster NCE uses telemetry technology to collect network data in real time, and uses big data analytics and machine learning algorithms to learn network behaviors and identify faults. It proactively discovers 85% of potential network faults and provides intelligent root



## Customer Benefits

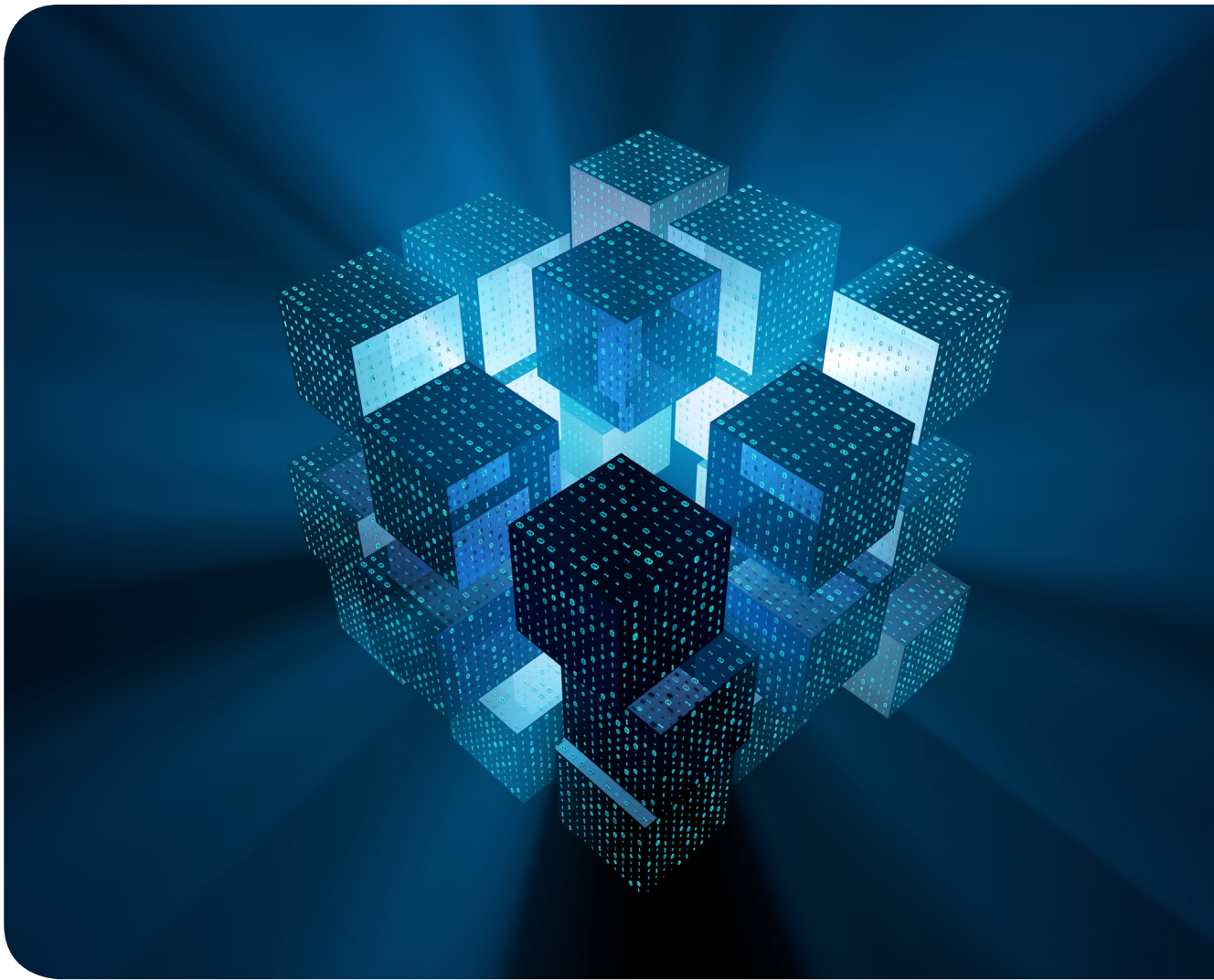
Huawei's SD-WAN Solution with Multi-Cloud Enhancement provides the following benefits:

**1. One network across multiple clouds:** Multiple networking models are supported to meet different branch network requirements. The

cause analysis for superb network service experience.

Huawei's SD-WAN Solution with Multi-Cloud Enhancement provides powerful networking, high-quality experience, and easy O&M capabilities to meet the multi-cloud interconnection requirements of small-, medium-, large-, and even ultra-large-sized enterprises, carriers, and service providers. Huawei's SD-WAN products have been serving more than 50,000 customers worldwide, and

Huawei's SD-WAN Solution received Gartner Peer Insights Customers' Choice distinction in 2021. The solution provides enterprises with high-quality cloud migration experience while improving the reliability, flexibility, and O&M efficiency of enterprise branch networks. It also makes sure branch networks are always online and ensures service continuity and stability.



# 02

**IoT Evolves from  
Simple Services Oriented  
to Lightweight Data  
Collection to Complex  
Services Featuring  
High-Density Collection +  
Control Collaboration**







## Trend

Amid the current digitalization wave, enterprises often suffer from a lack of entity-based real data, insufficient digital contacts, and failures to build in the digital space a digital twin system that accurately maps to entities. IoT is the foundation for the digital and intelligent transformation of any physical device. GSMA predicts that, by 2025, there will be 24.6 billion IoT connections worldwide, with a compound annual growth rate (CAGR) of 13%. Meanwhile, industrial IoT devices will outnumber consumer IoT devices by 2024. With the help of IoT, enterprises can obtain more data to improve production efficiency. And with the maturity of 5G and Wi-Fi 6E technologies and ecosystems, IoT is shifting from simple services focused on lightweight data collection to complex services featuring high-density collection and control collaboration. In addition to meeting the requirements of common scenarios such as retail and education, IoT has gradually extended to production scenarios such as smart manufacturing, power control, and ports, which pose higher requirements on connections. The major changes are as follows:

**1. Industry 4.0 is increasingly dependent on IoT.** Without IoT, it would not be possible

to provide large-scale data collection and monitoring required for improving industrial capabilities. For example, a large automobile factory deployed a large number of robots and AGVs, as well as connecting more than 20,000 cameras, meters, and sensors through the big data platform to monitor and analyze the production process in real time. To ensure a highly intelligent, flexible, and transparent production process, production elements require real-time synchronization and interaction as well as connections with 99.999% reliability and millisecond-level latency. In addition, complex factory environments have higher requirements on the anti-interference positioning technologies for terminals.

**2. Internet of Medical Things (IoMT) continues to develop.**

The IoMT connects patients, medical personnel, medical institutions, and medical devices to enable standardized collection and analysis of patient and device data, medical waste tracking, high-value asset stocktaking, wristband patient monitoring, infusion monitoring, medical consumable tracking, and positioning of apparatuses such as wheelchairs. For example, in a large hospital, 150,000 low-

power medical apparatuses, of more than 400 types, are connected to the IoMT. Real-time display of their track and status information significantly improves medical efficiency.

**3. Smart cities are constructed on a large scale.** Using city IoT as their foundation, smart cities adopt AI technologies to improve city management. Generally, a city IoT involves millions of terminals. In the first phase of the Shanghai IoT center, for example, nearly 100 types of facilities, totaling 5.1 million and spreading over seven districts, connect to the IoT. What's more, over 34 million data records are generated every day. In the future, the number of sensing terminals will increase to tens of millions. In complex smart city scenarios, especially reservoir, meteorology, and electric power scenarios, low-power data backhaul without Internet access and power supply is a must-have.



## Challenges

### Challenges Facing Enterprises in IoT Deployment

**1. Low terminal online rate:** Connectivity is the first step to achieving industry digitalization. Currently, there are many legacy terminals, especially in the production and manufacturing fields, where the terminal online rate is only 20%. And this terminal online rate gets even lower for terminals closer to endpoints. The low digitalization level directly leads to difficult data collection, high costs, and low efficiency.

**2. Difficult data interaction:** Traditional IoT systems are constructed independently, resulting in communication interfaces and protocols of IoT terminals varying from vendor to vendor. Most subsystems use non-IP cabling and require protocol conversion for data interaction. The IT and OT networks are separated, preventing data from being transmitted between systems, which in turn hinders effective collaboration. Against this backdrop, it is vital to eradicate IoT information silos in order to enable communication based on semantics, data sharing, and collaboration between IoT terminals, thereby maximizing data value.

**3. Complex deployment and commissioning:** Each scenario has its own requirements on sensors in terms of sensing technologies, environment adaptability, and communication technologies. After going online, most IoT terminals need to communicate with the IT network to transmit data to the big data platform for unified processing. In some scenarios, trenches need to be dug to deploy IoT terminals. The resulting long installation duration, complex deployment and commissioning, and high construction requirements significantly drive up costs.

**4. Difficult network O&M:** IoT is typified by large numbers of terminals, complex connections, wide coverage, and scattered locations. In addition, a large number of sensors are dumb terminals. This means that once a fault occurs, the troubleshooting workload is heavy, efficiency is low, and fault recovery time is long. As such, ultra-large networks urgently require intelligent and efficient O&M and optimized connection experience.

**5. Low security and reliability:** IoT terminals are widely dispersed, and some terminals (especially dumb terminals) have minimal

security protection capabilities. This makes the IoT vulnerable to network intrusions and attacks. As the IoT expands in scale, it needs to meet increasingly higher security requirements for behavior identification to prevent terminal spoofing and guarantee secure access.



## Recommendations

### **Provide Simpler Networking and Communication, More Secure Access and Control, and More Intelligent Edge Computing to Achieve Ubiquitous Connectivity and Efficient Communication for Digital Information**

**1. Unify access technologies.** Unify different connection modes through technical redesign to change the current situation featuring independent networking of isolated systems and avoid the large-scale use of various proprietary protocols on the network.

- Use Ethernet for all wired access scenarios to reduce cabling costs. There are various types of cables in the IoT market, such as RS232, RS485, RJ45, USB, and CAN. By replacing different interface types with Ethernet, O&M efficiency can be improved for enterprise networks. The Ethernet network supports multiple connection modes, such as P2P and P2MP, and provides high-bandwidth transmission at multiple rates, such as 10 Mbps, 100 Mbps, and 1 Gbps. On top

of this, the Ethernet network can supply power to terminals through twisted pairs, reducing cable deployment costs and cabling complexity.

- Wireless access revolves around Wi-Fi and integrates multiple technologies. In particular, the mature and popular Wi-Fi 6 technology boasts a wide array of advantages. In scenarios where reconstruction or capacity expansion is difficult, Wi-Fi 6 can provide Mbps or higher bandwidth for a single terminal (such as a video terminal). In new network deployment scenarios, Wi-Fi 6 can be deployed for devices that require elastic capacity expansion. In addition to facilitating capacity expansion, Wi-Fi 6 also supports the mobility required by IoT terminals, such as office terminals in conference rooms and robots for food delivery or security protection.

- Replace disparate IoT protocols with IP to enable unified communication. IP-based physical connections, such as Wi-Fi connections, simplify network deployment, enabling plug-and-play of IoT terminals. They provide a unified communication basis for IoT protocols to enable IoT data communication. In addition, IP-incapable terminals can integrate the lightweight IP protocol stack into their operating systems through SDKs. IPv6 technology provides sufficient addresses for massive connections, laying the foundation for all-IP networks.

**2. Deploy intelligent edge gateways.** IoT generates massive amounts of data, which needs to be processed and analyzed. Edge gateways can move computing services closer to end users or data sources. Edge

gateways are deployed at the edge of a network, and connect the physical and digital worlds through functions such as network interconnection and protocol conversion. They allow data to be initially processed, such as being cleaned, converted, compressed, and extracted, close to where the data is obtained. Edge gateways bridge the edge and cloud through remote terminal units (RTUs) or programmable logic controllers (PLCs).

