



Intelligent Cloud–Network IT Architecture and Integration White Paper





CONTENTS

01

Cloud Network Development and Challenges

01	1.1 Changes to Operator IP Networks in the Cloud Era
05	1.2 New Challenges Faced by Operators in the Cloud Era
05	1.2.1 Competition from OTT Providers
08	1.2.2 Challenges Relating to Cloud Network Operation Upgrade
12	1.3 Technological Innovations Address Structural Problems
12	1.3.1 Evolution of Intelligent Cloud-Network Technology
14	1.3.2 Vision of Intelligent Cloud-Network Development

02 Architecture and Usage Scenarios of the Intelligent Cloud-Network

17	2.1 IT Architecture of the Intelligent Cloud-Network
17	2.1.1 Overview
19	2.1.2 Target IT Architecture
21	2.1.3 Intelligent Management & Control System: NaaS
23	2.1.4 Next-Generation Cloud Network Operation System: E-commerce Operation
25	2.2 Usage Scenarios of the Intelligent Cloud-Network
25	2.2.1 Pre sales: topology service for cloud product intelligent recommendation
28	2.2.2 In sale: connection service realizes one-stop opening of cloud network service
30	2.2.3 After sales: analysis service to realize tenant self service



CONTENTS

03

Key Technologies in the Intelligent Management & Control System

34	3.1 Key Technologies in the Topology Service
34	3.1.1 Cloud Access Path as a Service
37	3.1.2 Intelligent Cloud Graph Algorithm
41	3.1.3 High-Performance Elastic Control Plane
42	3.2 Key Technologies in the Connection Service
42	3.2.1 Intent-driven Orchestration
44	3.2.2 High-Reliability Configuration Plane
47	3.3 Key Technologies in the Analysis Service
47	3.3.1 Multi-dimensional Cloud Network Visualization
48	3.3.2 Intelligent Assurance
50	3.3.3 Data Plane with Powerful Computing

04 IT Architecture and Integration Ecosystem Construction

52 **4.1 Challenges to IT Architecture and Integration**

53 **4.2 IT Architecture and Integration Lab**

53 4.2.1 Integration Lab Ecosystem Plan

54 4.2.2 Integration Lab Management Process

56 **4.3 IT Architecture and Integration Practices**

05 Summary

57 Summary

06 References

58 References



01 Cloud Network Development and Challenges

||| 1.1 Changes to Operator IP Networks in the Cloud Era

In terms of communication, humanity has evolved from the humble beginnings of smoke signals and drums to the explosion of information currently sweeping the world, and we now find ourselves on the cusp of a new era featuring ubiquitous computing, software-defined everything, and intelligent Internet of Things (IoT). After three industrial revolutions – the first characterized

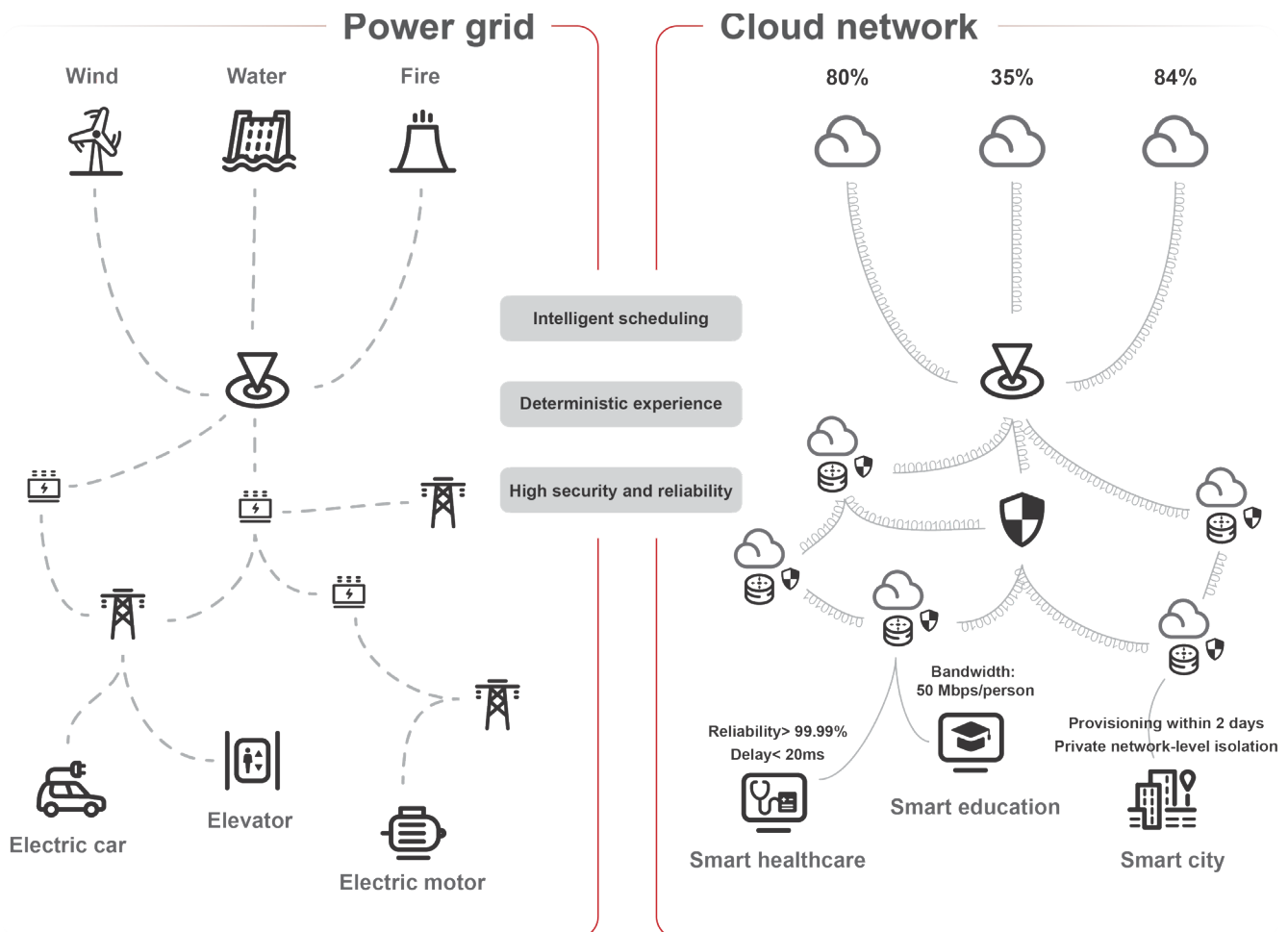


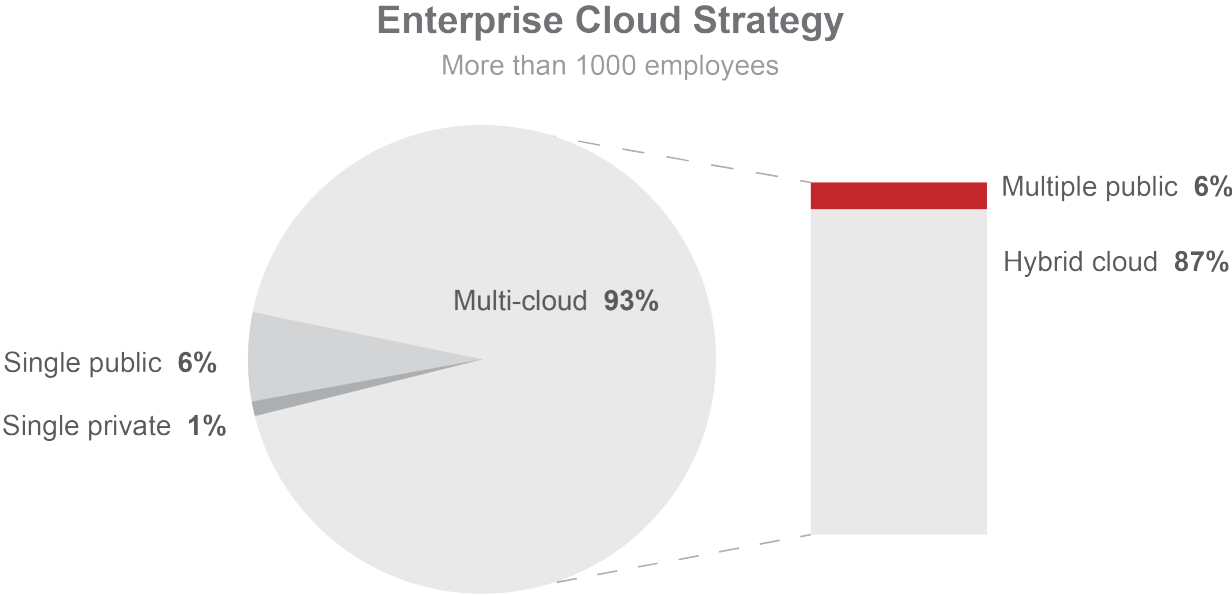
Figure 1-1 Digital impetus created by cloud networks in the fourth industrial revolution

by mechanization thanks to the invention of the steam engine, the second heralded by the invention of electricity, and the third introduced following the invention of computers – we now find ourselves embracing a fourth industrial revolution led by new technologies such as cloud computing, big data, IoT, and artificial intelligence.

Cloud computing forms the core digital impetus in this fourth industrial revolution, providing sufficient intelligence and computing power for the rapidly developing IoT terminals in thousands of industries to extract the required information and knowledge from big data. Similar to the role filled by power grids, cloud networks are now required to transfer the computing power of the cloud to industries around the world.

Fueled by national strategies and digital transformation trends, an increasing number of

enterprises are now migrating their services to the cloud. During its FutureScapes 2020 event, the International Data Corporation (IDC) predicted that 85% of enterprises will have deployed new digital infrastructure in the cloud by 2025. Cloud applications will also evolve from Internet applications, such as portal websites and e-commerce systems, into key information and core production systems. In addition, considering factors such as cloud migration costs, different underlying technologies serving different departments, disaster recovery of data, and asset sovereignty compliance, one cloud alone cannot satisfy all enterprise requirements. Consequently, multi-cloud and hybrid cloud (private cloud + public cloud) are set to become primary strategic choices for enterprises.



Source: Flexera 2020 State of the Cloud Report

In addition, multi-branch cloud has become a mainstream requirement as enterprises continue to

accelerate their digital transformation, with network requirements changing accordingly.

- **Change 1: From "Fast Cloud, Slow Network" to Integrated Cloud-Network Scheduling**

During the early stages of enterprise cloudification, private clouds, industry clouds, and public clouds are predominantly used and automation is implemented in the cloud, providing users with online subscription and out-of-the-box e-commerce experience. During the middle phase, hybrid cloud and multi-branch cloud become the mainstream, requiring cloud access connections to offer the same agility as intra-cloud connections do. However, private line provisioning still requires weeks or even months, which does not meet enterprise cloudification requirements. As such, operators must upgrade traditional networks to intelligent cloud-networks in order to provide e-commerce experience with integrated cloud-network scheduling.

- **Change 2: From "Good Cloud, Poor Network" to Consistent Cloud and Network Experience**

Data centers (DCs) use the simplified spine-leaf architecture to implement one-hop through of traffic between any two hosts, resulting in cloud experiences featuring low latency, non-blocking communication, and guaranteed service-level agreements (SLAs). Information and core production systems are gradually shifted to the cloud as enterprise cloudification enters the middle phase, posing high SLA requirements. For example, the cloudification of information systems requires high bandwidth and deterministic latency, while that of core systems requires ultra-low latency. (The differential protection service of a power grid demands latency of under 2 ms). The last-mile cloudification pattern adopted by the traditional Overlay networks is unable to meet these SLA requirements. Operators must deliver E2E cloud-network SLA assurance and consistent experience to users.

1.2 New Challenges Faced by Operators in the Cloud Era

1.2.1 Competition from OTT Providers

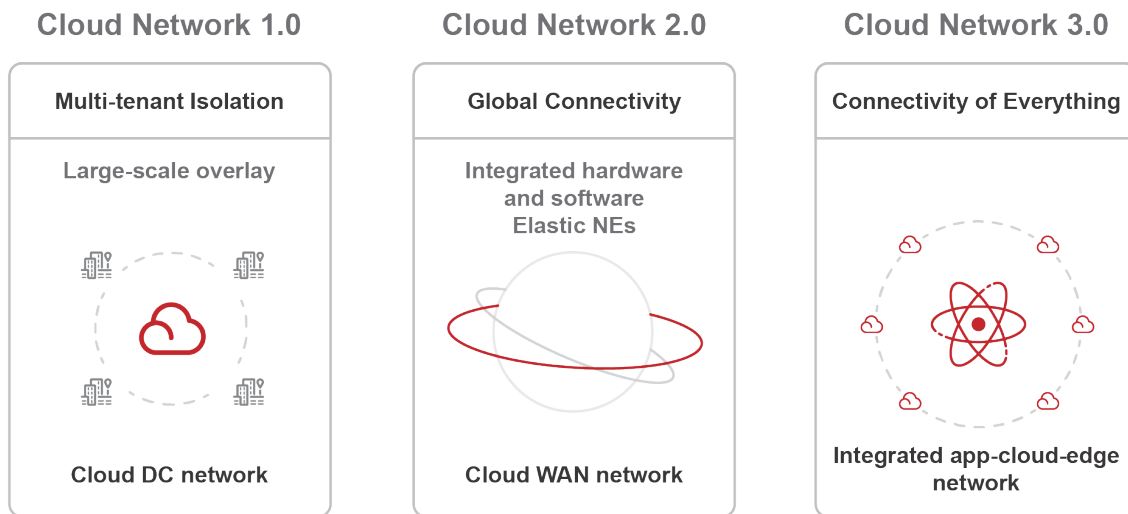


Figure 1-2 Mainstream OTT Cloud Networking Development History

Just as cloud networks have evolved into a cornerstone of the digital economy, so too has enterprise cloudification become an overwhelming trend. Consequently, competitive cloud networks have grown into an essential asset. Over-the-top (OTT) cloud providers are gradually moving from DCs to cloud WANs, with the ultimate goal of building an integrated app-cloud-edge network. In contrast, cloud providers prefer to building their own cloud backbone networks and gradually moving points of presence (POPs) downward into cities. In this regard, cloud providers utilize network virtualization technologies to build a cloud WAN and numerous products such as high-speed inter-cloud interconnection, SD-WAN branch cloudification, and private line cloudification. Meanwhile, with their focus on user experience, OTT providers implement network capabilities as services, empowering cloud WANs with the following cloud features:

- **Real-time provisioning:** Services can be provisioned on a cloud platform in minutes following tenant payment, and a tenant network can be quickly built to support multi-branch and multi-cloud connection.
- **Pay-per-use:** Enterprises pay for the actual traffic they use, allowing them to flexibly purchase bandwidth packages and then allocate or adjust bandwidth among sites in real time.
- **Self-service:** Tenants can perform all operations on a cloud platform, including service provisioning, network O&M, and real-time network quality querying.