- Local processing: IoT requires computing to be carried out closer to physical devices or data sources. To quickly analyze data generated by IoT sensors and devices and thereby accelerate response or problem solving, data needs to be analyzed at the edge instead of being sent to the central site for analysis.
- Open container: Edge gateways provide standard open APIs to connect to the enterprise IoT platform for real-time deployment and provisioning of IoT applications. They can load applications of various industries for terminal collaboration based on the open container platform.

**3. Deploy a centralized management and control platform.** After an IoT is deployed, the network running status is visible only on dedicated tools such as the network management platform. This makes it difficult for decision makers to have an intuitive view of the overall running status, affecting capacity expansion decision-making and support for major events. These difficulties make it particularly important to set up a management channel between the backhaul network and IoT. This is where a centralized management and control platform comes in.

It supports data standardization, connection management, and centralized O&M. In addition, the northbound interface of the platform connects to the intelligent operation center (IOC) to show the running status of the backhaul network and IoT, including the bandwidth usage, the number of terminals, and the online status of terminals. This centralized management and control platform consists of two components:

- Network management: supports a myriad of functions, such as network service management, network security management, user access management, network monitoring, network quality analysis, network application analysis, alarms, and reports. Besides these, it is capable of big data analytics and provides open standard interfaces for connecting to the IOC.
- IoT management: registers and manages terminal types, running protocols, terminal IDs, and terminal MAC addresses. In addition, it processes, stores, and converts data sent by IoT terminals, as well as providing standard interfaces for connecting to the upper-layer IOC or applications.

**4. Improve security based on AI.** Manually managing vast numbers of IoT terminals is complex and results in high management costs, while existing IoT systems are not easy to configure or operate. Making matters worse, terminal security awareness of users is usually insufficient. In response to these challenges, AI and machine learning technologies can be leveraged to improve security capabilities in terms of massive access and unified management and control.

- **Secure access:** An AI-empowered IoT system can defend against spoofing or unauthorized access of IoT terminals. Smart terminals can use built-in security SDKs and secondary authentication for secure access. Dumb terminals, which lack authentication capabilities, need to extract terminal traffic characteristics to identify terminal types, vendors, and SNs. Then, only terminals matching specified service types are allowed to access the network. In terms of asset identification, the IoT system intelligently identifies unknown assets and categories through passive traffic listening. It also adaptively scans and identifies specific assets. The unsupervised clustering algorithm based on group relationships enables the system to discover multiple types of unknown terminals before classifying them, improving the accuracy of security access management.
- **Security management:** IoT firewalls, sandboxes, and probes are deployed to analyze abnormal or malformed attack packets and application-layer malicious threat traffic on the entire IoT network in real time. These security devices then send such IoT traffic to the security situational awareness system for real-time security situational awareness of the entire network. In addition, unsupervised learning is introduced to analyze traffic, intelligently identify abnormal behavior, and use the self-learning behavior identification model for behavior restoration. This helps to detect spoofing, unauthorized, and hijacked terminals, which in turn accelerates unknown threat diagnosis and proactively blocks spoofed, hijacked, and virus-infected terminals.





## Huawei's Intelligent IoT Sensing Network Solution

The following figure shows the overall architecture of the intelligent IoT sensing network, which consists of four layers: device, edge, pipe, and cloud.

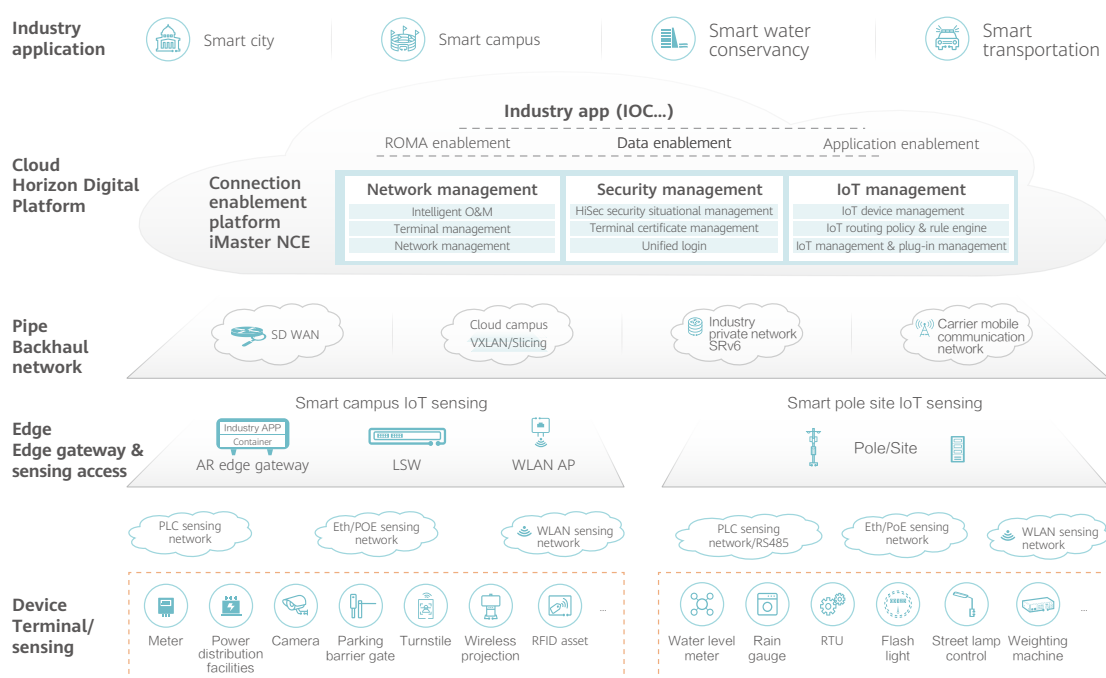


Figure 1-4 Overall architecture of Huawei's Intelligent IoT Sensing Network Solution

**1. IoT terminal layer:** end sensor of the IoT sensing network, bridging the physical and the digital worlds. Two types of terminals are available, each differing in the application scenario:

- Indoor: IoT sensing terminals for smart campuses
- Outdoor: IoT sensing terminals for smart pole sites

**2. Edge gateway & sensing access layer:** "nerve

ending" of the IoT sensing network and also the key to determining the solution usability.

- Connects to the OT network (supports operation instruction communication between IoT terminals), providing reliable connection and local service survival.
- Connects to the CT network (supports IT application data communication), providing good security, maintainability, and manageability.

**3. Backhaul network layer:** "neural network" of the IoT sensing network, ensuring efficient, reliable, and secure IoT data transmission.

- Campus intranet: VXLAN technology allows multiple services to be carried on a single network. Different services are divided into different virtual subnets for service isolation and security.
- WAN backhaul network: SD-WAN can be used to optimize investment efficiency. Important services can be transmitted through private networks, and less important services can be backhauled through public networks.
- IoT security: Security firewalls are deployed to identify abnormal traffic, as well as defend against malformed packets and encrypted traffic.

**4. Cloud platform layer:** "nerve center" of the IoT sensing network, implementing basic functions such as network management, security management, and IoT management. This layer can manage network devices as well as centrally manage and control IoT terminals and services. With its open standard interfaces, the layer also supports interconnection with the IOC.

- Network management: includes intelligent O&M, terminal management, and network management.
- Security management: includes HiSec security situational management, terminal certificate management, and unified login.
- IoT management: includes IoT terminal management, IoT routing & rule engine, IoT model management, and plug-in management.



## Customer Benefits

Huawei's Intelligent IoT Sensing Network Solution brings the following benefits:

- 1. Seamless access:** The solution implements IP-based Wi-Fi 6 wireless access and PLC-IoT access to reduce cables by more than 40%. Seamless access technology is used for automatic guidance, eliminating the need for complex onsite configuration and implementing automatic network access of various terminals. In this manner, IoT terminals can communicate with each other as soon as they access the network.
- 2. Simple deployment:** Huawei Wi-Fi 6 APs can provide IoT slots to work with IoT expansion modules and implement IoT functions such as Bluetooth, RFID, ZigBee, and UWB. These APs are ideal for various fields such as enterprise asset management, electronic shelf label (ESL), city intelligent environment control, and industry high-precision positioning. In addition, they also leverage technologies such as multi-network integration deployment and intelligent interference avoidance to improve network utilization and reduce TCO by 50%.
- 3. One-hop cloud access:** The edge IoT gateway standardizes various heterogeneous IoT protocols and converts data into languages that can be understood by cloud applications. This ensures that IoT terminals can communicate with cloud applications as soon as they connect to the edge IoT gateway, achieving one-hop access to the cloud.
- 4. One-network wide visualization:** Through standard interfaces, the enablement platform automatically collects the topology and status

data. It then generates the topology and association between the backhaul network and IoT terminals through association calculation. All these enable the IOC to detect and display network-wide connections and IoT terminals, including the network-wide topology, network quality, terminal status, and alarm information.

- 5. One-stop integrated security:** Secondary authentication or fingerprint recognition is used to prevent IoT terminals from spoofing and ensure their access security. For secure communication of IoT terminals, network devices can identify IoT protocols, implement protocol security, and encrypt data before transmission. This prevents IoT data flows from being stolen, tampered with, and replayed. In addition, the solution supports AI-based network-wide security situational awareness

and analysis, blocks malicious traffic in real time, and isolates terminals with security threats, ultimately implementing security management and control of IoT terminals.

The Intelligent IoT Sensing Network Solution focuses on IoT networks closely related to industries and user services to provide an intelligent, convenient, and reliable ICT solution. It aims to build intelligent and open networks and platforms, as well as provide an open ecosystem for a myriad of industries. In this way, service systems, and upper-layer applications in each industry can be deployed on the IoT network in a fast and simplified manner.





# 03

**Cloud-based  
Network Security Service  
Solutions Become  
Increasingly Mature**





## Trend

As enterprises go digital and move to the cloud, network security has become one of the most crucial parts of any enterprise. In the past, it was a common practice for enterprises to implement onsite deployment of multiple security products for network protection, such as firewalls, intrusion prevention systems (IPS), sandboxes, vulnerability scan devices, and situational awareness systems. However, due to the shortage of professional security personnel, many enterprises are unable to take full advantage of these security products to achieve sound security protection. After some security products go live, security alarms go unnoticed, security protection policies go unchanged, and threat databases and protection methods are outdated. Consequently, the security protection is inadequate. Nowadays, multi-cloud, IoT, and remote office are on the rise, and network security boundaries keep expanding. This leads to increasingly rampant and targeted ransomware. Adopting more complex policies, ransomware attacks lead to frequent security incidents such as data breaches. Taking this into account, traditional security monitoring, detection, and response methods require significant changes to address the risks posed by new technologies

and business plans.



## Challenges

### Challenges Facing Enterprises in Traditional Network Security Deployment

#### 1. High network security construction costs:

At first glance, network security appears to be a game between an attacker and defender. In actual fact, it is a contest between myriad attack and defense techniques. This means that to have a plurality of defense techniques, enterprises or organizations must understand each stage of attacks, evaluate the attack techniques in the next stage based on each attack stage, and formulate defense measures accordingly. So, in the pursuit of more effective defense, enterprises invest heavily to build their own network security systems. This includes investing in firewalls, intrusion detection systems, tamper-proof systems, antivirus

software, and network behavior management systems. All these incur high costs. And the reality is that larger investment does not necessarily mean a more secure and robust network.

**2. Poor network security defense:** In conventional security solutions, valid and urgent security events usually cannot be effectively distinguished among a large number of security event logs reported. Security products work separately, and threat analysis is one-sided, failing to provide global overall analysis. As a result, threats cannot be accurately identified or handled in a timely manner. Worse still, threat databases are not promptly updated on network security protection devices, which adversely affects the service capability and analysis accuracy. Facing a host of new unknown threats, conventional security solutions cannot provide adequate network defense.

**3. Network security work that needs to be carried out constantly:** From the perspective of network threats' lifecycle, security threat events occur erratically and do not have obvious burst characteristics. Even if security devices are deployed, without professional security management processes and security event warning mechanisms, security O&M personnel are incapable of monitoring the internal network security status 24/7 and are therefore unable to respond in a timely manner.

**4. Insufficient capabilities of security personnel:** Traditional network security services are implemented primarily by people. This makes them a kind of asset-heavy operation and places high requirements on the capabilities of network security maintenance personnel. In practice, it is difficult for an enterprise or

organization that does not focus on network security to develop high-level talents in the network security field. And for some small- and medium-sized enterprises (SMEs), the cost of hiring professional security personnel is too high. As a result, most SMEs are weak when it comes to security management and hence cannot effectively handle security incidents.



## Recommendations

### Enterprises Combine Local Security Capabilities with Network Security Cloud Services to Improve Security Detection, Analysis, and Response Capabilities and Enhance Security Operations Through Continuous Attack-Defense Confrontation

Enterprises are raising higher requirements on network security, while manageable security service modes are becoming increasingly mature. Against this backdrop, the traditional O&M mode of "security products + local onsite O&M" has shifted to the cloud service-based mode, and providing network security protection capabilities in the form of cloud delivery is becoming a common choice for network security investment. In addition, the increasing popularity of cloud services makes enterprises more willing to embrace security solutions delivered in the cloud. According to Gartner, by 2024, 90% of hosting security service providers will give up building their own security platforms and instead opt for SaaS-based commercial solutions.

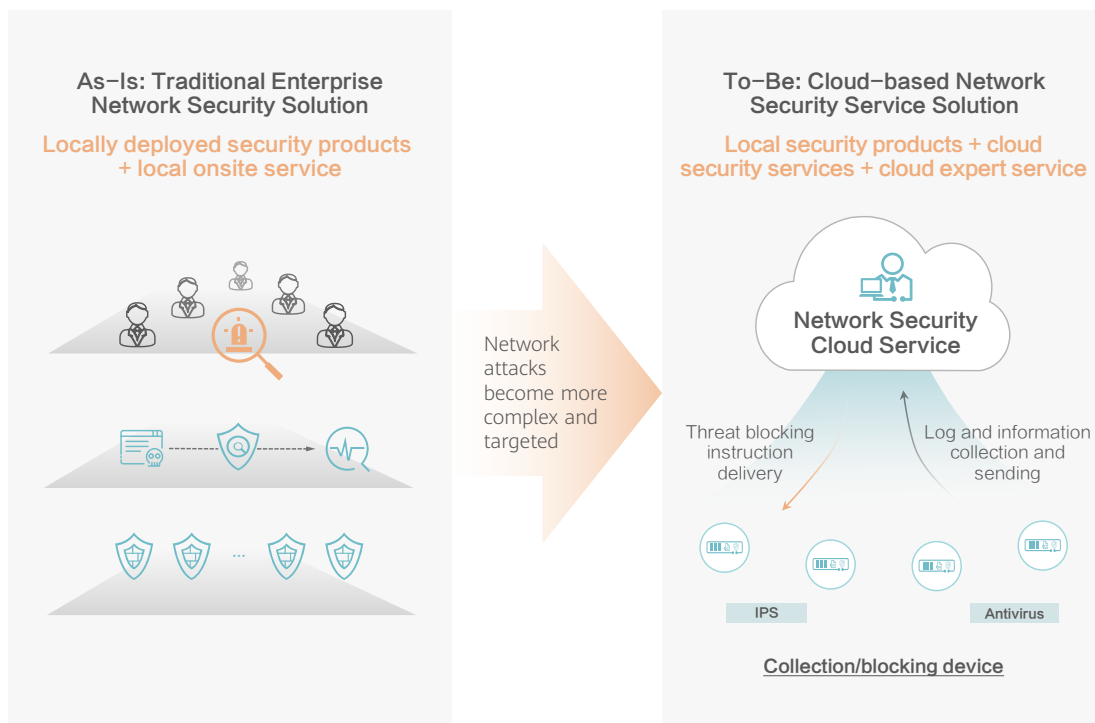


Figure 1-5 Evolution of network security services

With cloud-based network security services, enterprises can obtain real-time, intelligent, and accurate protection capabilities through on-demand subscriptions. This accelerates network security deployment and reduces complexity of local security devices. It also slashes costs related to large-scale security deployment, including operational costs and related IT resources. All these merits help enterprises address the contradiction between the increasingly complex threat environment and the lack of skilled network security personnel. What's more, enterprises can connect existing network devices, including routers, firewalls, or SD-WAN devices, to a cloud-delivered security platform on which policies are globally applied. This can help to ensure consistent security and seamless user experience.

Intelligent security analysis and automatic handling algorithms are used to improve security

analysis efficiency and provide customers with efficient and intelligent security managed services. They can also be used to solve the fundamental problem that some customers lack a proper understanding of network security. A large amount of customer sample data helps continuously improve service capabilities and analysis accuracy, thus reducing the overall false positive rate of security devices. Cloud services offer security consulting, security tool services, cloud experts, and self-developed tool sharing for customers who are capable of security O&M, improving user experience. The security platform continuously evolves to provide more security capabilities. Customers can subscribe to such security capabilities on demand based on actual network security construction requirements in multiple scenarios.



## Huawei's Qiankun Security CloudService Solution

Huawei's Qiankun Security CloudService Solution consists of the Huawei Qiankun Security CloudService platform, which is deployed on HUAWEI CLOUD, and Huawei TianGuan protection nodes, which are deployed on the customer's local network. The solution implements collaboration between cloud services and local devices to build a simple, efficient, and easy-to-use security cloud service solution.

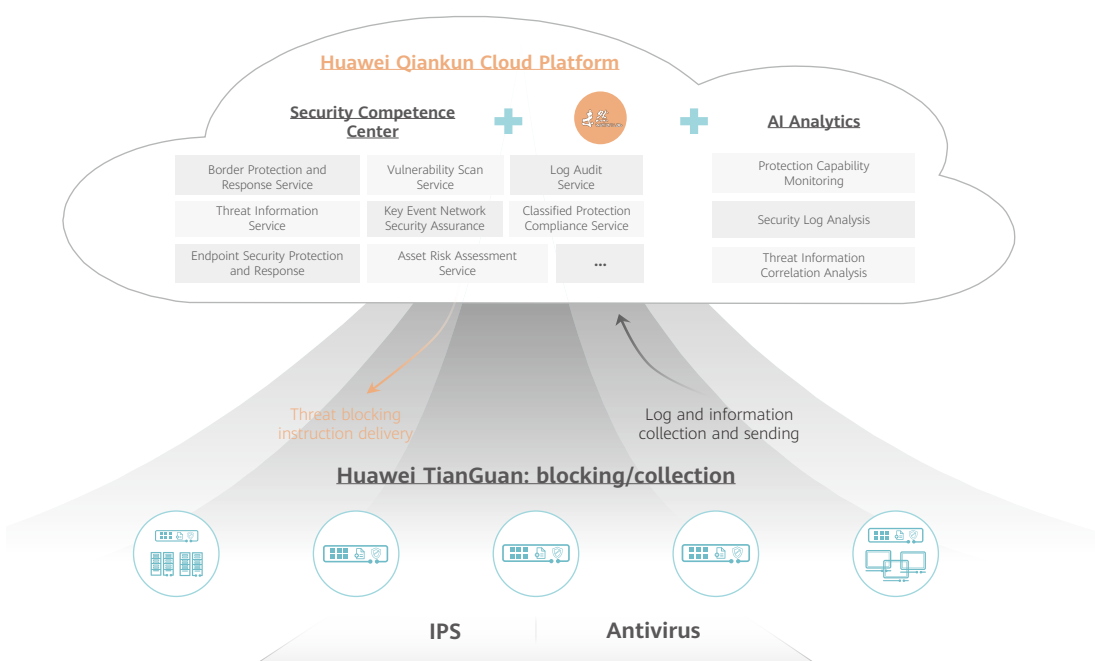


Figure 1-6 Huawei's Qiankun Security CloudService Solution

- TianGuan:** These devices are deployed at the local network egress of the customer and can help guard against unknown threats by leveraging AI capabilities as well as subscription-based functions, such as IPS, antivirus, and URL filtering. In addition, TianGuan works with the cloud service platform and serves as the basis of secure cloud services. Its core capabilities include:
  - Offers comprehensive content security capabilities, such as intrusion prevention and malicious file detection, to detect and block application-layer attacks.
  - Has a built-in Huawei security AI engine — AIE, which provides AI security detection capabilities at the edge and can perform detection tasks that cannot be completed based on traditional signatures. These tasks include those relating to brute force cracking, C&C,

DGA, and ECA algorithms.

3. Works with the cloud service platform to report key information related to security events, which are handled in a closed-loop manner based on instructions sent from the cloud service platform.
- **Huawei Qiankun cloud platform:** Based on the security logs and collected evidence data reported by TianGuan, the cloud platform implements security event analysis and protection policy association, and provides users with services such as security analysis, event handling, security warning, and security consulting. The core capabilities of the cloud platform are as follows:
    1. Receives key information related to security events reported by TianGuan protection nodes, analyzes security events in "machine + manual" mode, and sends accurate analysis results to users.
    2. For users who have authorized the cloud to automatically handle security events, the cloud platform provides the automatic closed-loop handling service to directly deliver closed-loop policies to TianGuan. For all other users, the cloud platform offers security event handling suggestions that guide users to handle security events by themselves in a closed-loop manner.
    3. Provides users with weekly and monthly reports as well as SMS notifications of urgent security events. It also provides customers with unified security analysis, expert services, and security event handling guidance by SMS and email to make security O&M easy to understand and efficient.



## Customer Benefits

Huawei's Qiankun Security Cloud Service Solution brings the following benefits:

1. **Lower deployment threshold:** Cloud services can be used to load service-oriented features on demand based on user service scenarios. This reduces deployment time, allows quick delivery of security capabilities, and enables continuous operation assurance for better defense. Powerful security solutions and best practices are deployed to help organizations comply with strict government policies, protect customer data, ensure business continuity, and minimize downtime.
2. **Personalized delivery:** Enterprises vary greatly in terms of scale, requirements, and capabilities. Based on organization requirements, security services can be customized in terms of security service capabilities, security situational awareness, and security event notification.
3. **Continuous upgrade of protection:** Customer sample data is utilized to continuously improve service capabilities and analysis accuracy. Cloud threat information, intelligence technologies, and big data technologies are employed to enhance automatic closed-loop threat handling capabilities. Real-time upgrade on the cloud and local devices as well as continuous iteration of network security services help continuously improve network defense capabilities.
4. **Accelerated threat response:** Managed maintenance and hosting capabilities are provided as services to help quickly detect threats and automatically authorize closed-loop threat handling, preventing theft or breaching

of core information assets.

- 5. Zero-trust access:** User access behaviors are evaluated to identify high-risk behaviors. If any such behaviors are found, user access is blocked or the user's access permissions is re-confirmed. In addition, access behavior management capabilities are enhanced for hybrid office and IoT access to mitigate risks.
- 6. Intelligent defense system:** Intelligent defense technologies driven by security big data will continuously mature. Algorithms can be introduced to cloud services more conveniently to form an intelligent security architecture consisting of analysis, control, and enforcement, covering the cloud, network, edge, and devices.

Currently, more than 10,000 deployments of Huawei Qiankun Security CloudService have been made for more than 10 industry customers

to provide convenient and effective innovative security cloud services. It supports more than 10 security services, such as intrusion detection, border protection and response, anti-ransomware attack, vulnerability scan, network threat assessment, log audit, threat information, emergency handling, monthly security report, and SMS notification. More security services will be rolled out through monthly iterations. Regarding the brand name Qiankun, Qian means "Heaven" in Chinese and represents Huawei cloud service platform, and Kun means "Earth" and represents Huawei TianGuan deployed locally. Huawei Qiankun is committed to building a robust network security space for customers through innovative network security cloud services.