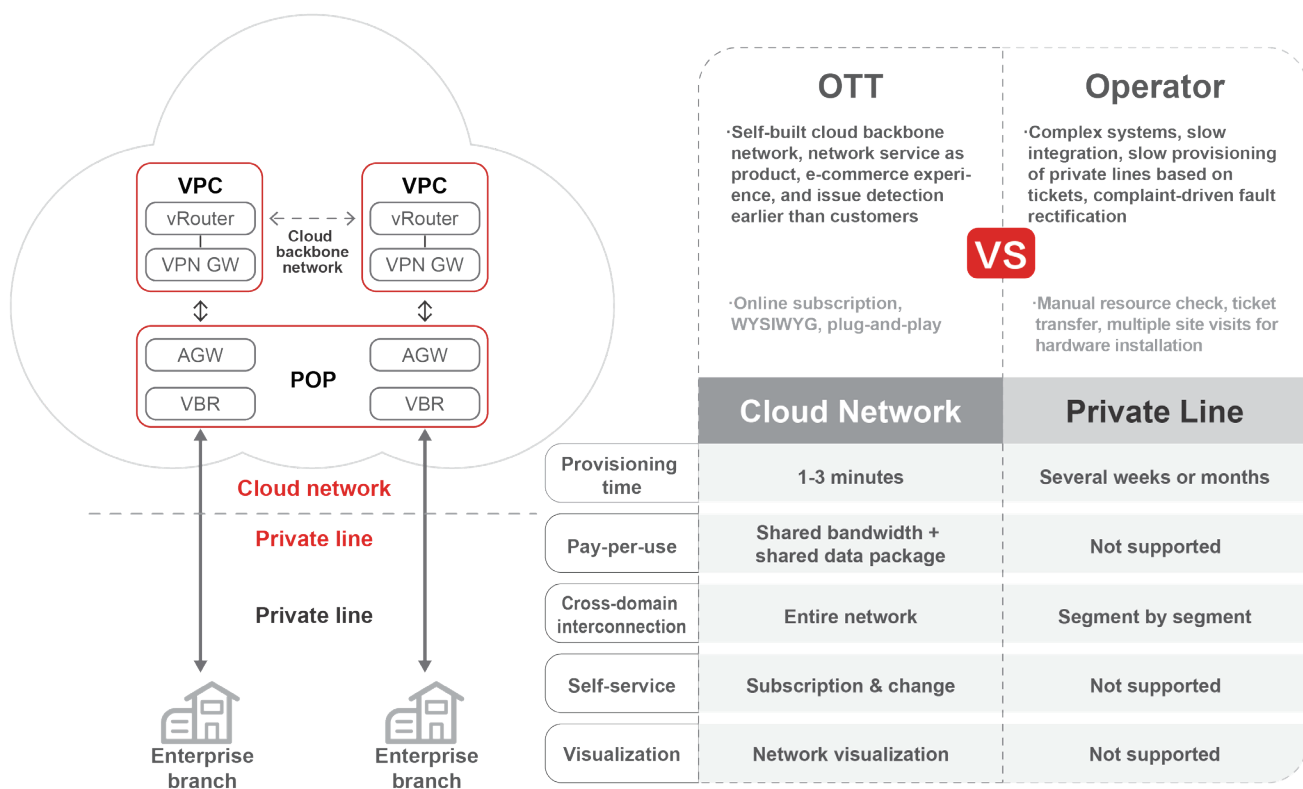


Figure 1-3 Comparison between OTT cloud networks and operator private lines

Compared with the online subscription option available in OTT cloud network products, the current experience offered by operator private line products is less than ideal.



Pre-sales: Cloud-network resources are invisible, and operators are unable to guarantee SLAs.

Upon receiving a customer's order from a service subscription platform, account managers are limited to using an inventory system when querying network resources (such as access devices and fibers) at the customer's location. However, this approach cannot accurately estimate service provisioning durations or appropriately evaluate service latency and quality. Consequently, account managers avoid guaranteeing SLAs in contracts, and network latency cannot be monetized.



In-sales: Due to restrictions on ticket transfers and manual cooperation, service provisioning typically requires more than a month.

After a customer signs a private line contract, a service provisioning system will distribute tickets. Related processes including resource check and design, pipeline construction, device purchase and installation, data configuration, and service commissioning are all completed manually and in a serial manner. As such, almost two months are required to provision a simple cross-province private line, which is unacceptable to enterprises targeting cloudification. As operators lack agile cloudification capabilities, potential enterprise customers tend to gravitate towards OTT vendors or startup companies whose SD-WAN solutions can implement such services, albeit at the cost of SLA assurance in the last mile.

After-sales: Service blocking occasionally occurs, and E2E service quality is invisible.



Once services have been provisioned to customers, the contract fulfillment phase begins. Currently, operators have no E2E integrated cloud network operation platform – their O&M pattern is still layer-, segment-, and profession-specific. If customer services are blocked or have deteriorated, they cannot determine whether the root cause lies within their own systems or within the private lines of operators, leading to a large number of customer complaints as they attempt to resolve the issue. On the operator side, the layer-, segment-, and profession-specific maintenance pattern requires multi-person collaboration, resulting in low locating efficiency and poor customer experience.

Facing competition from OTT providers, operators will lose any traffic-related advantages in the cloud era if they fail to deliver superior product experience to customers by upgrading their cloud network operation systems. Leveraging SD-WAN technology, OTT providers divert traffic to the POP on their self-built cloud backbone network in close proximity. Tenants only need to purchase bandwidth packages for flexible cross-region interconnection. Ultimately, traffic will be gradually pulled away from operator backbone networks, and traditional operator private line services will be confined to the last mile. As a result, the upgrade of cloud network operations has become an urgent task for operators in the cloud era.

1.2.2 Challenges Relating to Cloud Network Operation Upgrade

Compared with OTT providers, operators face greater challenges with regard to the upgrade of cloud network operations. First, operator networks are now even larger and more complex at

the network layer. To provide tenants with quality-guaranteed virtual networks, operators must overcome a host of technical challenges. Second, traditional operation habits are network-centric, with many processes driven by tickets and involving human intervention. As such, it is difficult to clear process breakpoints and achieve machine-machine interface automation. Last but not least, the cloud network operation ecosystem faces challenges relating to excessive BSS, OSS, and controller vendors, a lack of integration standards and specifications, and interface customization among systems, all of which leads to difficult system integration and slow service rollout.

While some operators today have taken the lead by exploring automatic cloud network operations, their IT systems still adopt the industry paradigm of domain-based management

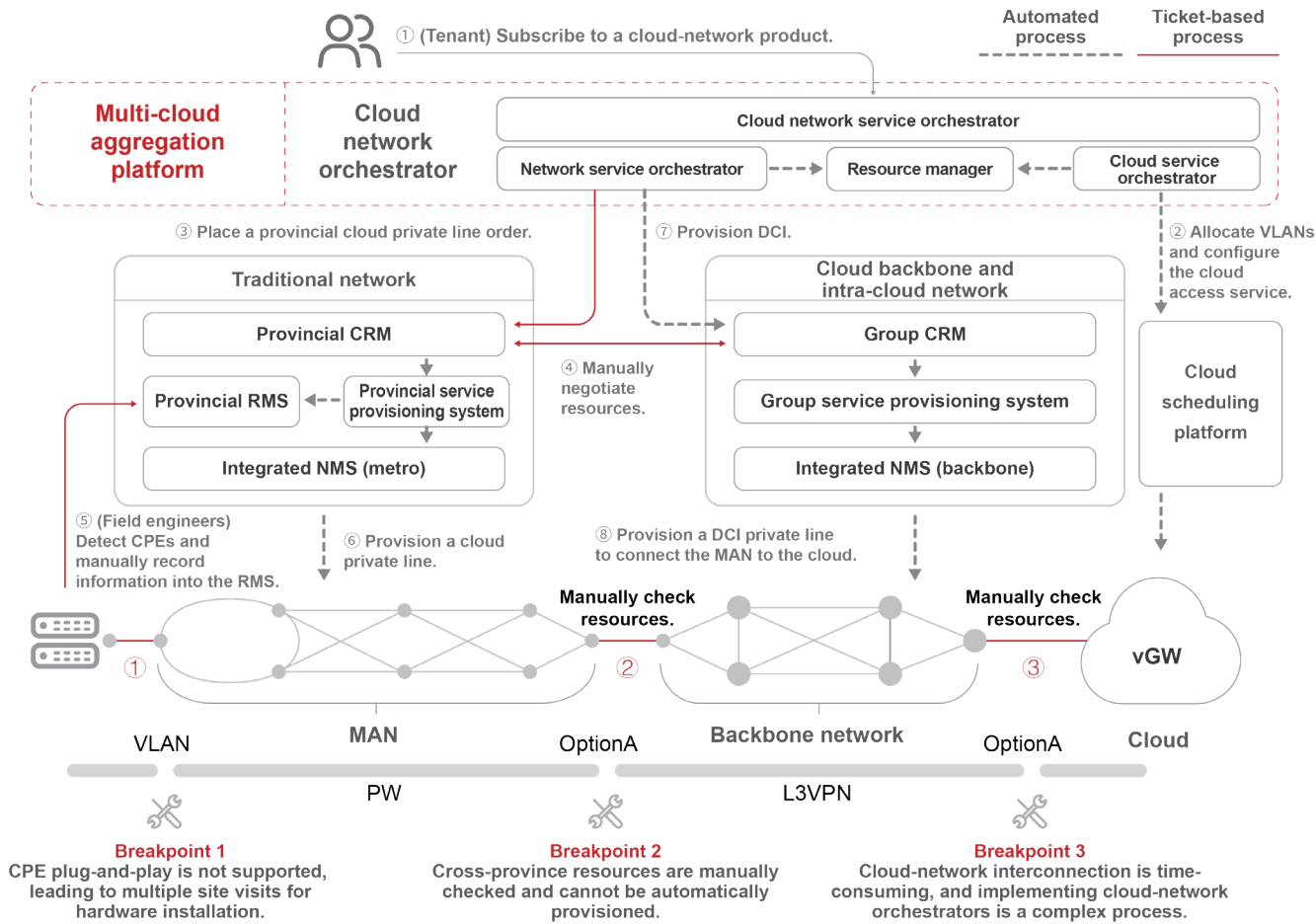


Figure 1-4 Breakpoints in operator IT system integration

and hierarchical collaboration. This leads to some difficulties and breakpoints during system integration and operations.

● **Breakpoint 1: No real-time resource management system (RMS) is available, CPE data is manually recorded, and hardware installation requires multiple site visits.**

Currently, the service activation system involves three major components: resource management, service provisioning, and network management. The service provisioning component first invokes RMS interfaces to map the 9-level addresses in the physical world to NE IDs, and then invokes the northbound interfaces (NBIs) of the network management system (NMS) to provision services. The NMS is responsible for VPN and tunnel configuration for NEs.

The numerous components of the activation system lead to a complex cooperation process and a high degree of coupling, requiring hardware installation engineers to visit the site multiple times. After installing CPEs, they need to manually enter CPE information on the RMS to activate services. Once activated, hardware installation engineers must visit the site again to verify the provisioned services. Any error in CPE information will lead to service activation failure.

Given the above challenges, upgrading the entire system to an install-and-provision experience is a daunting task. Automatically detecting online CPEs requires the use of machine-to-machine interfaces between the RMS and the NMS. However, the RMS is an offline system in the traditional process and

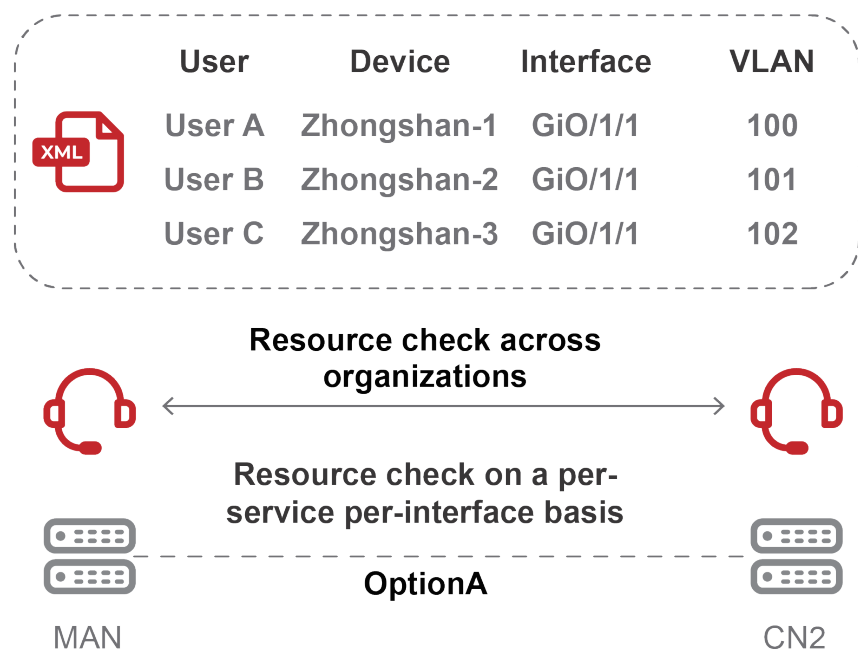


Figure 1-5 Cross-region concatenation of service VPNs

expensive to reconstruct as an online system. If the RMS cannot be reconstructed, automation cannot truly be achieved.

● **Breakpoint 2: Service VPNs are concatenated across provinces and resources are manually coordinated, making private line automation a tricky prospect.**

As operators traditionally build and manage networks by region, provisioning a cross-province service usually requires the concatenation of multiple VPN segments. While the responsibility matrix is clear among O&M teams, this pattern involves some fatal disadvantages:

○ **Network-service coupling:** A large number of tenant-level VPN configurations exist on border devices, and they are difficult to maintain.

○ **Challenging private line automation:** Management systems resort to manual resource checks due to complicated physical-virtual mapping and an inability to obtain cross-domain link information, making it extremely difficult to plan resource allocation for each service and interface.

Consequently, service provisioning across multiple management domains relies on tickets and manual cooperation, and can require up to two months to provision a simple cross-province private line.