# 04

## Data Center Networks Are Evolving to All-Ethernet







 **Trend**

Recent years have witnessed the wide deployment of mobile Internet, big data, cloud computing, and blockchain applications, as well as the increased adoption of data centers for experience-intensive applications such as 5G intelligent industrial control, high-performance computing (HPC) simulation and verification, and AI risk control. Against this backdrop, data centers play a pivotal role for traffic and services in the digital economy era, while there is also growing momentum in various technological innovations and transformations, such as infrastructure as a service. For service objects, a data center network connects computing and storage servers to transmit data between server resources, in addition to serving various upper-layer applications of cloud computing. Any change in cloud, computing, or storage services will disrupt data center networks.

On-demand services and elastic resources are two typical characteristics of the cloud. The open Ethernet architecture is well poised to meet cloud service requirements thanks to its high interoperability, scalability, and agility. This architecture can also be flexibly invoked by the cloud, in addition to delivering high-level security in multi-tenant scenarios. As such, the open Ethernet has become the de facto standard

of general-purpose computing networks. In centralized storage and HPC areas, traditional networks use closed technologies such as FC and InfiniBand, which feature poor interoperability and elasticity and slow evolution, failing to keep up with cloud data centers' requirements. According to IDC, FC's share of the data center market is only 5% of Ethernet's, while IB's is less than 1%. Ethernet switch shipments continue to eat into the FC and InfiniBand switch market shares. Indeed, the increasingly widespread adoption of cloud computing technologies in data centers increases networks' demand for Ethernet switching, making intelligent and lossless Ethernet the best choice now and in the future.

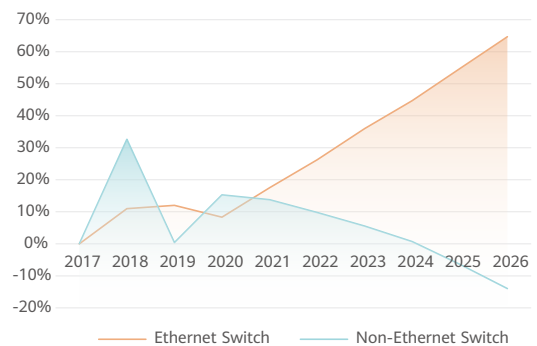


Figure 1-7 IDC: Growth rates of shipped Ethernet and non-Ethernet data center switches, including forecasts (2017 to 2026)

## All-Flash Storage Drives Ethernet-based Data Centers

Data surge and data value mining drive the innovation of storage media, with HDDs quickly being phased out by SSDs, which improve the storage performance by nearly 100-fold. This makes FC a system bottleneck in storage network scenarios in terms of bandwidth and latency due to the following reasons:

1. FC features closed technologies and poor interoperability, posing great challenges to the industry ecosystem and continuity.
2. FC undergoes sluggish development. For large-scale commercial deployments, its maximum bandwidth has rested at 32G. Storage services demand faster and higher-quality networks.
3. FC suffers from shortage of O&M professionals, with fewer than 5% of Ethernet O&M professionals. The end result is high FC network O&M costs and inefficient troubleshooting.



## PCIe Computing Units Are Replaced by Ethernet, Significantly Improving Performance

Currently, the data center server CPU market is dominated by the Intel x86 architecture, which mainly uses PCIe 3.0. PCIe 3.0 offers a limited number of lanes, with a single lane supporting only 8 GT/s data transfer rate. AI supercomputing servers have entered the era of 100GE NICs. This means that the PCIe 3.0 architecture has become a performance bottleneck in high-throughput and HPC scenarios. CPU/GPU vendors are replacing the PCIe bus to break through the bus rate bottleneck and provide higher computing power through Ethernet ports.



### Challenges

#### Three Challenges for Data Center Networks Evolving to All-Ethernet

1. **Packet loss:** Service data surges, with network performance becoming a bottleneck. Ethernet is naturally prone to packet loss, and as such falls short of performance requirements of HPC, high-end storage, and other performance-critical use cases.
2. **Management efficiency:** In recent years, small and midsize data centers across the globe are increasingly replaced by large or ultra-large data centers. Data center networks grow in management scale but still heavily rely on expertise in network construction and change. Manual service planning takes several months, manual review is error-prone, and service provisioning is unverifiable. As

a result, installation, deployment, and joint commissioning take 2 to 4 months, and more than 85% of faults are exposed only after complaints. The traditional management mode involving diverse tools and platforms severely hinders network O&M.

**3. Multicloud and multi-scenario:** To guarantee the stability of core services and rapidly

respond to service changes, enterprises prefer to deploy agile services on public clouds and stable services on private clouds. This, however, results in a complex architecture. In addition, network requirements vary significantly by service scenarios across industries, posing higher requirements on network openness and as-a-service offerings.



## Recommendations

### Use the Converged Ethernet Technology to Replace the Three Siloed Physical Networks in Traditional Data Centers, Achieving Convergence in a Larger Scope Across a Wider Range of Scenarios

As all-Ethernet is increasingly adopted in data centers, the three siloed physical networks in traditional data centers will ultimately be unified. Enterprises should use all-Ethernet when upgrading their data center networks to become unshackled from the restrictions of the appliance solution in terms of limited scale, separated management, closed architecture, and applicable scenarios. This achieves convergence in a larger scope across a broader range of scenarios.

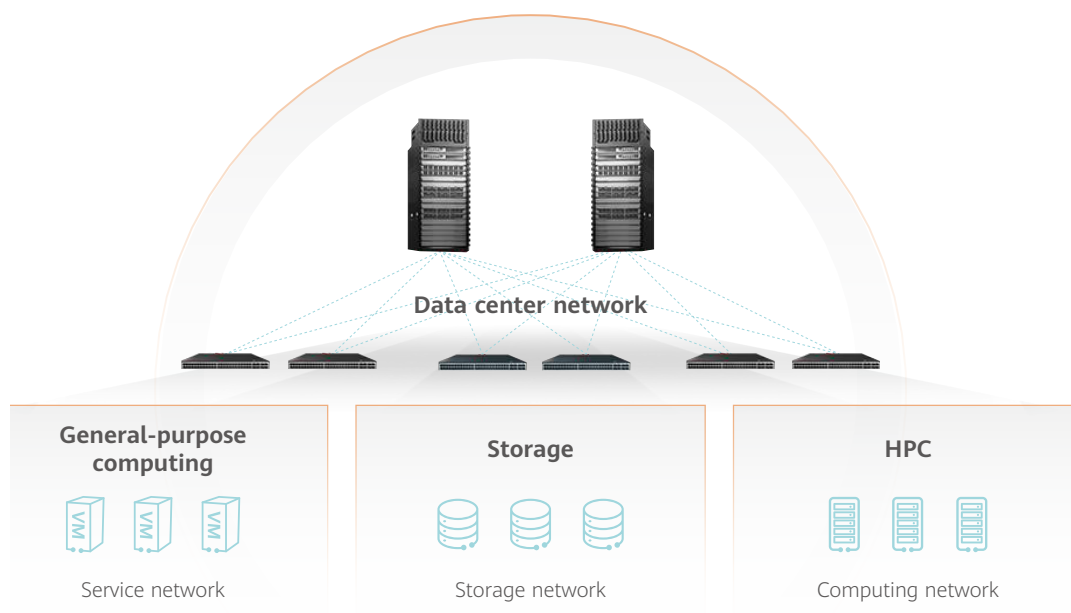


Figure 1-8 All-Ethernet architecture of data centers

**1. Lossless Ethernet network, converging traffic transmission:**

General-purpose computing, storage, and HPC networks are carried on the Ethernet technology stack. Unifying the networking protocol and using a mix of TCP and RoCE data flows for transmission help to overcome the limitations of the traditional distributed architecture.

**2. Full-lifecycle automated management, implementing convergence of management, control, and analysis:**

Based on the unified network digital twin base, big data, and AI, automation is achieved throughout the full lifecycle spanning planning, construction, maintenance, and optimization. This avoids manual processing of a large number of repetitive and complex operations. Plus, based on massive data, network prediction and prevention capabilities are drastically enhanced, achieving centralized management across tools and platforms.

**3. All-scenario service capabilities, implementing all-scenario convergence:**

Core service capabilities such as physical network services, logical network services, application services, interconnection services, network security services, and analysis services of data center networks are abstracted. This enables flexible access of offline and online data on devices from multiple vendors based on the open service-oriented architecture. This, in turn, meets unified network orchestration requirements in private cloud, public cloud, hybrid cloud, and other industry scenarios, as well as supports flexible and intelligent scheduling of computing power across clouds without being limited by regions or scenarios.



## Solution

### Huawei's CloudFabric 3.0 Solution

In response, Huawei launched the CloudFabric 3.0 Solution, which consists of CloudEngine data center switches and iMaster NCE — an autonomous driving network management and control system. It implements an all-IP architecture for computing, storage, and service networks, supports IPv6, and is the first to offer L3.5 autonomous driving network capabilities. Also, this sophisticated solution supports full-lifecycle automation and network-wide intelligent O&M of data center networks, reducing OPEX by 30% and enabling intelligent upgrade of enterprises.



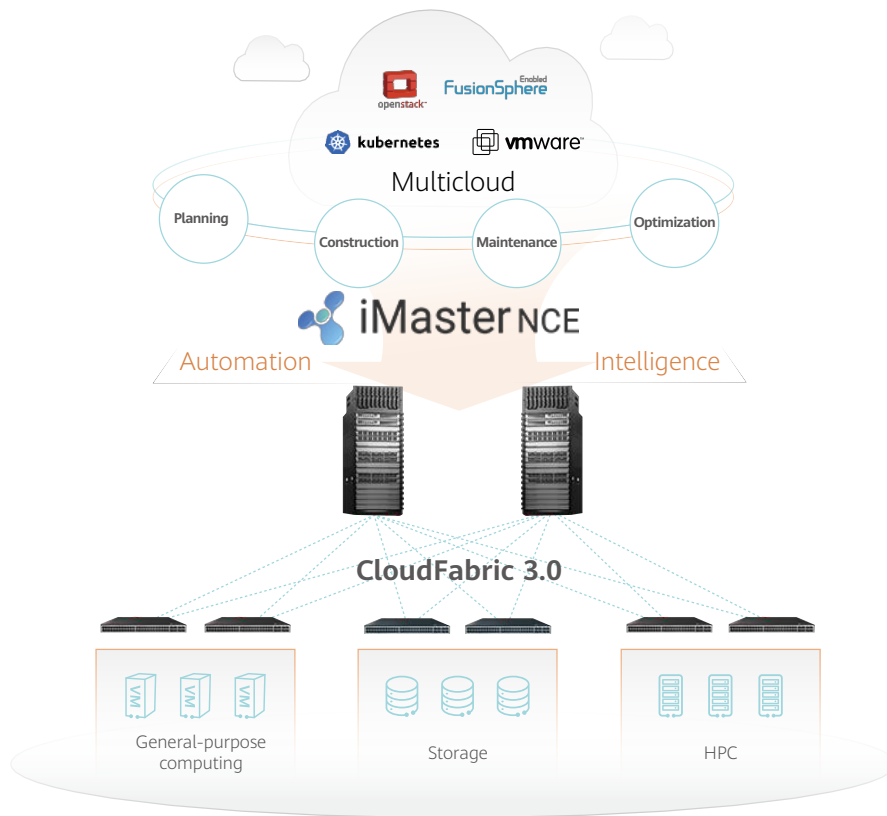


Figure 1-9 Architecture of Huawei's CloudFabric 3.0 Solution



## Customer Benefits

Huawei's CloudFabric 3.0 Solution brings the following benefits:

**1. All-Ethernet HPC network, unleashing 100% of computing power:** Packet loss on traditional Ethernet is a performance bottleneck, with a packet loss rate of just 0.1% halving computing power. Over the past four decades, experts worldwide have worked tirelessly to eliminate packet loss on Ethernets. Some of these experts tried to control the packet transmission speed through flow control and backpressure.

This method, however, frequently halted packet transmission, leading to ultra-low throughput. Not only this, as network application traffic continues to grow in diversity and complexity, controlling the packet transmission speed becomes less practical. That's where Huawei's innovative iLossless algorithm comes in. It implements real-time and precise speed control, eliminating packet loss and doubling the computing power with the same network scale.

**2. All-Ethernet storage network, improving**

**vstorage performance by 93%:** Among all service scenarios, the financial active-active data centers are the most demanding of storage network performance. Data transmission through optical fibers involves a static delay of about 5  $\mu$ s/km. Data centers within a city may be located 30 to 70 km away from each other, resulting in a delay 100 times higher than that in short-distance transmission, significantly increasing the complexity of flow control. To resolve this issue, Huawei added distance variables to the short-distance lossless transmission algorithm and created the innovative iLossless-DCI algorithm for long-distance transmission scenarios. This exclusive algorithm predicts and copes with traffic changes based on big data analytics, achieving lossless data transmission over distances of up to 100 km at 200 Gbps. Further to this, the storage networks built on Huawei's solution require 90% fewer links, improve the IOPS by 93%, and reduce network delay by 49% compared with FC networks in both intra- and inter-DC scenarios.

### 3. Full-lifecycle automated O&M, enabling second-level service deployment, and "1-3-5" troubleshooting:

Currently, semi-automated O&M mode is frequently used in the industry. In this mode, networks are manually designed and verified, and configurations are automatically delivered. Huawei offers an innovative solution that introduces digital twins to network management, enabling full-lifecycle network automation. Leveraging digital network modeling, this purpose-built solution can comprehensively evaluate over 400 network design factors, recommend optimal network design solutions based on the evaluation results, and verify

configuration changes in seconds. With network knowledge graphs, it can achieve "1-3-5" intelligent O&M: faults detected in 1 minute, located in 3 minutes, and rectified in 5 minutes. In addition, with big data mining and modeling, this solution discovers correlations between network objects and fault spreading rules to accurately detect 90% of potential faults.

### 4. Unified management of multi-cloud and multi-vendor heterogeneous networks, slashing cross-cloud service deployment time from months to days:

Heterogeneous networks are now very widely used in multi-cloud scenarios, where multiple sets of controllers need to be deployed to manage devices from different vendors. In such scenarios, a service change cannot be made with just one controller. If the controllers cannot handle service changes, device vendors need to step in and implement related requirements in later versions, which takes 3–6 months on average. Not only this, these controllers also need to be connected to cloud management platforms, creating a heavy adaptation workload. On top of this, there are many APIs in the controllers' southbound and northbound directions, which makes deploying a cross-cloud network time-consuming. All of these hamper the utilization of computing power across areas. To address this, Huawei's CloudFabric 3.0 Solution defines a unified NE model and builds an open southbound framework to centrally manage multi-vendor devices and dynamically load device drivers. In addition, Huawei's CloudFabric 3.0 Solution provides thousands of network API services in the northbound direction, enabling flexible network orchestration on the cloud management platform and slashing the service rollout time from months to just one week.

To date, Huawei's CloudFabric 3.0 Solution has been deployed in data centers of more than 21,000 customers across sectors such as finance, government, Internet, manufacturing, and energy. In the future, digitalization will continue to drive continuous network innovation. As

such, Huawei will continue to enhance its Ethernet network capabilities for data centers to fully unleash computing power and facilitate enterprises' intelligent upgrade.

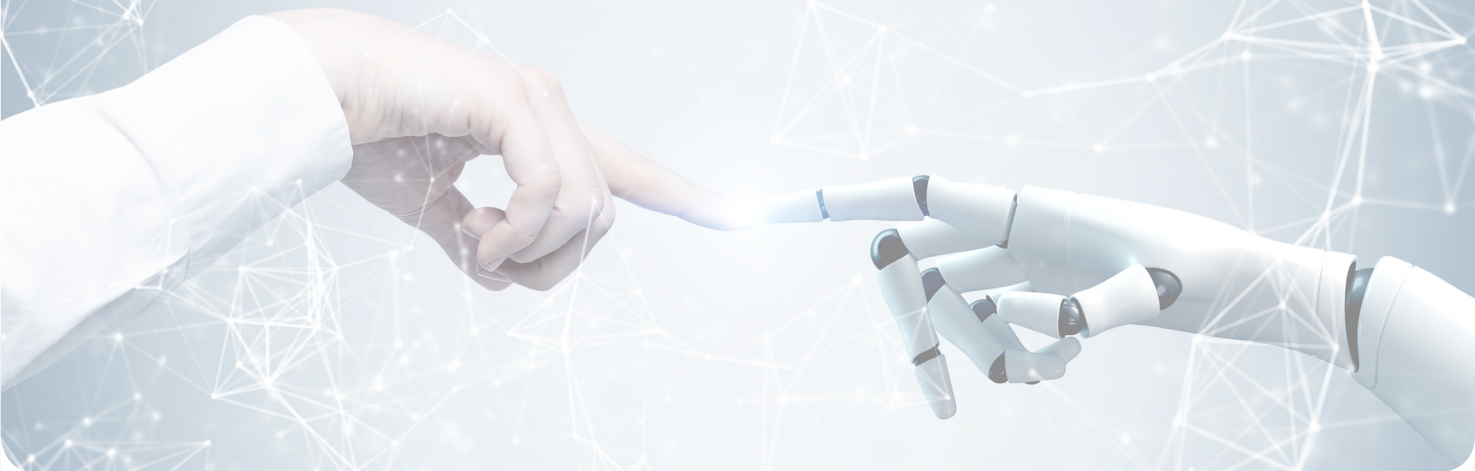


# 05

## **AI-based Hyper-Automation Is Changing the Network Management Mode**







## Trend

Driven by new technologies such as mobility, big data, cloud computing, and AI, the number of NEs, technology stacks, and services involved in the enterprise IT architecture increases exponentially, yet the workforce of the enterprise O&M department remains unchanged. This puts great pressure on network O&M. Generally, O&M personnel can locate the cause based on massive logs and monitoring data after detecting service fluctuation, which by then may have already resulted in huge losses. As the demand increases for agile provisioning of new services, enterprises often need to quickly respond to market changes to stay competitive. Traditional device-centric O&M lacks insights into user and service experience and passively responds to faults. This fails to provide the user and service experience assurance required in today's digital transformation era.



## Challenges

### Pain Points of Device-Centric O&M

- 1. Device-centric, lacking insights into user experience:** Traditionally, the network management system (NMS) provides functions such as device management, topology management, and alarm configuration. O&M personnel can monitor topologies and alarms on the NMS to identify network exceptions. However, as terminals proliferate and digital services diversify, normal running of devices does not necessarily mean good user and service experience. For example, when there is strong co-channel interference, wireless users connected to an AP will have poor Internet access experience even if the AP is running properly. Likewise, when QoS configurations are incorrect, user experience of some applications will be poor even if network devices are running properly.
- 2. Passive response to faults, relying on onsite fault locating and rectification and resulting in slow fault recovery:** Network O&M personnel have to always be prepared for possible faults, especially during major holidays or big events. Once a fault occurs, O&M personnel need to immediately check the network topology and log in to devices

through the CLI to locate the fault. More than 60% of faults need to be rectified on site. If the fault symptom disappears, O&M personnel have to wait until the fault recurs or attempt to reproduce the fault. What's worse, wireless reconstruction further exacerbates the troubleshooting difficulty. Due to the complexity of the wireless environment, more than 90% of faults need to be located on site.



## Recommendations

### Upgrade O&M from Device-Centric to Data-Centric

Compared with traditional O&M, the network architecture of data-centric O&M requires the following changes:

#### 1. Network devices need to provide data collection and edge intelligent analysis capabilities.

For networks, AI can play a truly meaningful role after it is used to mine valuable data. Networks generate massive data, alarms, and logs every day, which is very taxing for enterprise O&M personnel. However, only a tiny proportion of the data is of value, and the data is not obviously associated with the service quality. As such, the obtained information is of little value to services even if the most advanced AI algorithms are used. The key to overcoming this problem is to mine the source of valuable data. Therefore, network devices need to report data in real time, and preliminarily analyze raw data on NEs locally or perform computing acceleration using matrix algorithms such as the neural network

algorithm. The purpose is to process and analyze data of a large number of distributed nodes in order to prevent a large amount of data from being sent to the management and control center and consuming computing resources.

#### 2. The intelligent network analyzer is introduced to implement intelligent analysis based on big data and AI.

The intelligent network analyzer detects user and application experience, identifies faults and potential faults, locates root causes, and intuitively displays the results in a way that O&M personnel can easily understand. It can also perform intelligent global network optimization and intelligent prediction of NE- and service-level resources for network planning guide. The intelligent network analyzer provides the following features:

##### 1. Detect user experience and implement visualized experience management:

- 360-degree experience visualization and journey playback of a single user
- Experience visualization of all users

##### 2. Proactively identify user and service experience problems, identify potential faults and root causes, and provide rectification suggestions, or even automatic rectification:

- Detect faults immediately once they occur.
- Identify users and applications with poor experience.
- Identify potential problems and eliminate them in advance.
- Locate root causes of faults, provide rectification suggestions, and even automatically rectify the faults.



## Huawei's Native Intelligence Data Communication Network Solution

Huawei's Native Intelligence Data Communication Network Solution consists of the data collection layer and intelligent analysis system.

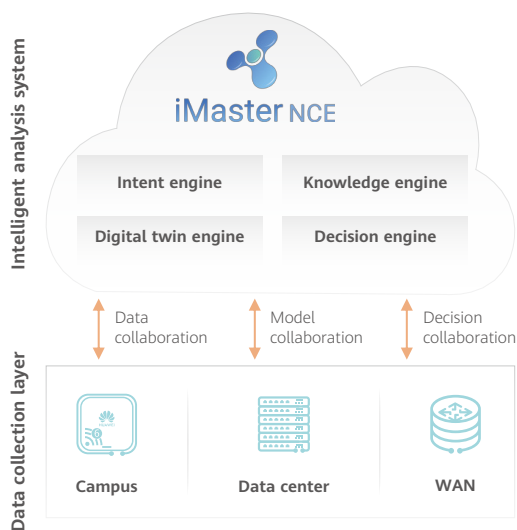


Figure 1-10 Architecture of Huawei's Native Intelligence Data Communication Network Solution

**1. Data collection layer:** Network devices collect metrics and information about terminals, devices, and applications from various dimensions, such as terminal access logs (including protocol interaction logs), terminal performance metrics, radio performance metrics, device performance metrics, and audio/video service performance metrics. Traditional NMSs use the Simple Network Management Protocol (SNMP) to obtain device metrics. However, this approach fails to provide data-

centric O&M. With the Streaming Telemetry technology, Huawei campus network devices can remotely collect data from terminals at a high speed for network monitoring. This data collection mode is 20 times faster than SNMP-based data collection, and data can be collected within 10 seconds.

**2. Intelligent analysis system:** The network analyzer is built based on Huawei's big data analyzer is built based on Huawei's big data platform and eschews the traditional resource status-based monitoring mode. It performs feature analysis and baseline calculation using machine learning algorithms, and automatically identifies network faults, demarcates faults, and optimizes networks. In addition, it displays analysis results on a variety of GUIs, providing end-to-end high-quality network experience for enterprise networks.