● **Breakpoint 3: Cloud-network interconnection is time-consuming, and implementing cloud-network orchestrators is a complex process.**

Some operators focus on multi-cloud connection business scenarios, building cloud backbone networks and introducing a multi-cloud aggregation platform to provide tenants with VPC interoperability services across cloud providers. Essentially, as cloud backbone and DC networks both use the VPN concatenation mode, the multi-cloud aggregation platform must possess cloud network orchestration capabilities, while physical interfaces and VLAN resources must be planned for cloud-network interconnection in advance. When tenants apply for VPCs and cloud access private lines online, the multi-cloud aggregation platform automatically allocates idle physical

interfaces and VLAN resources and provisions VPCs and cloud access private lines.

Today, cloud-network interconnection is a complex process, and the implementation of cloud-network orchestrators is fraught with difficulties. One of the main reasons relates to the interconnection of cloud-network orchestrators with NMSs through network-level interfaces, which expose all the network's technical details to the cloud-network orchestrators. As network-level interfaces include tens of thousands of parameters, system integration necessitates large workloads and frequent communication among engineers. If individual engineers possess differing understandings of interface parameters, cloud-network interconnection will fail, altering the interconnection process. Consequently, system integration currently requires an average of six months. On the other hand, the cloud platform provides just dozens of VPC API parameters – VPC APIs are service-oriented interfaces that shield technical details, ensuring fast interconnection between the multi-cloud aggregation platform and the cloud platform. To achieve a consistent cloud and network experience and accelerate IT system integration, the network side must upgrade to service-oriented interface interconnection.

||| 1.3 Technological Innovations Address Structural Problems

1.3.1 Evolution of Intelligent Cloud-Network Technology

DC networks were the first to successfully implement service automation and e-commerce operations, enabling operators to learn the following in terms of technology selection:



Simplified network: The simplified spine-leaf networking is introduced to performance-optimized DCs (PODs) in order to build a non-blocking, highly reliable, auto-scaling, and easy-to-maintain infrastructure.



Simplified protocol: The virtual extensible local area network (VXLAN) protocol is introduced to implement any-to-any connectivity in DCs, simplifying tenant network model design and avoiding VPN concatenation.



Simplified interface: As the tenant network model is simplified, the cloud platform can easily abstract service-oriented VPC APIs to shield network implementation details and facilitate the integration of the multi-cloud aggregation platform.

Compared with DC networks, operator WANs are larger in scale and involve more complex networking, requiring both agile connections and guaranteed SLAs, and driving the introduction of innovative technologies. SRv6-based intelligent management & control is the key enabler for intelligent operator cloud networks, and the following are some vital technologies:



Cloud access path as a service: SRv6 BSID-as-a-service technology is used to pool resources on complex WANs and reconstruct irregular physical topologies into a standard spine-leaf virtual simplified infrastructure that uses BSID as virtual links. The centralized path computation and closed-loop autonomy capabilities of the intelligent management & control system help guarantee BSID SLAs, forming a non-blocking virtual simplified network with high reliability and deterministic latency.



SRv6 one-hop through: SRv6 paths are orchestratable, enabling one-hop through between any two nodes and one hop to cloud from CPEs. In this way, the tenant network model is simplified and VPN concatenation is no longer required.



Network as a service (NaaS): As SRv6 one-hop through simplifies the tenant network model, intelligent management & control systems can implement scenario-specific service-oriented NBIs, shield technical details, and simplify the integration of upper-layer cloud network operation systems.

To summarize, technological innovations bring new hope to operator cloud networks. OTT providers have clouds but not networks, while operators possess both. In addition, operators boast another natural advantage – wide coverage on the last-mile network. Consequently, operators need only improve cloud network operations in order to achieve greater success in the cloud era given their inherent network advantages.

1.3.2 Vision of Intelligent Cloud-Network Development

Cloud networks – networks that connect and enable clouds – have become the foundation of the digital economy. To date, over 50 countries have formulated digital strategies and plans related to such networks, and building a new cloud-oriented service network has become an inevitable trend for operators. Distinct from traditional networks, cloud networks must meet cloud requirements for the network. Taking China Telecom as an example, its Technical White Paper on Cloud-Network Convergence in 2030 divides cloud requirements for the network into five categories: network performance, network availability, network intelligence, flexible adaptation,

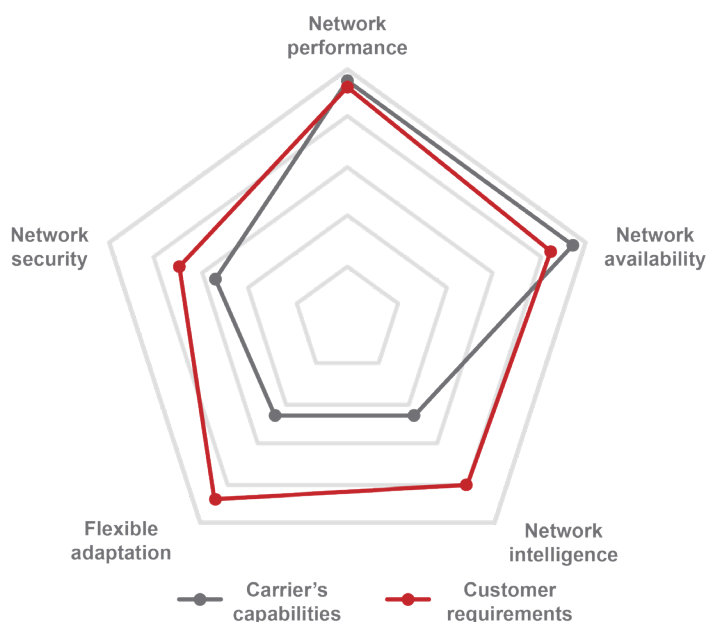
and network security.

As illustrated by this figure, the largest gaps between operator networks and cloud requirements lie in flexible adaptation and network intelligence. To put it another way, the invocation speed of network services is far behind cloud requirements.

iMaster NCE is committed to becoming the core enabling engine of the intelligent cloud-network and helping operators improve cloud network operations. First, it increases network responsiveness to the

cloud, ensuring integrated cloud and network scheduling. Second, it fully exploits the wide coverage of operator networks to provide cloud access connections with guaranteed SLAs and deliver consistent cloud and network experience. Third, enterprise users can enjoy one-stop subscription of cloud network products and comprehensive e-commerce service experience. Through its new "five-ones" capabilities (one hop to cloud, one-network wide connection, one-click fast scheduling, one fiber for multiple purposes, and one-stop integrated security), Huawei aims to maximize the value of operator network resources and fully leverage the complementary advantages of clouds and networks, laying the foundation for operators to provide DICT services capable of integrating clouds and networks.

Cloud requirements on the network



Source: Technical White Paper on Cloud-Network Convergence in 2030 by China Telecom

One hop to cloud

SRv6 cloud access paths streamline cross-domain connections. Thanks to such groundbreaking technologies, it is no longer difficult to configure cross-domain connections manually, and services can access clouds through a single network within minutes.

One-network wide connection

Through the NaaS architecture, networks can be used as conveniently as clouds, providing tenant-level interfaces to shield network implementation details and reducing system integration time by 90%. Thanks to intelligent distributed path computation, ultra-large networking and massive tenant interconnection are achieved.

One-click fast scheduling

Combining network and cloud factors, the intelligent cloud graph algorithm provides optimal cloud access paths for enterprises and enables integrated scheduling of cloud and network resources, contributing a 30% increase in cloud and network resource usage.

One fiber for multiple purposes

Hierarchical slicing provides deterministic service experience for thousands of industries, meeting such varied SLA requirements as enterprise video surveillance, office system cloudification, and teleconferencing. One fiber can connect to different private network slices to provide fine-grained experience assurance.

**One fiber for multiple purposes
One-stop integrated security**

Comprehensive cloud-network-security defense capabilities facilitate the detection of hidden attacks within minutes and near-source blocking of threats, delivering convenient security services to users.



02 IT Architecture and Usage Scenarios of the Intelligent Cloud-Network

2.1 IT Architecture of the Intelligent Cloud-Network

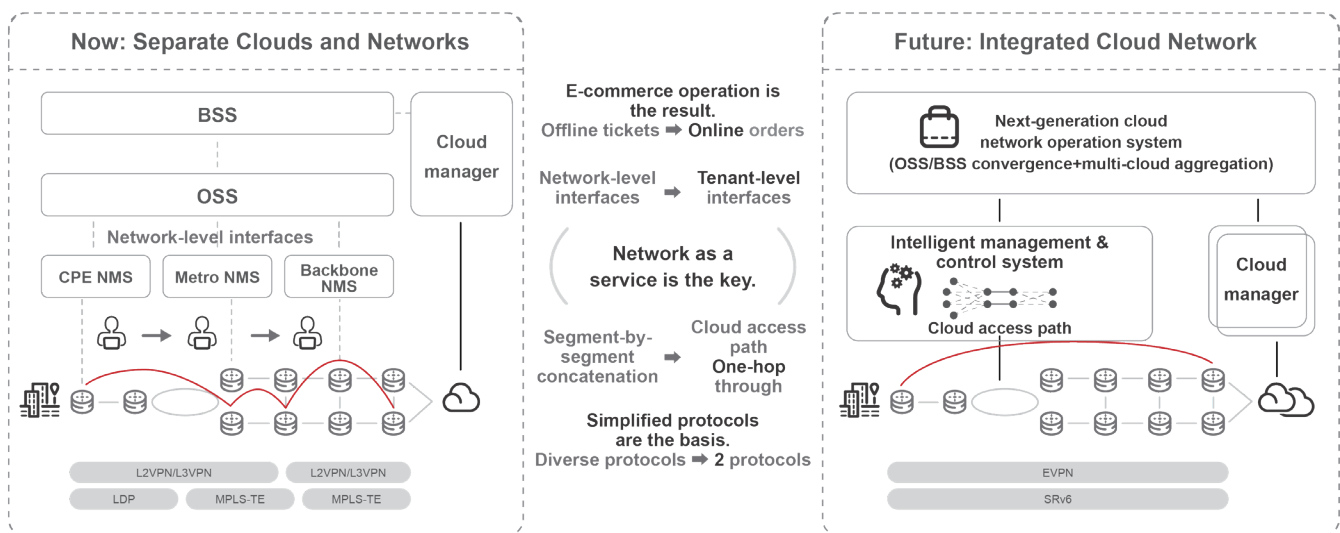



Figure 2-1 Architecture of the intelligent cloud-network

2.1.1 Overview

Driven by the need for smart operations, separate clouds and networks must be integrated into a single cloud network. This leads to transformation of technologies at the following layers:


Network infrastructure layer: Simplified protocols are the basis.



Traditional network protocol technologies are complicated. For example, a diverse range of tunnels are available – LDP, MPLS-TE, and BGP-LSP – and each type cannot be independently established across domains. This in turn leads to various VPN concatenation technologies, including VLL, VPLS, and L3VPN. In addition, networks and services are coupled, involving a high number of configurations on network devices. This all leads to complex maintenance and automation.

The intelligent cloud-network integrates traditional complex protocols into two simplified alternatives: EVPN and SRv6. SRv6 is a next-generation SDN network enabling protocol which helps intelligent management & control systems achieve centralized path computation and cross-domain one-hop through while avoiding VPN concatenation.

Intelligent management & control layer: NaaS is the key.



Conventional NMSs use network-level interfaces to interconnect with an OSS, but this results in complex integration involving thousands of parameters and exposes technical details of the network to the OSS. Furthermore, the OSS needs to manage multiple NMSs and support cross-domain VPN orchestration due to the limited management capacities of conventional NMSs, which increases the difficulty of OSS development.

The intelligent cloud-network introduces an intelligent management & control system which utilizes NaaS technology to provide tenant-level service-oriented interfaces for the OSS, while also shielding technical details relating to the network. Tenant network provisioning and adjustment can be completed with fewer than 100 parameters, greatly simplifying OSS integration.

Network operation layer: E-commerce operation is the result.

The BSS only automates tickets on traditional networks, with service provisioning still relying on manual operations. Consequently, e-commerce shopping experience cannot be delivered throughout the pre-sales, in-sales, and after-sales processes.

In the intelligent cloud-network era, a next-generation cloud network operation system is required to integrate conventional OSS and BSS functions and offer the multi-cloud aggregation function. This system will invoke the network service capabilities of the intelligent management & control layer through service-oriented interfaces, while one-stop subscription to cloud-network products will provide tenants with an ideal e-commerce shopping experience.



2.1.2 Target IT Architecture

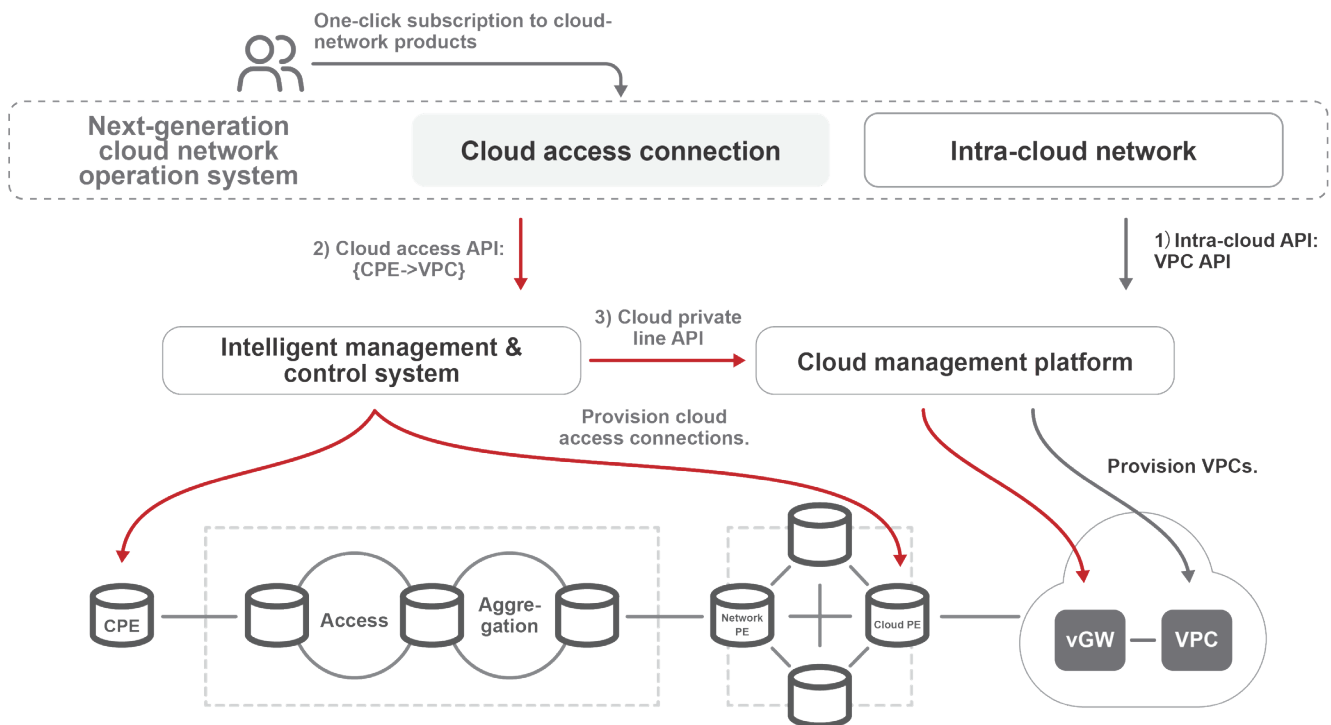


Figure 2-2 Target IT architecture of the intelligent cloud-network

In the above figure, the target IT architecture of the intelligent cloud-network is built on the following principle: The intelligent management & control layer leverages NaaS technology to provide interconnection interfaces with simplified parameters, shielding network implementation details, while the cloud network operation layer focuses on providing tenants with subscription to cloud-network products and e-commerce experience. The intelligent management & control layer offers the following service-oriented interfaces:

- **Cloud management platform: intra-cloud API and cloud private line API**



Intra-cloud API: provisions dedicated virtual private clouds (VPCs) consisting of virtual switches and routers for tenants. After the next-generation cloud network operation system invokes this API, the cloud management platform automatically configures virtual switches, virtual routers, cloud servers, and other related components to generate a dedicated subnet.