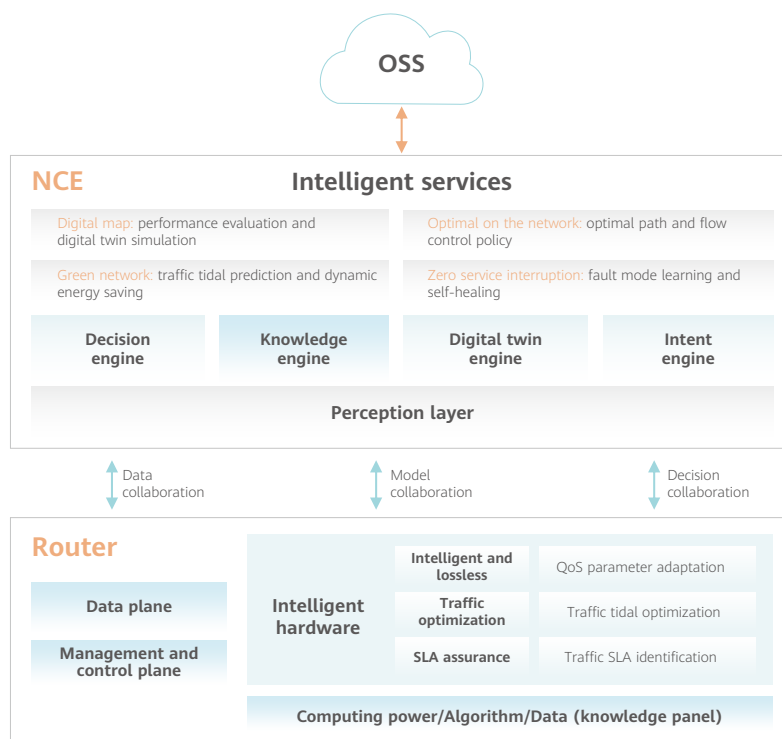
Huawei's Native Intelligence Data Communication Network Solution includes the IntelligentWAN Solution for WANs, IntelligentCampusNetwork Solution for Campus Networks, and IntelligentFabric Solution for Data Center Networks.





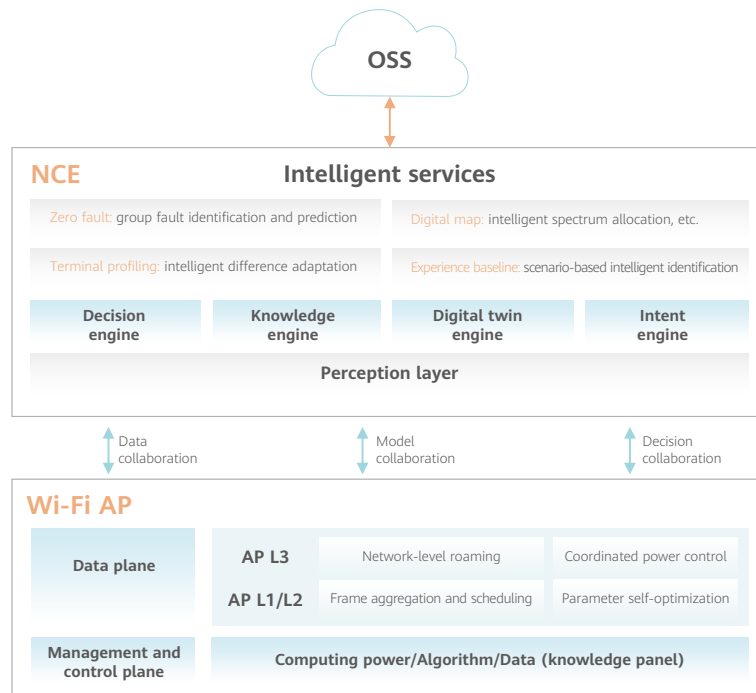
## Customer Benefits

IntelligentWAN Solution: Providing Native Intelligence for WANs



- 1. Multi-dimensional exception identification and network health visibility:** In-situ Flow Information Telemetry (IFIT) is used to ensure real-time SLA awareness at the service and packet levels, and to quickly detect service quality in terms of packet loss, delay, and jitter in end-to-end or hop-by-hop mode, helping quickly demarcate and locate faults. A large amount of configuration, alarm, log, and KPI data from various dimensions is reported, covering all status data generated by the running system. More than 80,000 KPIs are monitored. Devices equipped with AI chips use the NCE online learning and collaboration technology to quickly identify network exceptions and detect silent faults, with an accuracy rate exceeding 90%.
- 2. Intelligent fault diagnosis based on AI and knowledge graph:** Based on Huawei's years of O&M experience in fault diagnosis, up to 200 million samples are used for AI training, covering the analysis of root causes for more than 200 types of faults of nine categories, while raising the accuracy rate of root cause diagnosis to 99%.
- 3. Precise fault rectification and self-healing:** Precise suggestions for rectifying faults are provided for more than 90% of typical faults to implement service fault self-healing and ensure high-quality SLA experience. Self-healing rules are orchestrated to automatically close the O&M process.

## IntelligentCampusNetwork Solution: Providing Native Intelligence for Campus Networks



### 1. Network health evaluation, proactively identifying 85% of potential network faults

- Multi-dimensional network health evaluation: Perform wired and wireless network health analysis and periodically push reports.
- Minute-level fault demarcation and locating: Proactively identify 200+ issues of eight categories and predict potential risks in advance.

### 2. Visualized user experience, reducing user complaints by 90%

- Experience visualization throughout the user journey: Provide visualized real-time journey experience of each user at each moment.
- Protocol tracing of access issues: Quickly locate user access issues, analyze root causes,

and provide rectification suggestions.

### 3. Application experience assurance, shortening fault locating time by 95%

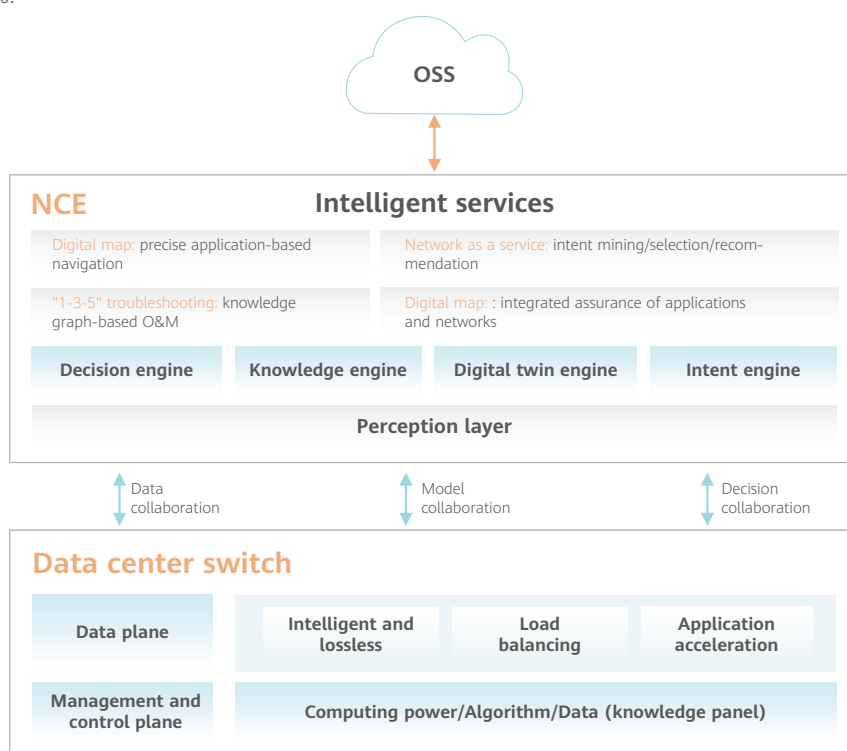
- Intelligent identification and awareness of applications: Identify 1000+ mainstream applications through AI and proactively detect the application quality.
- Minute-level application fault locating: Use the exclusive in-band flow measurement technology to implement fault demarcation and locating within minutes.

### 4. Intelligent radio calibration, improving the network performance by 58%

- Predictive calibration: Predict AP loads and implement automatic optimization of wireless networks, boosting network performance by more than 50%.

- AI roaming: Establish roaming baselines based on different terminal types and provide differentiated roaming steering, improving the roaming success rate by 70%.

## IntelligentFabric Solution: Providing Native Intelligence for Data Center Networks



Huawei's IntelligentFabric Solution brings the following benefits for data center networks:

- "1-3-5" troubleshooting:** Leveraging Telemetry, iMaster NCE-FabricInsight collects data on the management, forwarding, and data planes of the entire network in all scenarios, and detects exceptions within 1 minute. In addition, it uses the knowledge graph to automatically identify the root causes of faults and potential risks within 3 minutes, as well as provide effective rectification suggestions. Furthermore, iMaster NCE-FabricInsight cooperates with iMaster NCE-Fabric to recommend fault handling plans, enabling typical faults to be quickly rectified within 5 minutes.
- Network intent verification:** iMaster NCE-FabricInsight provides service intent verification on the data plane. In key service assurance scenarios such as service changes, it delivers 24/7 automatic verification of whether the network intent meets expectations and identifies full-path connectivity. It also detects service and underlay interconnection exceptions within seconds, automatically analyzes root causes for abnormal paths, and notifies users to promptly handle the exceptions.
- Network change visibility:** As data center networks are subject to frequent network changes, traditional manual O&M faces pressing challenges in terms of detecting thousands of device configuration changes

and learning tens of thousands of entries per device. With network snapshot management, iMaster NCE-FabricInsight supports automatic and manual synchronization of snapshots from the dimensions of device configuration, entry, topology, capacity, and performance. In addition, it automatically analyzes differences before and after changes, and clearly displays the detection results.

- **IP 360 management:** When production systems are migrated to the cloud, the VMM automatically completes VM deployment and migration. However, information such as VM node location, VM migration or offline time, and VM distribution cannot be quickly found, meaning that only passive O&M can be performed on the network side. iMaster NCE-FabricInsight provides IP 360 analysis to quickly learn the number of online VMs and the distribution of top N switches connected to VMs, helping network administrators effectively plan resources in advance. iMaster NCE-FabricInsight supports full lifecycle management of network-

wide VMs, displays VM logout, migration, and login records in real time, and provides network-wide IP snapshot analysis. It also compares all IP address changes before and after network changes, and checks whether exceptions such as VM logout occur.

- **Intelligent analysis of network-wide logs:** After a network fault occurs, a large number of logs are generated, among which 95% are invalid. Traditionally, logs are manually checked one by one, which is time-consuming and labor-intensive. iMaster NCE-FabricInsight visualizes network-wide log events, including the multi-dimensional trends, distribution statistics, and details from Layer 0 to Layer 4. In addition, it supports noise reduction and convergence of abnormal logs. More than 200 default aggregation and clearance rules are preset in the system, and rules can be manually customized to improve log analysis efficiency.



# 06

**Industrial Networks  
Are Moving Towards  
IT/OT Convergence,  
Enabling Intelligent  
Industrial Upgrade**







## Trend

### Industrial Control Is Becoming Remote and Centralized, and Intelligent Industrial Transformation Is Gaining Momentum

**1. The demand for remote and centralized control surges, driving up least-staffed and even unstaffed onsite production.**

The industrial production control rooms of a traditional factory are divided into three levels: onsite operation room, factory scheduling room, and base main scheduling room. The operation room is located at the production site. Harsh or dangerous onsite operation environments are common in many industries, such as the chemical industry and metallurgy. It is therefore vital that such industries can perform onsite operations through remote and centralized control in a least-staffed or even unstaffed manner.

**2. Seamless data transfer facilitates intelligent industrial transformation.** The basic requirements of Industry 4.0 intelligent production are to use network information technologies and advanced manufacturing tools to improve the intelligence of production processes, facilitate cross-system data flow (including

data collection, analysis, and optimization), and enable device performance awareness, process optimization, and intelligent production scheduling. Big data can play its role only when data is fully collected and transferred with as little loss as possible. In addition, to implement AI machine vision-based quality inspection, intelligent production scheduling, and process optimization, the computing power needs to be deployed at the edge or even onsite. As industrial intelligence gradually penetrates into industrial sites, the convergence between control and intelligence and between real-time and non-real-time data flows is driving the industrial control system to develop towards the next-generation intelligent industrial control architecture.



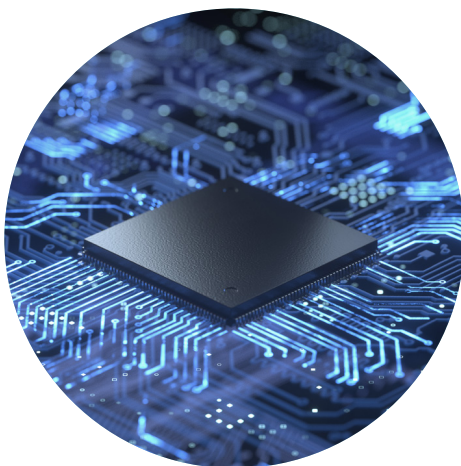
## Challenges

### New Challenges Facing Traditional Industrial Networks

**1. Existing industrial control systems generally**

use LAN architectures such as industrial Ethernet and industrial bus, which cannot meet the requirements of remote and centralized control. Take industrial Ethernet as an example. The maximum distance between two nodes is 100 m. If the distance exceeds 100 m, the two nodes cannot work. This cannot meet the remote and centralized control requirements of large enterprises. Direct fiber connection can meet the remote control requirements of only a few devices and is inapplicable to enterprises with large numbers of control devices. In a base of a steel enterprise, the control systems for thousands of controlled devices within a radius of 20 km need to be moved to the centralized control center. If direct fiber connection is used, thousands of pairs of optical fibers longer than 40 km need to be deployed, which is unacceptable to the enterprise.

2. **Disparate traditional industrial control protocols are difficult to interoperate with each other. As such, a large amount of data**



is accumulated on siloed networks, making it difficult to perform big data analytics and closed-loop optimization. Consequently, the value of industrial data cannot be fully mined to meet the requirements of intelligent industrial evolution. Large numbers of non-standard protocols cause many data silos. Traditional industrial field networks mainly use fieldbus or industrial Ethernet technologies. The separate development of different industries has led to multiple incompatible field network technical standards, such as ProfiBus/ProfiNet and EtherCAT. These industrial control systems generally use a closed architecture and can use only external sources to achieve a certain level of intelligent manufacturing.



## Recommendations

### Build Advanced Industrial Networks to Facilitate Data and Intelligence Access, As Well As Accelerate Intelligent Industrial Transformation

1. **Connect devices to the network.** Improve the online rate of industrial terminals by adopting a combination of technologies, such as Wi-Fi, IoT, 5G, and optical fiber, thereby allowing data to be perceived comprehensively and flow freely. For flexible manufacturing, reconstruct wired network devices on demand to improve device networking flexibility and minimize production line adjustment time after a production task is delivered.

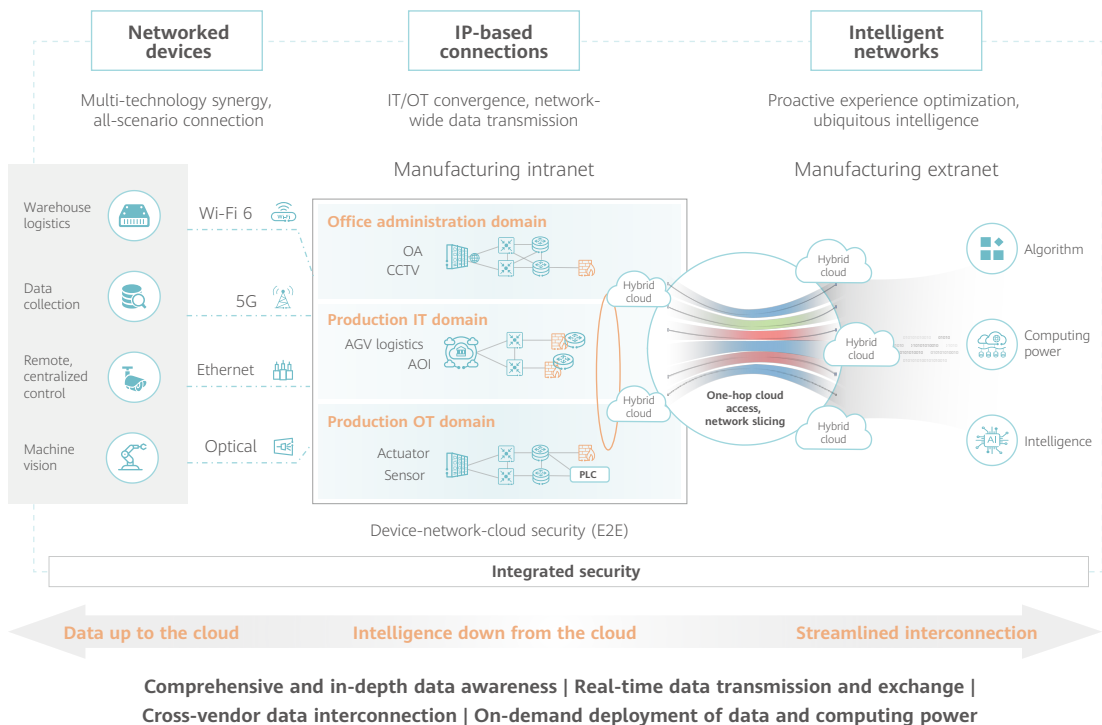
**2. Deploy IP-based connections.** Use IPv6 Enhanced to improve deterministic service capabilities of IP networks and achieve IT/OT convergence. IPv6 Enhanced innovations, especially DIP, provide deterministic service capabilities of IP networks for industrial scenarios. They spur the IP-based development of industrial networks, as well as facilitating the construction of fully connected factories and the development of next-generation intelligent industrial control systems. In this way, they help to accelerate the digital transformation of the manufacturing industry.

**3. Build intelligent networks.** Improve differentiated service and experience assurance capabilities for different services, management and O&M capabilities for massive numbers of IoT terminals, and intelligent defense capabilities for guarding against security threats. These capabilities

include intelligent service identification and experience assurance, introduction of trustworthy industrial identifiers for automatic and trusted network access, AI fingerprint identification of industrial terminals, intelligent management and control of network behavior, joint orchestration and proactive optimization of industrial services and networks, as well as big data-based fault demarcation and locating.



## Huawei's Manufacturing Cloud-Network Solution



### 1. Continuous Wi-Fi 6 networking, stable connectivity, IoT convergence

Smart antennas enable networks to be automatically adjusted according to the movement of users, achieving zero coverage holes in all scenarios, stronger signals, and faster speeds. AI roaming ensures that terminals remain connected and services remain available during roaming. AI continuous networking enables network-wide quality awareness, fault prediction, and automatic optimization.

### 2. Industrial-grade IoT gateway, edge intelligence

IoT gateways with rich interfaces and industrial-grade design are adopted to match various IoT scenarios. These gateways provide edge intelligence and multi-container management and allow partner applications to be deployed on demand. Moreover, they can convert industrial protocols to IP and serve as an underlying open platform that integrates control, management, computing, and communication functions.

### 3. Converged transport, one network for multiple purposes

- Network slicing enables one network for

multiple purposes. Hierarchical slicing enables hard isolation to ensure deterministic bandwidth. A network can be partitioned into over 1000 slices, with a slicing granularity of 10 Mbps, preventing resource wastes.

- SRv6-based one-hop cloud access enables agile network adjustment upon cloud changes for multi-cloud access over deterministic-quality paths.
- DIP-based deterministic low latency (low jitter) meets industrial remote control requirements through joint efforts of the industry chain.

DIP has made great breakthroughs and started to move from technical prototyping to business innovation. In 2021, Huawei worked with partners such as Shanghai Jiao Tong University, Shanghai Baosight Software (600845), and Purple Mountain Laboratory to complete the world's first WAN cloud-based PLC test. In this test, deterministic network services were provided over a WAN IP network across 600 km to support the stable operation of remote industrial control systems based on cloud-based PLCs.



# 07

**Striding Towards  
Net5.5G Together,  
Connecting Ubiquitous  
Computing Power  
and Intelligent Living**



**Clearly, future networks promise tremendous potential and uncertainties. The entire industry needs to work together to explore these new technologies, move towards Net5.5G, build ubiquitous intelligent IP networks, and connect ubiquitous computing power and intelligent living.**

On our journey to 2025, digital capabilities will continuously improve the way we live and work. As the foundation of digitalization, data communication networks will deliver high-quality data and computing power to individuals and various industries, stimulate digital vitality, and unleash digital productivity.

**Connecting individuals:** The development of 5.5G will further drive the development of emerging 2C services, such as immersive XR, hundreds of billions of mobile IoT connections, and holographic/tactile Internet, greatly enriching people's digital life. It is imperative to increase bandwidth from 1 Gbps@anywhere to 10 Gbps@anywhere and reduce jitter from milliseconds to hundreds of  $\mu$ s. As the transport foundation of 5.5G, the data communication network needs to further improve its bandwidth and deterministic assurance capabilities.

**Connecting enterprises:** The digital transformation of various industries gradually enters a critical period, and a series of new application scenarios emerge one after another. Digital and intelligent capabilities will further enable enterprises to improve office production efficiency, optimize end users' service experience, and fully unleash digital productivity. On the one hand, enterprises connect sensors and IoT terminals of increasingly diverse types, such as NFC, BLE, Wi-Fi, and LoRa, to the network. On

the other hand, digital production technologies such as AOI require 3.2 Gbps ultra-high bandwidth per production line. IP networks are deeply involved in OT scenarios, enabling communication between production equipment. This poses new requirements on data communication networks in terms of high bandwidth, deterministic transport, and ubiquitous IoT capabilities. The expansion of IoT borders increases security threats. As such, it is imperative to expand security protection borders and improve security protection efficiency.

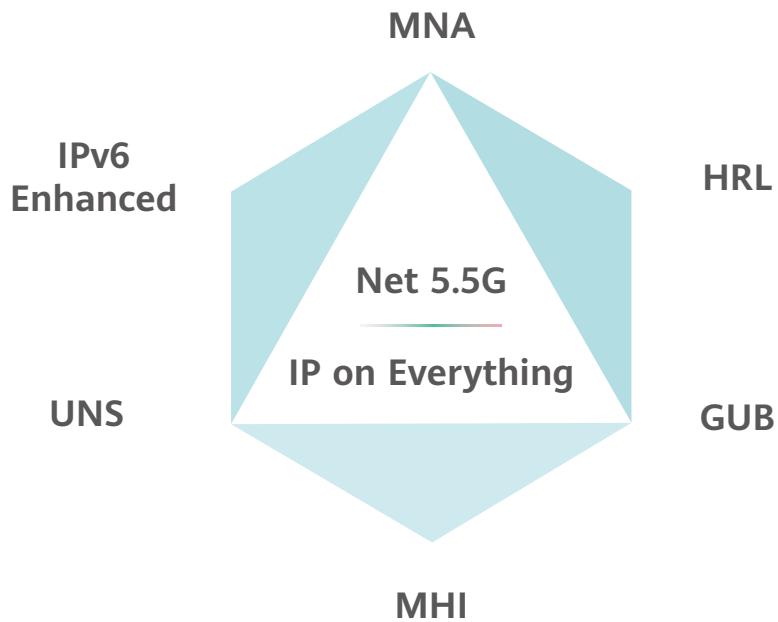
**Unleashing computing power:** Computing power is generated inside a data center. IDC predicts that the global computing power will have a CAGR of 50% in the next five years. The computing power of a single data center will evolve from the EFLOPS level to the hundreds of EFLOPS level, and the access bandwidth will rise to 800 Gbps. With the increase of computing power, the number of nodes on a single DCN increases accordingly, from six digits to seven digits. Therefore, the DCN must be capable of ultra-large-scale networking. Elephant flows occupy a large amount of bandwidth, and the network loads are usually uneven. According to statistics from Google and Peng Cheng Laboratory, the effective data center throughput for AI computing is less than 25%. It is essential to balance data flow scheduling and improve effective throughput. Because DCN Ethernets are

deeply intertwined with servers, the industry is coming to the consensus that all-Ethernet bus interconnection is the best solution. Computing chip leaders such as Intel choose XPU over Ethernet for high-speed interconnection. This poses a daunting challenge to ultra-low latency interconnection between CPUs/GPUs/memories.