Cloud private line API: provisions cloud access private lines for tenants. After this API is invoked, the cloud management platform creates virtual border routers and configures VPNs for them. As a cloud access private line product, this API enables cloud-network interconnection. It is also a service-oriented interface that enables one-segment connection within clouds.

● **Intelligent management & control system: cloud access API**

Cloud access API: provisions cloud access private lines or networks for tenants. After this API is invoked, the intelligent management & control system automatically establish cloud access connections between CPEs and VPCs as well as multi-cloud connections between VPCs, based on the cloud access intent of tenants. This API is also capable of product recommendation based on latency estimation in the pre-sales phase, and connection O&M and fault diagnosis in the after-sales phase.



2.1.3 Intelligent Management & Control System: NaaS

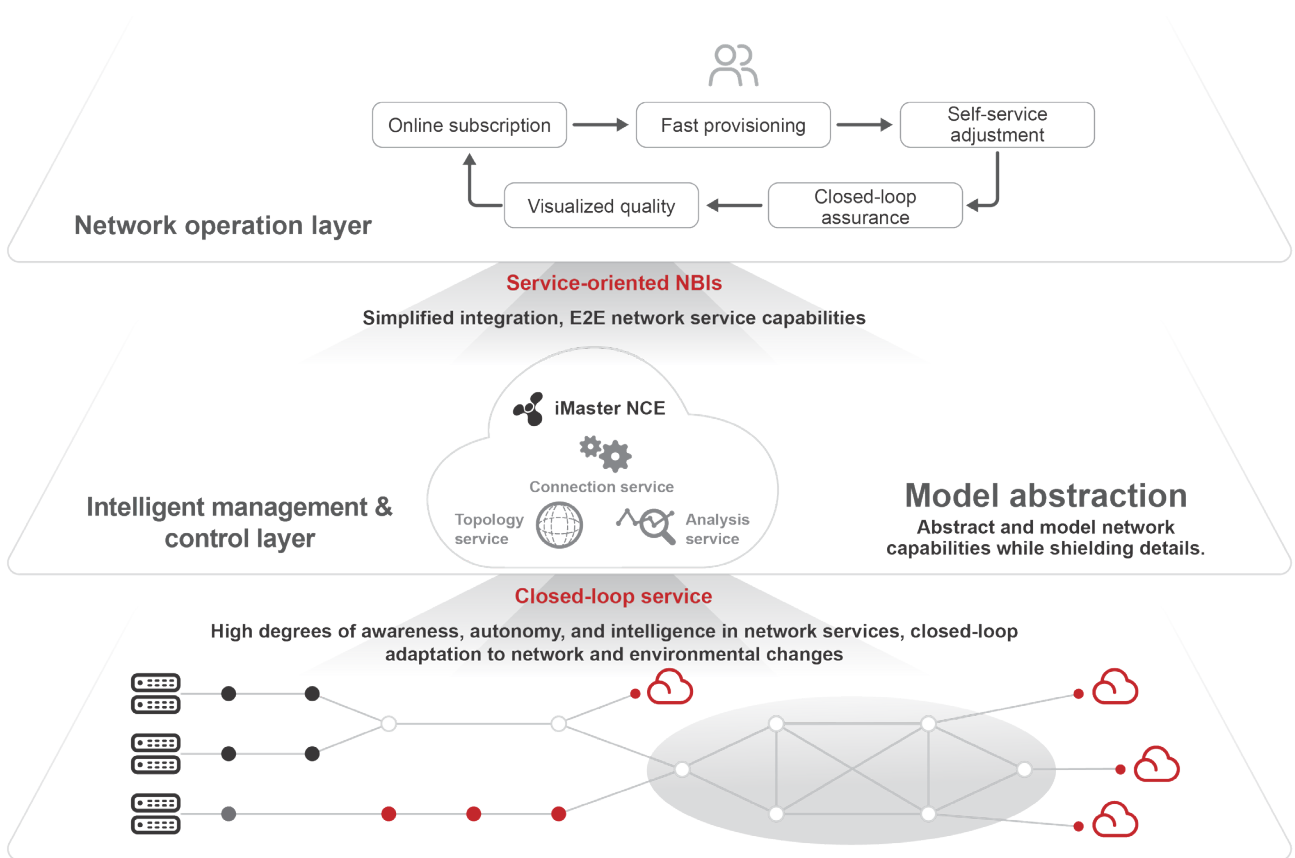


Figure 2-3 Intelligent management & control system – iMaster NCE

Positioned as an intelligent management & control system, iMaster NCE aims to become the core enabling engine of the intelligent cloud-network with the help of NaaS technology.

NaaS has three core functions:

- **Model abstraction:** abstracts and models network capabilities while shielding network implementation technologies. Network functions are defined as service modules that can be flexibly invoked and used on demand.
- **Closed-loop service:** Network services are continuously provided, and network device and service statuses are detected in real time. In light of exceptions in the service execution phase, policy-based self-decision making and intelligent repair recommendation capabilities are offered, which embody network intelligence and autonomy.
- **Service-oriented NBI:** Simplified NBIs focus on describing the functions of network services instead of network implementation details.

iMaster NCE provides three major network services:



Topology service: This is a core service provided by iMaster NCE for cloud network scenarios, supporting real-time network topology awareness, centralized path computation, and one-hop through. Other value-added functions include real-time network resource check and estimation as well as intelligent recommendation of cloud-network products.



Connection service: This service provides interfaces oriented to tenant network connection models to implement CPE plug-and-play, install-and-provision, as well as provision-and-test. This eliminates the need for real-time RMS reconstruction and multiple site visits for hardware installation that typically occur in the traditional network integration mode.



Analysis service: This service provides multi-dimensional and multi-layer quality analysis and fault diagnosis for tenants and network O&M personnel, while also visualizing the connection quality on tenant networks and supporting self-service diagnosis. For network operation centers (NOCs), proactive network fault awareness, analysis, and closure are supported.

These three services can be flexibly invoked and combined by the cloud network operation system on demand. From a hierarchical perspective, the connection service resides at the top layer and relies on topology and analysis services for flexible orchestration and combination. Together, they offer simplified tenant model-oriented interfaces to next-generation operation systems while completely shielding network technologies such as VPN, tunnel, and slicing. The involvement of fewer than 100 parameters greatly accelerates system integration.

2.1.4 Next-Generation Cloud Network Operation System: E-commerce Operation

In the IT architecture of the intelligent cloud-network, the next-generation cloud network operation system focuses on user-facing products and customer-facing service (CFS) functions, resource facing-service (RFS) functions are implemented by the intelligent management & control system and cloud platform, and NaaS interfaces are used for interconnection. In its entirety, this architecture benefits end users with integrated cloud-network operations and e-commerce experience.

In addition to conventional BSS/OSS functions, the next-generation cloud network operation system offers multi-cloud aggregation, cloud access connection, and other tenant portals related to cloud-network products. The OSS is no longer aware of network technologies, and instead retains only the tenant models of cloud-network products and interconnects with the intelligent

management & control layer through service-oriented interfaces. The overall functional modules can be classified as follows:



User management: provides functions such as tenant account management, online account creation, authentication, and rights- and domain-based management.



Product subscription: allows tenants to subscribe to cloud-network products online, manage orders, and approve processes.



Charging management: provides fee calculation and trend analysis for cloud-network products.



Product console: provides a portal for tenants to subscribe to cloud-network products online and monitor their status.

The above modules represent the primary products and CFS functions provided by the BSS. In contrast, the following OSS functions are not concerned with technical details and use NaaS capabilities directly at the intelligent management & control layer.

- **Intra-cloud product orchestration:** invokes the VPC APIs of the cloud platform to provision intra-cloud products based on tenants.
- **Cloud access product orchestration:** invokes the cloud access API of the intelligent management & control system to provision cloud access products based on tenants.

○ **Hardware installation management:** provides an online ticket system to manage the hardware installation process that relies on manual operations.

||| 2.2 Usage Scenarios of the Intelligent Cloud-Network

The following describes how the NaaS capability of the intelligent management & control system supports the next-generation cloud network operation system and provides pre-sales, in-sales, and after-sales functions and experience for end users.

2.2.1 Pre-sales: topology service for cloud product intelligent recommendation

In the pre-sales phase, iMaster NCE provides the underlay and overlay topology services for online check and real-time visualization of network resources. The optimal network path is located based on the enterprise branch location and cloud pool resources. Various optional cloud-network security packages are provided based on tenant SLA requirements, with support for one-stop subscription included.

○ **Underlay topology service:** Based on the network topology, the controller enables multi-factor (including latency, bandwidth, and hop count) path computation, fault-triggered path recomputation, and network reoptimization. The implementation of these service features depends on real-time topology change awareness and timely service path restoration, as well as real-time awareness of link bandwidth, latency, and tunnel traffic and precise optimization for network load balancing. As a result, the BGP-LS and Telemetry protocols are introduced between the controller and devices to report link information and collect link and tunnel quality information, respectively. BGP-LS, a link status collection protocol defined by IETF, uses the BGP mechanism to quickly flood link status routing information and is more agile and reliable

than Netconf. Telemetry enables fast and efficient data collection within seconds.

○ **Overlay topology service:** The overlay topology is a Spine-Leaf architecture-based logical topology derived from the underlay topology. The NEs in this topology include ABRs or ASBRs, and the links are SRv6 Policy tunnels, which are identified by BSIDs and carry the latency attribute. These links can be automatically optimized through the underlay topology service. Thanks to the "API as a service" capability of the overlay topology, only BSID identification and orchestration is required during service creation in order to meet SLA requirements, facilitating flexible and on-demand invoking of cloud applications. As such, fast and simplified building is a key feature of the overlay topology service. In this regard, the controller enables tunnel group planning to support the one-click creation of SRv6 Policy tunnels in batches, and implements a fully automated process for BSID allocation, tunnel latency collection, and overlay topology building.

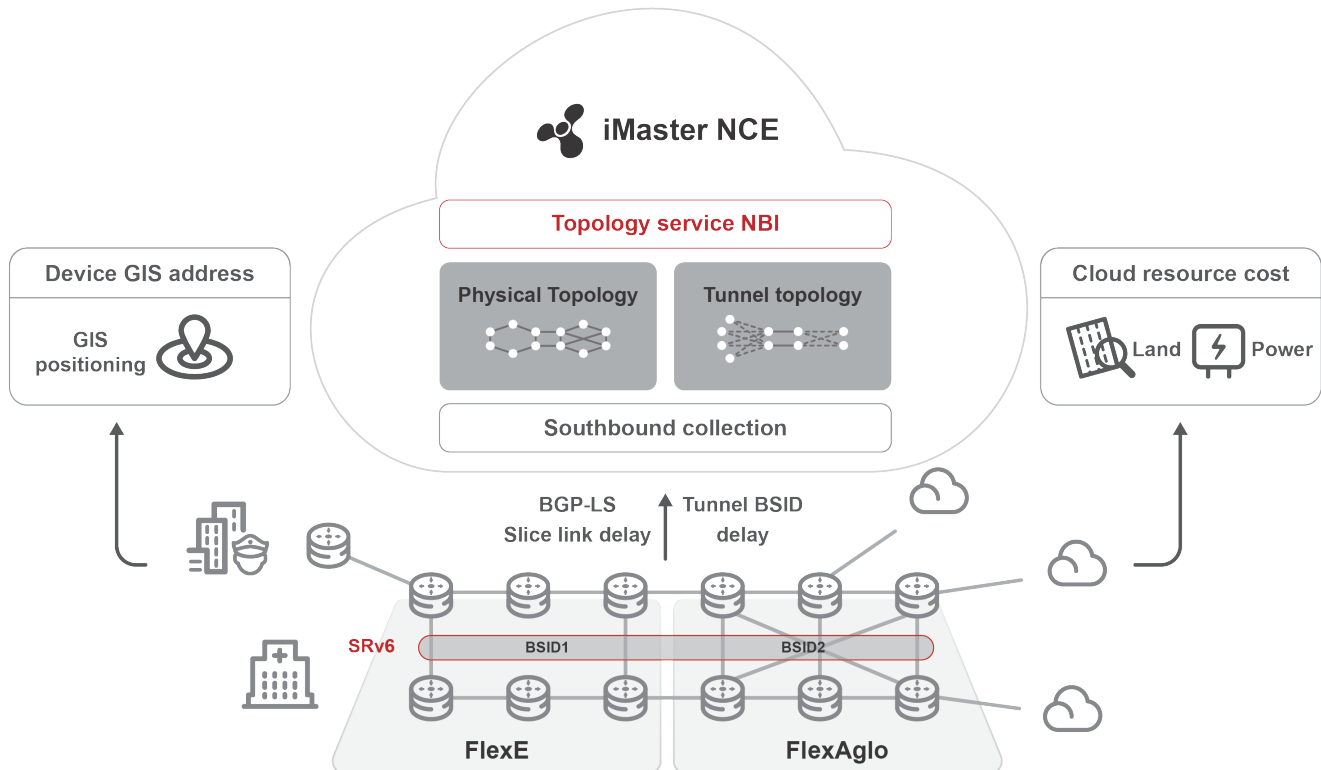


Figure 2-4 iMaster NCE Topology Service

With these topology services, operators can provide various cloud-network products on their operations portals:

Recommended latency circles and cloud pools in packages. Based on the enterprise branch, cloud pool, and CPE access locations, the management and control system can recommend latency for cloud services, as well as suitable cloud pools and network paths based on constraints such as cost, bandwidth, and reliability.

Recommended packages based on cloud-network products, similar to the varying service tiers offered by taxi-hailing applications. This approach helps monetize differentiated capabilities such as network latency, bandwidth, and reliability, and provides services with different SLA levels for enterprise customers.



2.2.2 In-sales: connection service realizes one-stop opening of cloud network service

iMaster NCE provides one-stop provisioning of cloud-network services and visualizes the entire order process for in-sales scenarios. Operators can deeply integrate iMaster NCE into their OSS and BSS domain systems through connection services such as service subscription, provisioning, and rate adjustment interfaces.

○ The service subscription interface is a highly simplified and intent-oriented SBI that allows OSS and BSS domains to focus on business design and product definitions, instead of network parameters. The following figure shows how this interface simplifies network parameters.

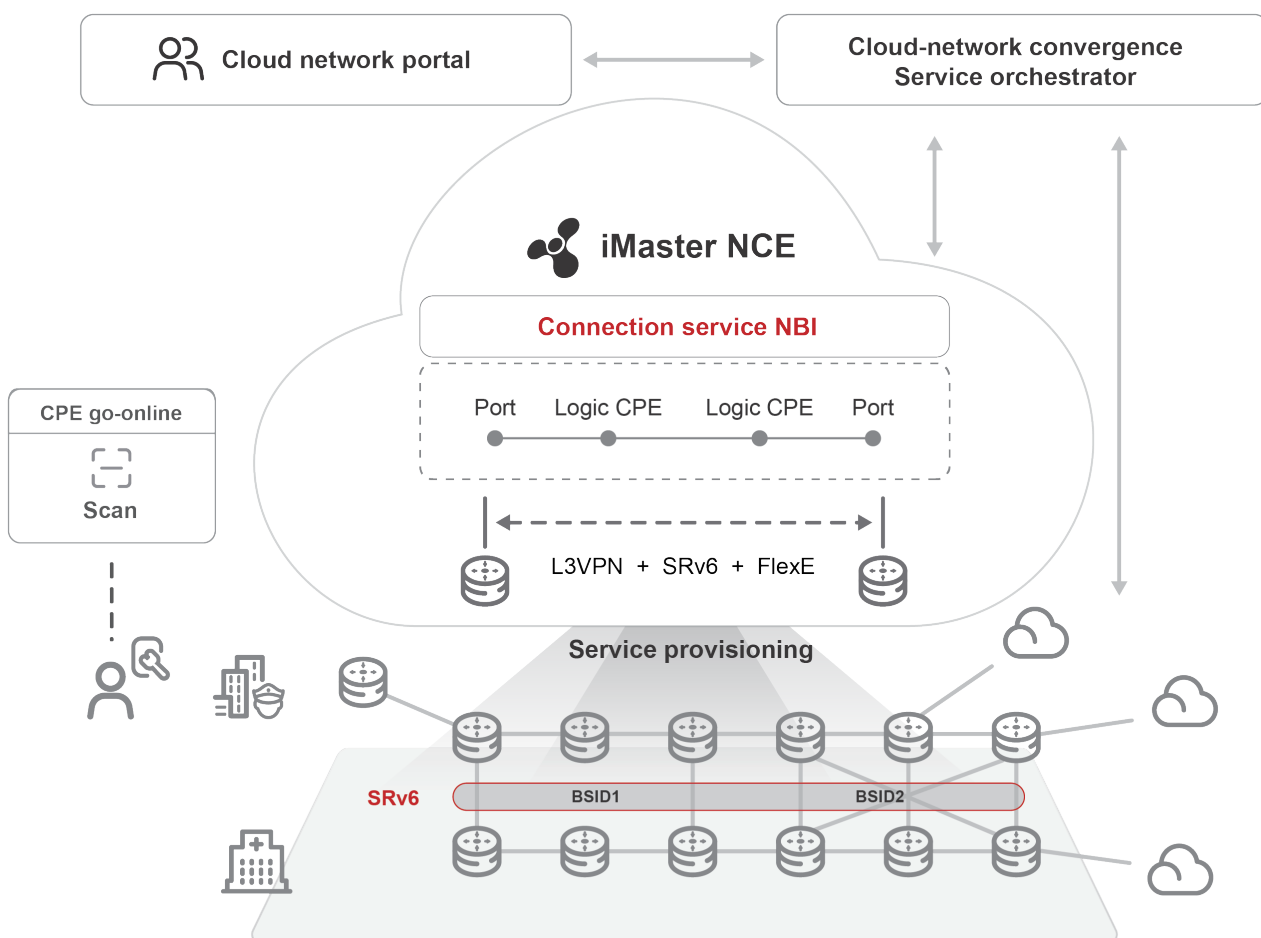


Figure 2-5 iMaster NCE Connection service

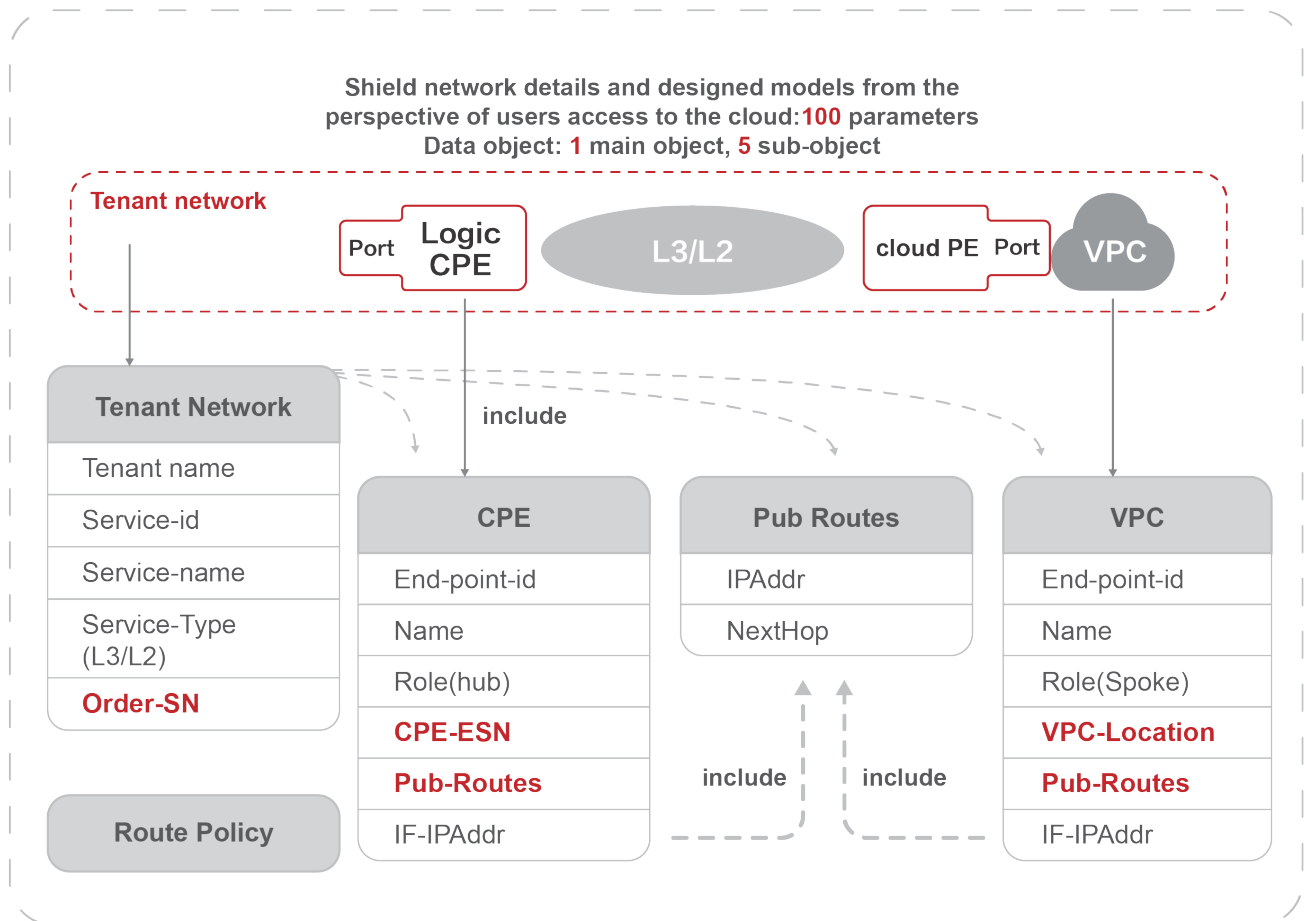


Figure 2-6 Simplified comparison of network parameters

As shown in this figure, the service subscription interface considers a cloud-network service as a large object (tenant network) with five sub-objects (offline site and interface, cloud site and interface, and VPC). Each object defines only service intents. The key to this simplified interface is building-block service orchestration. The management and control system provides basic service models (based on pre-existing definitions of cloud-network products) for quick creation of E2E service implementation logic, while maintaining a simplified interface for external access. The management and control system also has preset VPC access capabilities for different cloud pools to automatically match cloud resources and decompose configurations.

- The service provisioning interface enables automatic service provisioning based on PnP CPEs. This interface is applicable to scenarios where no CPEs are available during service subscription, and is designed to simplify the process for bringing CPEs online, automatically

identify online CPEs, and quickly provision a service. This SBI significantly expedites service provisioning in contrast to the conventional ticket transfer process and facilitates the prediction of the service provisioning time in OSS and BSS domains.

This interface features two key capabilities: simple service provisioning through a CPE QR code and service simulation verification. Field engineers can use an app to scan the CPE QR code on site, eliminating the need for NOC attendance. QR code scanning enables iMaster-NCE to automatically manage CPEs, perform dialing tests on optical fibers, and deliver basic configurations. Once the CPE is online, tenant service data can be automatically matched during service simulation, and path computation simulation is performed to confirm user satisfaction of service quality and to deliver service data from end-to-end.

- The service rate adjustment interface is designed based on the simplified service subscription interface to adjust the service rate per tenant, automatically limiting service rates and adjusting network path resources.

These connection service interfaces are designed for service subscription, provisioning, and adjustment. The information regarding the processes for invoking these interfaces can be sent to OSS and BSS domains in a prompt manner, facilitating the visualization of service provisioning.

2.2.3 After-sales: analysis service to realize tenant self service

Conventional solutions for IP network maintenance mode feature poor service quality awareness, difficult service fault locating, and time-consuming service recovery. To address these issues, the network analysis service implements "seconds-level" performance data collection, iFIT, intelligent, and big data technologies to make cloud-network services intelligent and visualize SLA information of these services in real time, such as bandwidth and latency.

In addition to conventional proactive network maintenance by operators, service SLA

visualization, management, and assurance on the tenant side are key to fulfilling operator contracts under cloud-network convergence. iMaster NCE provides multiple levels of maintenance modes in the analysis service, including tenant self-service, QR codes for site engineers, and proactive maintenance by NOC.

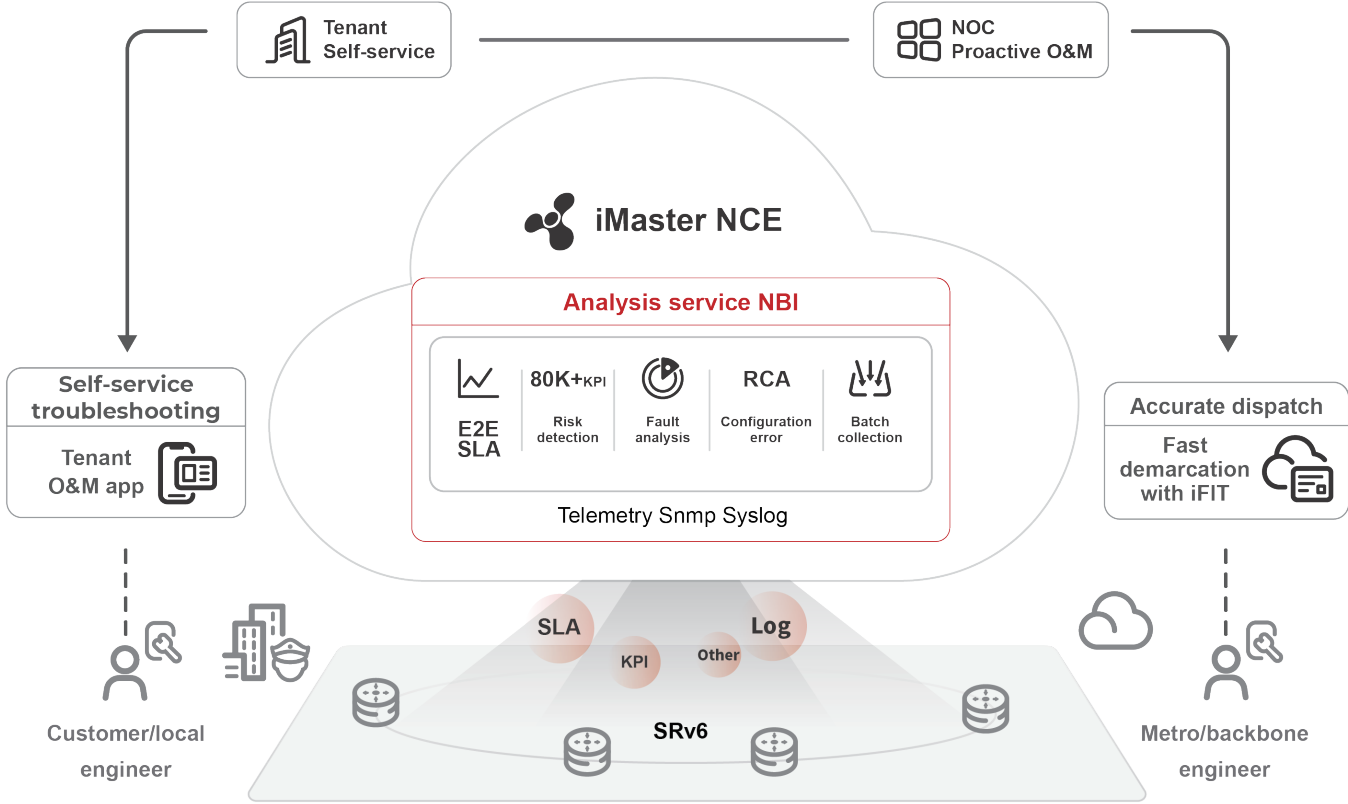


Figure 2-7 iMaster NCE Analysis service

○ Tenant self-service: Tenant service SLA visualization, reconciliation, and one-click fault reporting are key to the evolution of cloud-network convergence maintenance. Users can view service quality on the portal, receive service quality reports periodically, or report a service fault in one click and trace the fault rectification progress in real time. The analysis service provides a tenant-level service visualization interface to detect service quality in real time and automatically selects a suitable SLA detection solution based on different service models. This allows tenants to visualize services without delving into the technical side of diagnosis. The management and control system can automatically start or stop service SLA detection, sort and analyze detection



data, and generate report data.