Computing power transmission also faces new scenarios and changes. First, multiple clouds and diversified computing power have become a growing trend. According to Flexera 2021 State of the Cloud Report, 92% of enterprises adopt a multi-cloud strategy. Survey respondents use 2.6 public clouds and 2.7 private clouds on average, and computing power use tends to be diverse. For example, the manufacturing execution system (MES), video collaboration system, and other service systems tend to use general-purpose computing power; new vehicle R&D, wind resistance/collision experiments, and other simulation activities require powerful computing power (usually HPC); production line quality inspection, autonomous driving training, and

other activities tend to use AI computing power. Such diverse and distributed computing power drives up the demand for flexible interconnection between clouds over one network. Moreover, the AI and HPC data volume per transmission is as high as 10 TB/100 TB, requiring higher transport network bandwidth. AI computing power is deeply involved in enterprise production. For example, industrial motion control requires a jitter of 10  $\mu$ s.

To address these new requirements and challenges, Net5.5G adopts E2E SRv6 and provides enhancements from six dimensions: green ultra-broadband (GUB), massive heterogeneous IoT (MHI), high resilience & low-latency networking (HRL), IPv6 Enhanced, multi-domain network AI (MNA), and ubiquitous network security (UNS). These enhancements help continuously improve IP network capabilities, build a high-quality digital foundation, and connect ubiquitous computing power and intelligent living.



## 1. GUB

Bandwidth is the basis for the development of various digital applications. Currently, 8K videos require a bandwidth higher than 100 Mbps, and mobile cloud VR requires a bandwidth of 230 Mbps. At the same time, various AI applications are booming. In addition, the scale of datasets used for AI training is increasing from the TB level to the 10 TB or even 100 TB level. In a joint innovation between Huawei and China Mobile in network autonomous driving, it took seven days to transmit 40 TB training data to the data center through a 70 Mbps private line. Clearly, higher bandwidth is required, and only bandwidth capable of dynamic adjustment can support the development of these new services. In the future, an increasing number of high-quality services will emerge. Services such as immersive XR and holographic communication are all bandwidth-intensive applications. The bandwidth of a single immersive XR channel will reach 4.4 Gbps, that for transmitting HD mobile holograms will reach 10 Gbps, and that for holographic communication with digital twin experience will even reach the Tbps level.

It is estimated that network traffic will grow by 30% annually, with network bandwidth doubling in three years and increasing 10-fold in a decade. The network port rate will be upgraded from 100GE to 400GE/800GE. At the same time, breakthroughs will occur in hardware- and chip-related bottom-layer technologies. Chips will evolve from the current 2D/2.5D chiplet architecture to the 3D chiplet architecture. In addition, the converged heterogeneous NP processor architecture enables DCN switches and routers to evolve to 800GE ports. Hardware heat dissipation technologies will develop from device-level air cooling and liquid cooling to chip-level jet cooling and silicon-based micro-liquid cooling. In addition, more advanced

thermal interface materials will emerge, increasing the thermal conductivity 10-fold. On the wireless side, Wi-Fi bandwidth will develop faster. With the AP collaboration algorithm and D-MIMO enhancement, Wi-Fi 7 will deliver a peak bandwidth of 30 Gbps.

## 2. MNA

In the future, networks will face greater challenges in terms of complexity. Specifically, with 5G, 5.5G, and X2B services being widely deployed, the network scale will increase 10-fold; aligning with cloud services to provide cloud-like network experience, NaaS, and e-commerce-like experience requires 10-fold experience improvement; and agile service provisioning within days, fault self-rectification within minutes, and zero customer complaint require 10 times higher network O&M efficiency.

To address the preceding challenges, we have defined networks that can evolve to automation and autonomy. Just like how autonomous driving makes use of digital maps, network digital maps are the basis of online network planning. Network digital maps built through real-time and multi-dimensional awareness enable automatic and precise navigation of network paths and precise capacity expansion. In intelligent network analysis and simulation, a network simulation topology can be built based on the digital twin, and an ideal network configuration library can be built based on the real network configuration library. This way, network planning, deployment, and changes can be simulated based on the ideal library. On a large-scale network with 100K nodes, the configuration and data planes can be quickly simulated using fast simulation algorithms and verified before being deployed on the actual network. This avoids human errors during network configuration modification. The fault knowledge base is continuously enriched



through knowledge graph self-learning to enable automatic troubleshooting, alarm noise reduction, aggregation and analysis of root causes within 3 minutes, and identification of affected services within 5 minutes. AIOps, cloud AI, network-level AI, and NE AI enable intelligent closed-loop O&M through automatic training, self-growth, and self-decision-making. Moreover, networks can also quickly orchestrate AI operators, compute open and programmable paths, automatically optimize deteriorating service flows and traffic congestions, and automatically rectify runbook faults.

### 3. IPv6 Enhanced

Emerging services, applications, and scenarios lead to an explosion in data volume. As such, industries have high requirements on computing power and networks. Computing power is a resource that has become as ubiquitous as electricity. The network needs to make computing power easier to access and data easier to flow to meet users' needs. IP networks need to adopt a new protocol design to centrally orchestrate computing power and network resources, better schedule computing power, and provide differentiated, congestion-free, and low-latency transport.

Currently, networks tend to be unaware of applications. As a result, service quality can only be ensured by continuously increasing bandwidth, resulting in low network utilization. As the marginal effect gradually disappears, the continuous investment of carriers fails to bring corresponding gains.

APN6 makes full use of the programmability offered by IPv6/SRV6 and brings application information (IDs and SLA requirements) into networks, eliminating the boundary between applications and networks. In addition, APN6 uses a slicing technology capable of providing

10K+ slices over one network to provide refined operations for applications, enabling application-level service traffic diversion and differentiated SLA assurance. On top of that, application-side cloud-based resources can exchange information with the transport network. CFN compute-aware routing enables unified scheduling of cloud-network resources to meet new service requirements. To better implement cloud-network coordinated scheduling, the use of innovative technologies such as SRv6 is extended from WANs to ELBs in data centers to provide SRv6-based cloud access.

### 4. MHI

Digital development requires cloud-enabled data services to boost business and data touch points to be distributed throughout office, life, and production scenarios. After more than 20 years of development, IoT has shifted from a collection-oriented non-business-critical service to a control-oriented business-critical service. IoT solutions urgently need to provide high bandwidth, high-density coverage, and low latency.

In the future, we hope to introduce NG-SPE and OFDM technologies without adjusting existing single twisted pairs to upgrade network bandwidth from 100 kbps to 10 Mbps, thereby meeting the backhaul requirements of various onsite videos and reducing deployment costs by 50%. In the Wi-Fi access field, converged access through NFC, BLE, Wi-Fi, and LoRa enables APs to connect to terminals and sensors of various types, reducing complexity and costs. The access density increases from 1K/1000 m<sup>2</sup> to 100K/1000 m<sup>2</sup>, and the access bandwidth increases from kbps to Mbps.

### 5. HRL

By 2030, general-purpose computing power will

increase 10-fold to 3.3 ZFLOPS, AI computing power will increase 500-fold to 105 ZFLOPS, and the annual global data volume will increase 23-fold to 1 YB. Meanwhile, the data center scale will increase by hundreds of times. In the future, ultimate immersive experience will require an E2E motion-to-photon (MTP) latency of less than 10 ms, close to human's motion dizziness-free perception limit. In terms of remote surgery, the control precision of an operation moving at a speed of 1 m/s must be within 5 mm, the E2E latency must be less than 5 ms, and the reliability must be higher than 99.9999%. A growing number of emerging services require networks to provide deterministic experience assurance.

**Large-scale networking:** The innovative dragonfly topology ensures that the number of hops between any servers is the same and the latency is fixed. This prevents unbalanced scheduling caused by the traditional spine-leaf architecture and the resulting loss of computing power. What's more, adaptive routing reduces latency by 30% and shortens fault convergence from 100 ms to 100 ns. This enables an MFLOPS-level computing power pool to be converged within nanoseconds when a fault occurs. In addition, the newly introduced network-level balancing algorithm schedules and distributes DCN traffic in a unified manner, ensuring even traffic distribution and increasing the throughput to over 90%.

**Native SLA-compatible new QoS architecture:** The existing QoS architecture schedules traffic based on queue priorities, first forwarding traffic in queues with higher priorities. This architecture is mainly used to allocate shared resources and is not responsible for service quality. Therefore, there are limitations to SLA assurance, especially latency assurance.

Unlike the existing priority-based scheduling mode, the new QoS architecture quantitatively schedules traffic in an SLA-oriented manner to meet latency, bandwidth, and packet loss rate requirements. Machine learning is used to learn and predict network traffic characteristics in real time. AI inference dynamically and adaptively calls the capabilities of the new QoS architecture to achieve SLA targets through optimal queue scheduling.

**New protocol (DIP):** In a WAN scenario, multiple reachable paths exist between the source and sink nodes on the IP network, and many nodes participate in path computation. DIP needs to provide SLA-constrained topology path selection, node-specific QoS queue allocation, and constraint-based path and resource orchestration. In the future, multi-sensory experience, distributed machine learning, multi-party collaboration, and other applications will involve synchronous collaboration between multiple data flow connections. DIP must provide application/task-oriented multi-connection deterministic collaboration assurance capabilities to achieve the overall QoS objectives of applications/tasks.

**TSN 2.0 deterministic transport:** TSN is further developed for the internal networks of production campuses. By introducing capabilities such as gate scheduling, clock synchronization avoidance, and large-scale network orchestration, TSN can reduce latency from 10 ms to 100  $\mu$ s and orchestrate 1K NEs/10K flows within minutes, meeting digital production requirements.

**User-centric network slicing:** Network slicing is an important transport means of future user networks, and user-centric IP network slicing is an important evolution trend. Network slicing is shifting from providing connection-oriented resource slices to providing new types

of network service slices, such as those for link security, computing power, and data storage. In addition to providing on-demand and flexible customization capabilities, network slicing also supports mobility and real-time and elastic slice management and control.

### 6. Ubiquitous security

With the development of Internet of Everything (IoE), cloud native, and metaverse, the physical and digital worlds are gradually evolving and converging, and network boundaries are continuously extending. On the one hand, security boundaries and exposure surfaces are expanding sharply, while service security requirements are becoming diversified, dynamic, and inclusive. The traditional external security protection system can no longer meet the security requirements of future networks. In the future, security will be built into the very architecture of networks. Intelligent and automated security operations will gradually replace human analysts. And as network boundaries extend, security will become a basic necessity like water, electricity, and computing power.

Intelligent security protection technologies are widely used in the network security field to improve security protection efficiency and effect while significantly cutting costs. Technologies such as intelligent vulnerability discovery, vulnerability exploitation defense, and continuous protection effectiveness evaluation are used to achieve a risk identification rate of 100%. Meanwhile, simulation-based highly adversarial sample detection ensures that the detection rate of new types of APT attacks reaches 99%. The knowledge graph built based on hundreds of millions of malicious example families and distributed AI local self-learning enable the local self-analysis and closed-loop handling

rate to reach 80%. Automatic recommendation of playbook templates and machine-machine collaboration of security semantics automate threat hunting and investigation based on the network security digital map and unified security orchestration bus, improving efficiency 6-fold. Federated learning, differential privacy, and AI local training reduce the transmission and storage costs of threat analysis by 50%. In addition, distributed AI hardware acceleration improves the computing power 5-fold and reduces the total security protection costs by 70%.

Clearly, future networks promise tremendous potential and uncertainties. The entire industry needs to work together to explore these new technologies, move towards Net5.5G, build ubiquitous intelligent IP networks, and connect ubiquitous computing power and intelligent living.




**HUAWEI TECHNOLOGIES CO., LTD.**

Huawei Industrial Base  
Bantian Longgang  
Shenzhen 518129, P.R. China  
Tel: +86-755-28780808  
www.huawei.com



**Trademark Notice**

 HUAWEI , HUAWEI , are trademarks or registered trademarks of Huawei Technologies Co., Ltd.  
Other trademarks, product, service and company names mentioned are the property of their respective owners.

**General Disclaimer**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

**Copyright** © Huawei Technologies Co., Ltd. 2022. 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.