○ **QR codes for site engineers:** This maintenance mode enables last-mile diagnosis and maintenance to determine whether a service fault is caused by customers or the network. This mode is an effective complement to maintenance by NOC. Site engineers use a maintenance app to scan QR codes of CPEs offered by customers and upload CPE information. Then, the management and control system automatically searches for tenant services based on the uploaded CPE ESNs, and performs ping and trace diagnosis at the service and tunnel layers for services delivered from this site to other sites. The system also analyzes the optical power, alarm, and other information of links between the site and the network and provides fault diagnosis results, facilitating subsequent service maintenance. The maintenance app is flexible and efficient, resolving 70% of CPE problems.

○ **Proactive maintenance by NOC:** In addition to tenant self-service and QR codes for site engineers, iMaster NCE supports proactive maintenance based on in-depth analysis of the entire network.



Proactive monitoring and fault demarcation and locating based on service SLAs

The development of the iFIT technology enables real-time SLA awareness per packet per service, and E2E, hop-by-hop, quick service quality (such as packet loss, delay, and jitter) detection, facilitating efficient fault demarcation and locating.

In-depth insight into network KPIs

Huawei intelligent IP devices can collect and report 7 types of 80,000 network KPIs based on Telemetry, and implement an exclusive embedded intelligent technology to proactively identify and report abnormal KPIs.

Intelligent fault root cause diagnosis

The fault root cause algorithm is trained by 40,000 devices in an automation factory based on offline learning with over 160,000 historical fault information records and over 1000 network maintenance experience data records. Root cause analysis can be performed for over 100 types of fault diagnosis models to locate root causes within minutes. Root causes of silent faults can be identified. In addition, precise fault rectification suggestions are provided for over 90% of common faults to implement service fault self-healing and ensure SLA experience.

03 Key Technologies in the Intelligent Management & Control System

3.1 Key Technologies in the Topology Service

The topology service is the most important service provided by iMaster NCE, as it cloudifies operator networks and provides one-hop connection to any cloud access path. In addition, it intelligently detects network status changes and automatically adjusts and optimizes cloud access paths. As such, the topology service is key to the upgrade of cloud network operations. When building the topology service, iMaster NCE adopts three key technologies: cloud access path as a service, intelligent cloud graph algorithm, and high-performance elastic control plane.

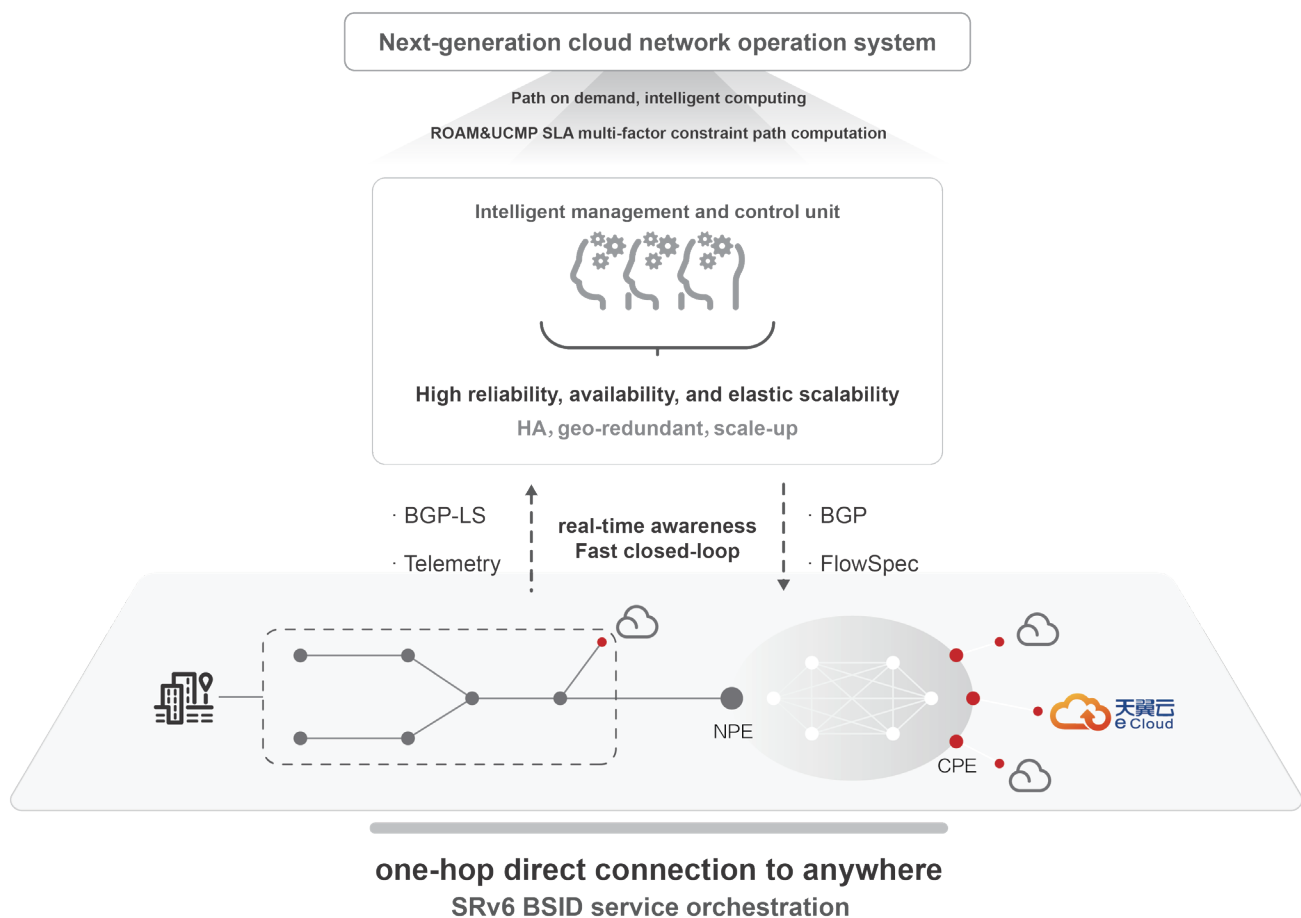


Figure 3-1 Key technologies in the topology service

3.1.1 Cloud Access Path as a Service

- Path navigation service in the digital world: real-time multi-dimensional topology, SLA-based automatic path computation, closed-loop and accessible while paths remain available.

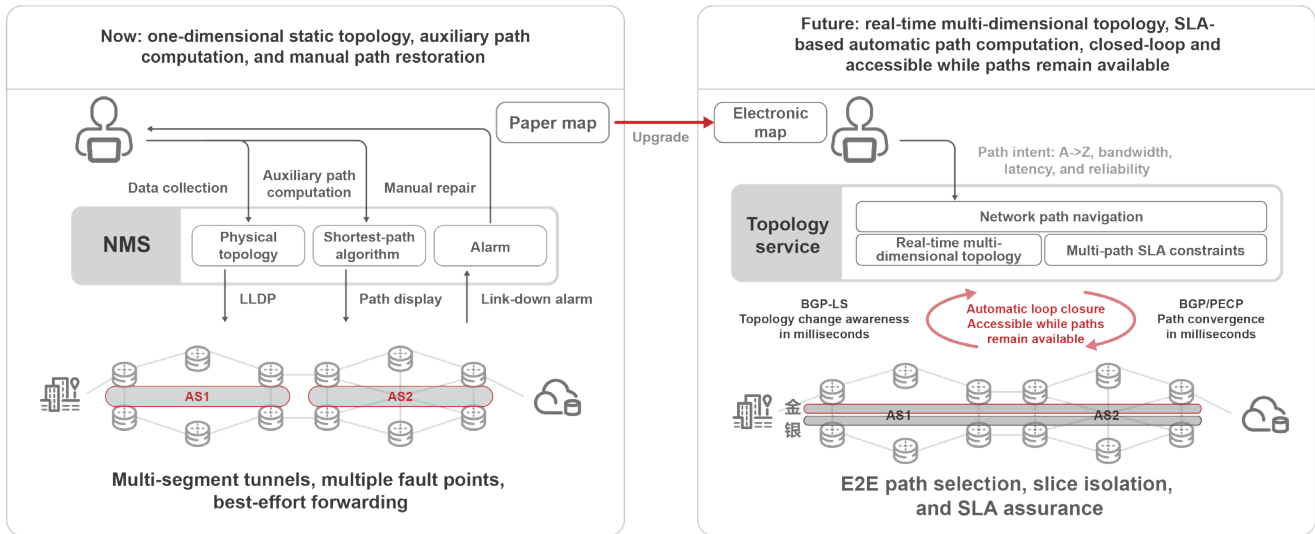


Figure 3-2 Figure 3-2 Cloud access path as a service

The essence of cloud access path as a service is to build a real-time, online, and intelligent path navigation service in the digital world. Before the availability of electronic maps and GPS systems, drivers had no other option than to consult old-fashioned paper maps which offered no indication of real-time road conditions or traffic jams. As a result, driving accuracy depended entirely on the skill and experience of the driver. Traditional NMSs are similar to those old paper maps, as they are unable to detect network connectivity or link latency in real time, and are therefore unable to determine the optimal network path or continuously guarantee path SLAs. In contrast, the topology service provided by iMaster NCE operates similar to electronic maps – by leveraging the SRv6 network programmability technology, it can find the optimal forwarding path through intelligent centralized path computation and continuously guarantee path SLAs based on service SLA requirements.

	Traditional NMS	Topology Service
Topology collection	One-dimensional topology: Layer 2 link connectivity without link quality status	Multi-dimensional topology: Layer 3 links, intra-IGP/AS topology, link bandwidth, and delay
	Non-real-time topology: minute-level and dependent link alarm awareness	Real-time topology: millisecond-level, real-time IGP link status notification, and real-time BGP-LS reporting
Path calculation	Accessibility-assisted path computation: CSPF shortest path algorithm calculates reachability.	SLA automatic path computation: multi-factor path computation based on bandwidth, latency, network slicing, and reliability
	Single link type: Only the P2P link type is supported.	Full link type: FlexEth slicing links, multiple parallel links between nodes
	Active/standby protection: There are two paths, and traffic is transmitted only on the primary path.	Multi-path load balancing: Multiple paths work in full-duplex mode and protect each other.
Path optimization	Manual recovery: hour-level, multi-point faults, service interruption, and manual recovery	Automatic convergence: Sub-second-level fault detection, automatic convergence, and link connectivity
	Manual traffic grooming: Day-level traffic, manual congestion detection, and manual adjustment	Automatic congestion control: minute-level, automatic aware of congested links, and automatic traffic optimization

Figure 3-3 Capabilities of the topology service

● **BSID as a service: one-hop through across management domains, cloud access path as a service**

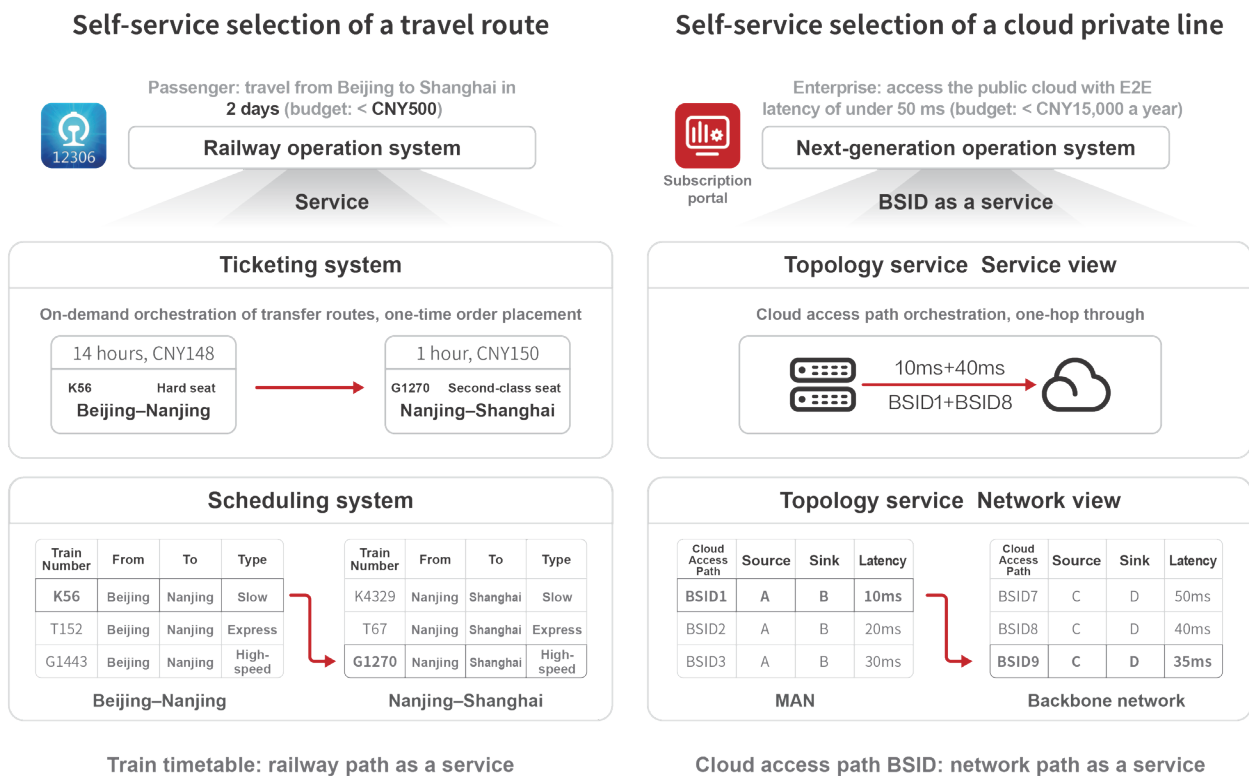


Figure 3-4 SRv6 Policy BSID as a service

As the technical carrier of cloud access path as a service, SRv6 Policy leverages the source routing mechanism to instruct packet forwarding based on an ordered list of instructions

encapsulated on the head node. The 128-bit programmability of IPv6 addresses significantly extends the scope of the network functions that SRv6 instructions can denote. In addition to the End.X instruction that denotes link forwarding, and the End instruction that denotes node forwarding, a binding segment identifier (BSID) is assigned to each SRv6 Policy. If a packet carries a BSID, it will be diverted to the corresponding SRv6 Policy.

Simply put, if we consider an SRv6 Policy as a network service, then its BSID is the interface that allows us to access the service. As such, we can design SRv6 Policies as a service release and subscription model. A BSID (network view) is much like a train ticket: we don't need to worry about who bought the ticket; we just need to take the passenger to the destination according to the committed service level. A passenger can also buy one or more tickets based on their travel needs. Similarly, an SRv6 Policy (service view) is equivalent to the passenger's route, which may carry multiple BSIDs to implement one-hop through. Finally, the topology service itself operates similar to a ticketing system, recommending the optimal travel solution (direct or transit) to customers.

The most significant benefit of SRv6 BSID as a service is network-service separation, whereby underlay BSIDs (network view) serve the overlay SRv6 Policies (service view) and shield them from changes in the physical world. For example, if latency increases due to faults or congestion in links, the underlay BSIDs automatically adjust the forwarding paths to ensure fulfillment of the guaranteed SLAs without causing any changes to the overlay SRv6 Policies. This makes fast service convergence and fault closure possible.

3.1.2 Intelligent Cloud Graph Algorithm

As an effective navigation service cannot be achieved without an intelligent path algorithm, iMaster NCE adopts the cloud graph algorithm for cloud networks. The most significant feature offered by this algorithm is the combination of both network and cloud factors, enabling

integrated intelligent scheduling of clouds and networks. In addition, the algorithm possesses the following key capabilities:

- **Multi-factor path computation**

In addition to SLA constraints such as service bandwidth, latency, and reliability, real-time network status is also considered to ensure the optimal path is found.



Bandwidth assurance: Path computation can be conducted in real-time bandwidth or reserved bandwidth mode. In real-time bandwidth mode, the algorithm regards the real-time bandwidth of topology links as a constraint during path computation, whereas in reserved bandwidth mode, it regards the sum of reserved bandwidths on all link-carried tunnels as a constraint during path computation. The latter mode is especially useful for cloud networks, as end users are charged based on bandwidth and committable bandwidth is a basic requirement.



Reliability assurance: The cloud graph algorithm fully considers the relationships between the working path, protection path, and network status. For example, the working and protection paths must be separate so that failure of one link will not interrupt both working and protection paths as well as services. In addition, the working and protection paths must not pass through the same shared risk link group (SRLG), so that failure of one optical path will not interrupt multiple links. (Link interruptions will affect the working and protection paths as well as services.) In this sense, the cloud graph algorithm can attain the guaranteed reliability for redundant paths in customer services.



Latency assurance: Path latency is the sum of hop-by-hop link latency and device forwarding latency. Link latency is relatively fixed and depends on distance, while device forwarding latency is associated with a range of factors, including traffic burst, path congestion, and queue priorities. The cloud graph algorithm uses network calculus technology to associate the forwarding latency with the reserved bandwidth of slices, ensuring absolutely deterministic latency for users.

● Network resource optimization

Once services have been running for a certain period, network resource usage becomes uneven, with some links becoming overloaded while others remain only slightly loaded. In this situation, network paths must be globally optimized to balance network load and improve network throughput without lowering SLA commitments to users.



Local optimization: If just one link is congested, we can recompute paths for tunnels carried by this link and divert traffic to lightly loaded links. The key to this function is priority preemption among tunnels, and we must ensure that high-priority tunnels always have the optimal SLAs.



Global optimization: All tunnels on the network are optimized to achieve load balancing. The most challenging aspect lies in the trade-off between computation speed and balancing gains. The cloud graph algorithm is able to perform global optimization on an ultra-large network with an excessive amount of tunnels.

● Path computation based on cloud and network factors

Using real-world analogies, we can think of the cloud as a hotel and the network as a road. When choosing a hotel, guests need to consider the hotel's service quality, price, and distance, as well as the road conditions and taxi fares related to the journey. One of the cloud graph algorithm's core capabilities is considering factors such as cloud costs and storage loads – in addition to traditional factors like network bandwidth and latency – to assist users in obtaining the optimal cloud-network product.



Latency circle: Centered on any device on the network, the latency circle helps users quickly locate all the cloud pools that meet certain latency requirements and select the most appropriate locations to build cloud pools with the widest coverage. Thanks to the reverse search approach, the cloud graph algorithm can compute a latency circle for an ultra-large network in seconds.



Package recommendation: Once users have entered all branch sites that need to access the cloud, the cloud graph algorithm recommends the optimal cloud pool location. In addition to being the most cost-effective cloud pool, it will also meet essential network requirements such as service bandwidth and latency. As the cloud graph algorithm integrates cloud factors into path endpoint constraints and leverages the multi-path optimization algorithm, it can quickly select multiple packages and help users purchase the most appropriate cloud-network products.



3.1.3 High-Performance Elastic Control Plane

As the brain of the network, the topology service functions as a centralized network path control point. Its performance and reliability are therefore of paramount importance, and iMaster NCE uses the following key technologies to build a high-performance high-reliability control plane:

- **Microservice + embedded ICT convergence architecture:** Control protocols comply with IETF standards, and use of the traditional CT NE design mode poses high requirements on the processing and storage efficiency of protocol packets. Consequently, iMaster NCE requires high-performance real-time processing functions such as BGP-LS and path computation, while embedded coding is used to improve the per-service processing performance. An IT-like microservice architecture is used to maximize its pipeline and high concurrency capabilities, achieving the ultimate goal of controlling massive amounts of tunnels on an ultra-large network in real time.
- **Elastic scale-out:** Based on the network scale and area division, multiple instances are used to flexibly scale out the path computation capabilities of the control plane.
- **99.999% reliability:** Remote disaster recovery and redundancy protection are supported. If the active control plane becomes faulty, the standby alternative automatically becomes active. Throughout switching, services remain lossless and network paths remain unchanged, while the

protocols between iMaster NCE and devices are enhanced to implement automatic best-effort and service takeover capabilities. This ensures that services are not interrupted even if devices are disconnected from iMaster NCE in extreme situations. Once it has recovered, iMaster NCE automatically takes over path computation and attempts to retain the original service paths, minimizing network flapping.

3.2 Key Technologies in the Connection Service

The connection service in iMaster NCE is designed for full-lifecycle automation of tenant networks. From the perspective of tenants, it defines network service capabilities, shields unnecessary technical details, and provides simplified service-oriented interfaces for the cloud network operation system to invoke. It combines intent-driven orchestration and a high-reliability configuration plane to enable real-time establishment and adjustment of a large tenant network with 100% accurate configurations.

3.2.1 Intent-driven Orchestration

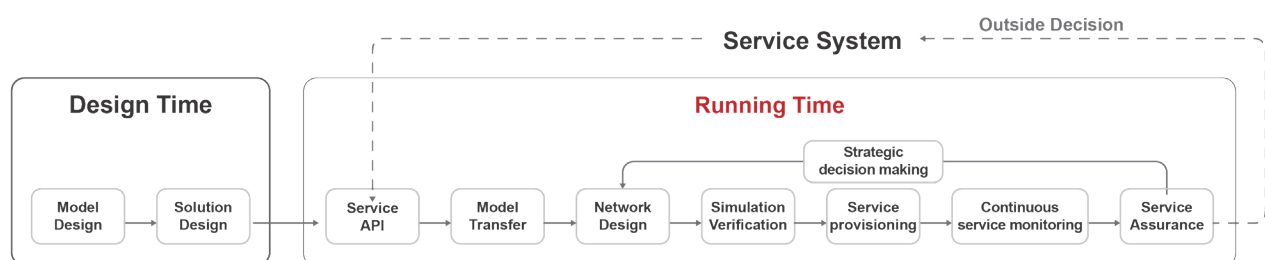


Figure 3-5 Design time and runtime of intent-driven orchestration

Intent-driven orchestration is a process that converts service requirements for networks into understandable, configurable, measurable, and optimizable objects and attributes. It

covers a series of automatic workflows, including model conversion, simulation & verification, service provisioning, service monitoring, service assurance, and policy closure. Intent-driven orchestration is divided into design time and runtime, and the intent engine must load the designed workflow scripts to runtime online so that new functions and workflows can be added without version upgrades. In the context of cloud networks, intent-driven orchestration ensures that the differences between network technologies are shielded in workflow design, enabling service-oriented NBIs to remain stable. Intent-driven orchestration provides the following key capabilities:



Workflow engine: iMaster NCE's network function modules are located at multiple layers, and those at each layer serve external systems through RESTful interfaces. For example, the topology service provides path computation and establishment interfaces, and the analysis service provides service performance testing and fault diagnosis interfaces. All atomic APIs can be registered with the workflow engine for the connection service to orchestrate their invocation sequence, thereby yielding intent-driven service-oriented interfaces for tenant networks.



Closed-loop policy engine: This engine offers flexible closed-loop processing to achieve high degrees of network autonomy. For example, if the analysis service determines that the latency of a connection on a tenant network exceeds the threshold, the corresponding latency-reducing action (such as path re-optimization) can be defined through the policy engine. In this way, no manual operation is required to handle network status changes, facilitating continuous fulfillment of tenant service SLAs.



Simulation & verification engine: The control plane verification/data plane verification (CPV/DPV) component is used to build simulation & verification capabilities on the control and data planes. Using a "network modeling + formal verification" pattern, it provides an objective and reliable quantitative basis for network change evaluation. CPV utilizes a protocol simulation engine for formal solution and verification of black holes, loops, and route reachability on the control plane, while DPV utilizes a forwarding simulation engine for formal solution and verification of forwarding paths on the data plane. Both technologies effectively ensure the accuracy of intent-driven orchestration designs in the connection service and prevent configuration errors from impacting the live network.

||| 3.2.2 High-Reliability Configuration Plane

Scale and elasticity represent the core competitive elements of the intelligent cloud-network. In terms of scale, the first challenge relates to the scale of physical networks, as tens of thousands of physical devices exist on operator WANs. The second challenge relates to the scale of tenant networks – large amounts of tenants equate to enormous VPN and tunnel configurations. In terms of elasticity, the biggest challenge involves industry tenants, as their massive sites require a large number of services to be deployed within a short period of time.

To address these challenges, it is necessary to build a high-performance high-reliability configuration plane. Traditional network devices are configured using the CLI protocol, which involves human-machine interfaces and is not capable of ensuring that all delivered configurations are correct. As such, the next-generation configuration plane oriented to cloud networks should be based on NETCONF/YANG. NETCONF is a new configuration protocol

that ensures configuration accuracy through capabilities such as configuration transaction, verification, and rollback. Likewise, YANG is a new data description language that is modular, programmable, and scalable – ideal for automation. Thanks to NETCONF/YANG, iMaster NCE can build the required high-performance high-reliability configuration plane.

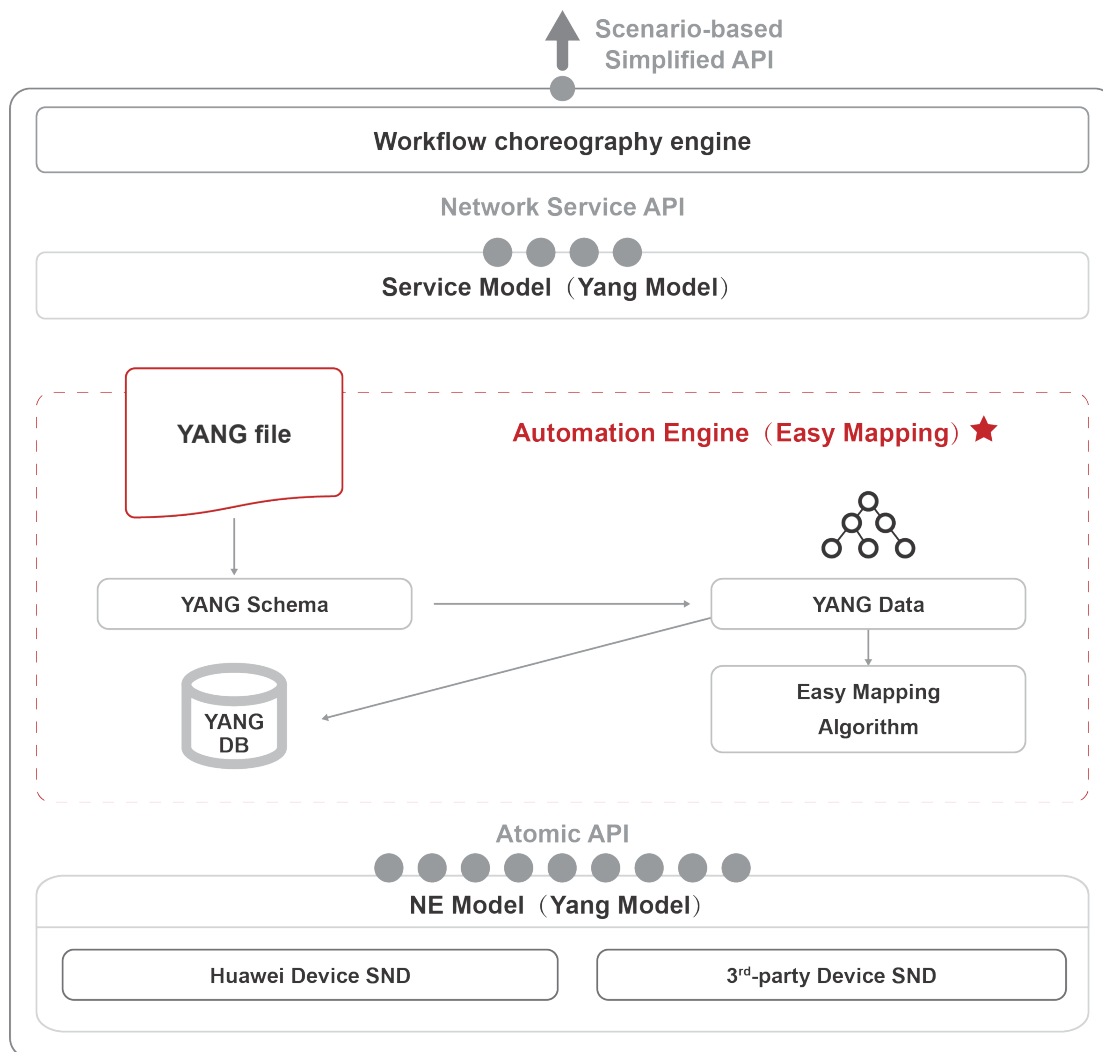


Figure 3-6 NETCONF/YANG-based high-reliability configuration plane

○ **YANG engine:** Once devices are managed by iMaster NCE, the YANG-based automation engine can quickly obtain configuration files and generate NE-level atomic APIs. It can also generate network service APIs based on custom YANG service models. The logic for decomposing network service configurations into NE service configurations can be flexibly programmed. To simplify such programming, the engine provides reliability mechanisms such as

transaction, rollback, and reconciliation for service provisioning.

YANG compilation

YANG loading, expression, and conversion; structure optimization, efficient serialization, and correctness check.

YANG database

storage and efficient retrieval with DataStore and GaussDB.

EasyMapping

domain-independent service model description, decomposition, orchestration, computation, and backtracking algorithms.

○ **High reliability:** Based on YANG engine technology, iMaster NCE builds a high-reliability configuration plane.

Transaction

Service provisioning is idempotent – when all connection services provision a service to multiple NEs, all NEs must be successfully configured. Otherwise, service provisioning is rolled back to the initial state. This capability ensures that the configuration models of the connection services are consistent with configurations on network devices.

Reconciliation

Connection services can initiate configuration consistency checks and automatically rectify any inconsistent configurations.

||| 3.3 Key Technologies in the Analysis Service

Service quality assurance is key to thriving cloud services, and sits at the core of intelligent cloud-network O&M. iMaster NCE's analysis service provides SLA visualization and quality assurance capabilities for network-side services, visualizing network-side information in multiple dimensions, proactively detecting service quality deterioration, and accurately demarcating and locating faults. Combined with advanced capabilities such as service path optimization, these features enable cloud network service quality that can be reliably guaranteed.

3.3.1 Multi-dimensional Cloud Network Visualization

iMaster NCE visualizes information from multiple dimensions, including network traffic, service SLA quality, and hop-by-hop SLAs of cloud access paths. This allows both operators and tenants to efficiently monitor networks and services and accurately determine their condition. Multi-dimensional cloud network visualization offers the following key capabilities:



Traffic map and report: Traffic information is the basis of network monitoring. The analysis service provides real-time traffic monitoring and historical data query capabilities regarding user VPNs, network links, device interfaces, and interface queues. Specifically, based on both VPN and network traffic, it monitors network loads in real time, adjusts possible congestion points in advance, and provides guidance for accurate network planning and expansion. It also analyzes user traffic usage to effectively guide operator marketing activities such as the recommendation of suitable packages.



Cloud network service SLA visualization: Packet loss and latency are key indicators of service quality. However, traditional networks adopt an out-of-band SLA detection solution which cannot adequately deliver the actual service SLAs or hop-by-hop SLAs of service paths. In contrast, the analysis service provides real service latency and packet loss information, including the E2E SLAs of network-side services and hop-by-hop SLAs of service paths, effectively supporting quality monitoring and assurance of cloud network services.



Cloud network service path visualization: The analysis service provides details of network-side devices and links traversed by cloud network services, accurately reproducing the cloud access paths of these services. If network switchover or link changes occur, the analysis service can obtain the updated service paths.



History backtracking: Users can view the history of the preceding data to facilitate in-depth analysis and network planning.

3.3.2 Intelligent Assurance

Intelligent assurance is a core capability of Analysis as a Service. Thanks to the built-in algorithms of its intelligent analysis engine, iMaster NCE is able to analyze network and service trends and risks and accurately locate fault points based on multi-dimensional network information. This combines with the controller's optimization function to quickly rectify service

faults, ensuring high reliability of the cloud-network. Intelligent assurance offers the following key capabilities:

Intelligent prediction and prevention

A comprehensive "health check, diagnosis, and treatment" solution has been designed to transform the network from fault-centric to health-centric. Big data and intelligent technologies are utilized to automatically draw a fault propagation diagram, facilitating root cause inference and proactive identification of potential risks in network resources.

Fast demarcation at cloud network edges

The one-click fault demarcation and diagnosis capability is provided for cloud and user-side PEs to help carriers quickly demarcate network faults: whether the faults occur on the user network, cloud network, or operator network.

Precise hop-by-hop measurement

In-situ Flow Information Telemetry (IFIT) is a next-generation network detection solution developed by Huawei. Compliant with IETF's IPv6 Application of the Alternate Marking Method draft, IFIT measures both E2E and hop-by-hop SLAs (such as traffic, packet loss, latency, and jitter) for actual service flows, enabling it to quickly detect and accurately demarcate and diagnose network quality faults. Compared with traditional detection technologies such as TWAMP and Y.1731, IFIT is more advantageous in that it increases the SLA detection precision to 10^{-6} and is able to directly locate faulty devices.

Fast Recovery of Cloud-Network Services

After IFIT accurately locates faulty links and nodes, users can quickly log in to devices from the IFIT page and then take flexible measures, including but not limited to adjusting device configurations (such as costs and port shutdown). They can also directly change paths on the controller's optimization page.

Interface Traffic Analysis in Seconds

The high-speed collection capability of Telemetry enables port traffic collection and presentation in a matter of seconds as well as refined reflection of network traffic bursts, effectively helping operators identify and analyze the impact of network traffic bursts on user services.

3.3.3 Data Plane with Powerful Computing

Built on big data and intelligent technologies, the analysis service provides real-time and historical data analysis capabilities for network-wide devices and services. To meet the diversity, real-time, and reliability requirements of data management, the following framework capabilities are required:

Model-driven efficient collection with Telemetry

Telemetry is a technology that remotely collects data from physical or virtual devices at high speeds. Devices periodically send information such as interface traffic, CPU, and memory data to collectors in push mode, which, in contrast to the conventional pull mode (ask and answer), provides faster and real-time data collection.



On network devices, the data sampled by Telemetry technology is described by models, which can be either proprietary YANG models customized by vendors or standard YANG models defined by standards organizations such as IETF. These models present network device data in an organized manner, and enable interaction between NMSs and devices.

Elastic scale-out and efficient computing

Analysis as a Service, which is based on network-wide data, must support distributed processing and elastic scale-out based on the network and service scale without affecting services. Its characteristics include:



- Distributed concurrent computing and TB-level data processing in minutes
- Distributed storage and fast data querying in seconds
- 100+ online clients
- Multi-copy storage, preventing data loss due to a single point of failure

04 IT Architecture and Integration Ecosystem Construction

||| 4.1 Challenges to IT Architecture and Integration

Within the IT architecture of intelligent cloud-networks, efficient integration of the intelligent management & control layer with traditional OSSs/BSSs or the next-generation cloud network operation system is key to e-commerce operations. To cope with the impact of e-commerce and the Internet on operator services, the TMF released an eTOM reference framework as a basic blueprint for OSSs/BSSs. In addition, the TMF defined a component collaboration and system delivery framework to help operators implement the next-generation operation support system (NGOSS).

However, in actual deployment scenarios, operators usually add new functions and propose their own framework standards to meet personalized requirements. Typical examples include China Telecom's Technical Specifications for Next-Generation Cloud Network Operation Systems, China Mobile's OSS 4.0, and China Unicom's OSS 2.0. This increases the difficulty of system implementation and prolongs integration test time. From the perspective of delivery, these components come from different suppliers around the world, and specific interface interconnection issues can only be encountered during onsite tests, which further delays the overall pace. As operators typically require between 6 and 9 months to finish an E2E integration project, network capabilities cannot be fully unleashed or quickly converted into salable service capabilities. This greatly increases the time to market (TTM) and puts operators at a disadvantage in terms of competition with OTT providers.

As a result, telecom operators face a number of common problems: optimizing OSS/BSS

collaboration processes and interfaces to meet automation/servitization requirements; reducing deployment and onsite customization costs; and shortening the integration cycle and TTM to better compete with OTT providers.

4.2 IT Architecture and Integration Lab

4.2.1 Integration Lab Ecosystem Plan

To solve the problems relating to OSS/BSS integration, Huawei is committed to building an integration lab capable of connecting OSS/BSS vendors, operators, and scientific research institutes. The lab provides an experienceable integration environment to benefit all stakeholders in the OSS/BSS value chain.

Integration Lab: Building an Integration Ecosystem Bridge and Multi-Party Value Chain

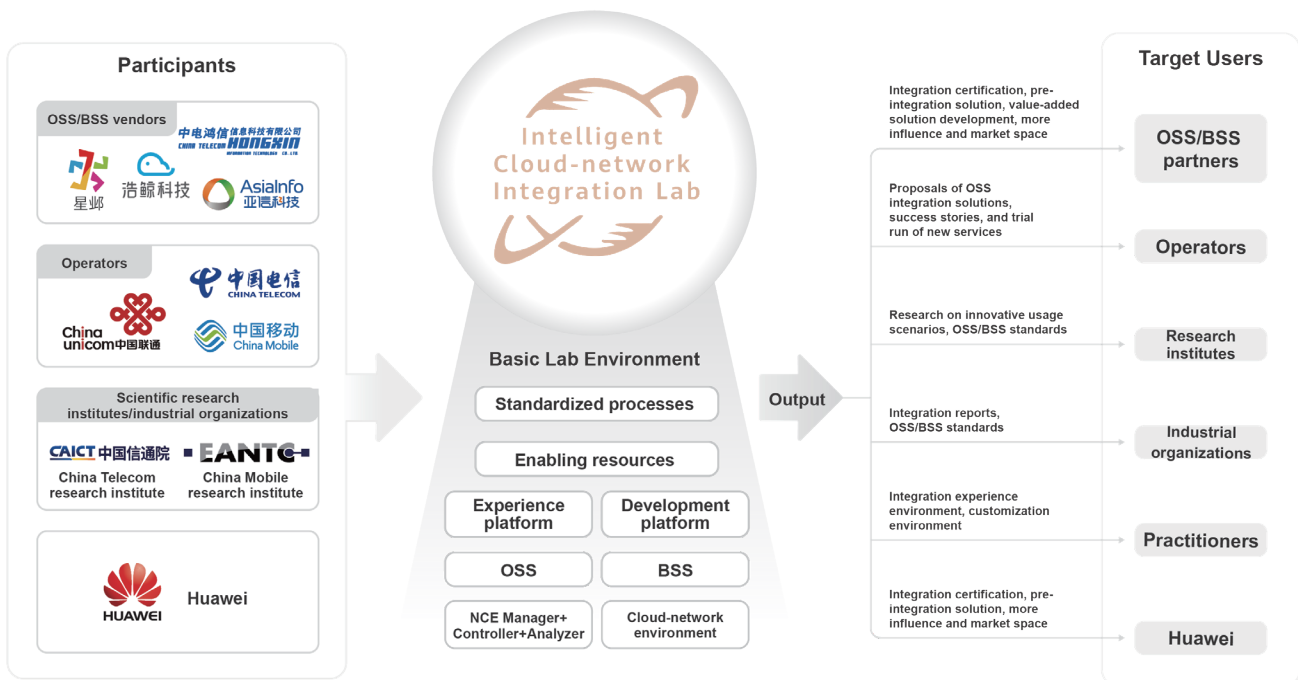


Figure 4-1 Overview of Huawei's intelligent cloud-network integration lab

Huawei will take the following three steps to maximize the value of its integration lab:

Step 1: Build a pre-integration and experience platform to verify integration interfaces in advance

based on service processes, and provide an E2E integration environment for lab users.

Step 2: Build an integration interface testing and learning platform, translate earlier integration experience into interface baselines, and help partners understand and use open network interfaces.

Step 3: Deepen cooperation between Huawei and operators and partners to facilitate the creation of innovative competitive cloud network solutions.

Huawei is committed to providing the following services for lab users:

- Users can experience API/GUI operations on OSSs/BSSs and intelligent management & control systems, or compile code themselves to try specific APIs.
- Typical operator networking environments are available, including China Unicom's intelligent MAN, and China Telecom's STN, new MAN, and SPN. Interconnection baselines are formed (for example, for China Telecom, China Unicom, and China Mobile) based on pre-integration and authentication standards, which help identify interconnection problems in advance and ensure interface compatibility. We aim to resolve 80% of interconnection problems in the lab, reduce onsite implementation risks and costs, and shorten the integration time.
- Onsite development and customization are simplified through tools, improving delivery capabilities and cost competitiveness, expanding application scenarios, and enhancing customer confidence.

4.2.2 Integration Lab Management Process

In terms of OSS/BSS integration management, Huawei has launched the mature Manage Alliance Relationship (MAR) process, wherein Huawei experts and ecosystem partners jointly design and test solutions, release test reports, and issue certificates to each other.

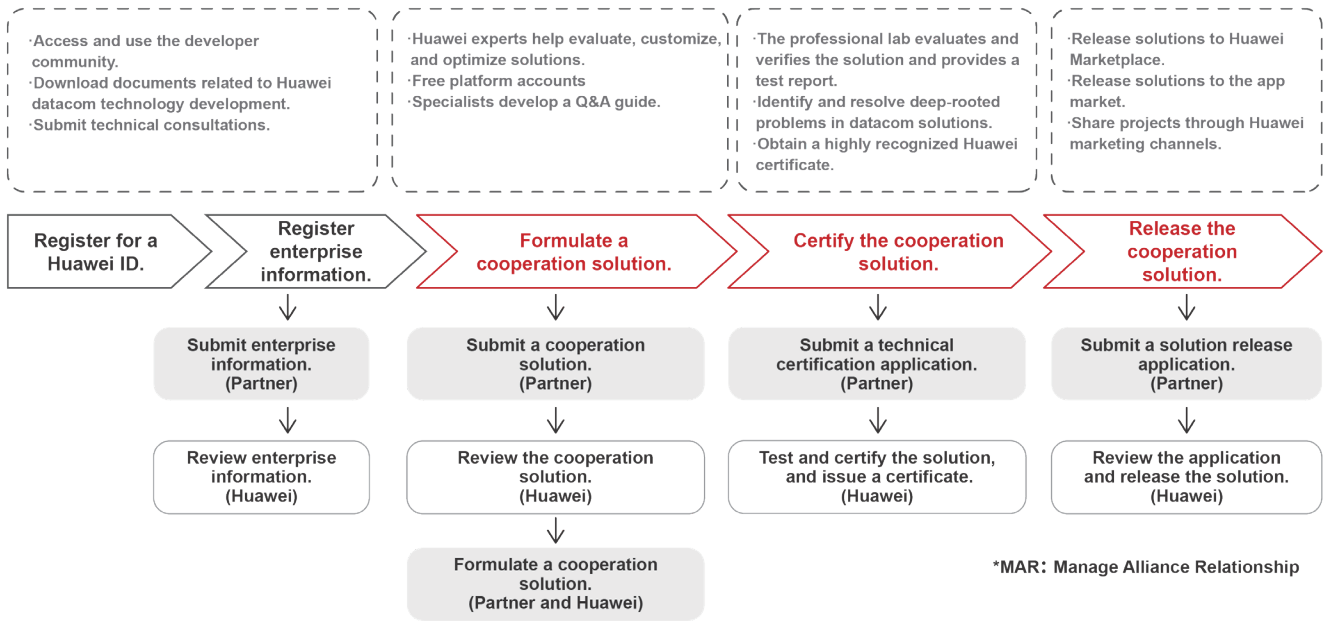


Figure 4-2 Huawei's MAR process

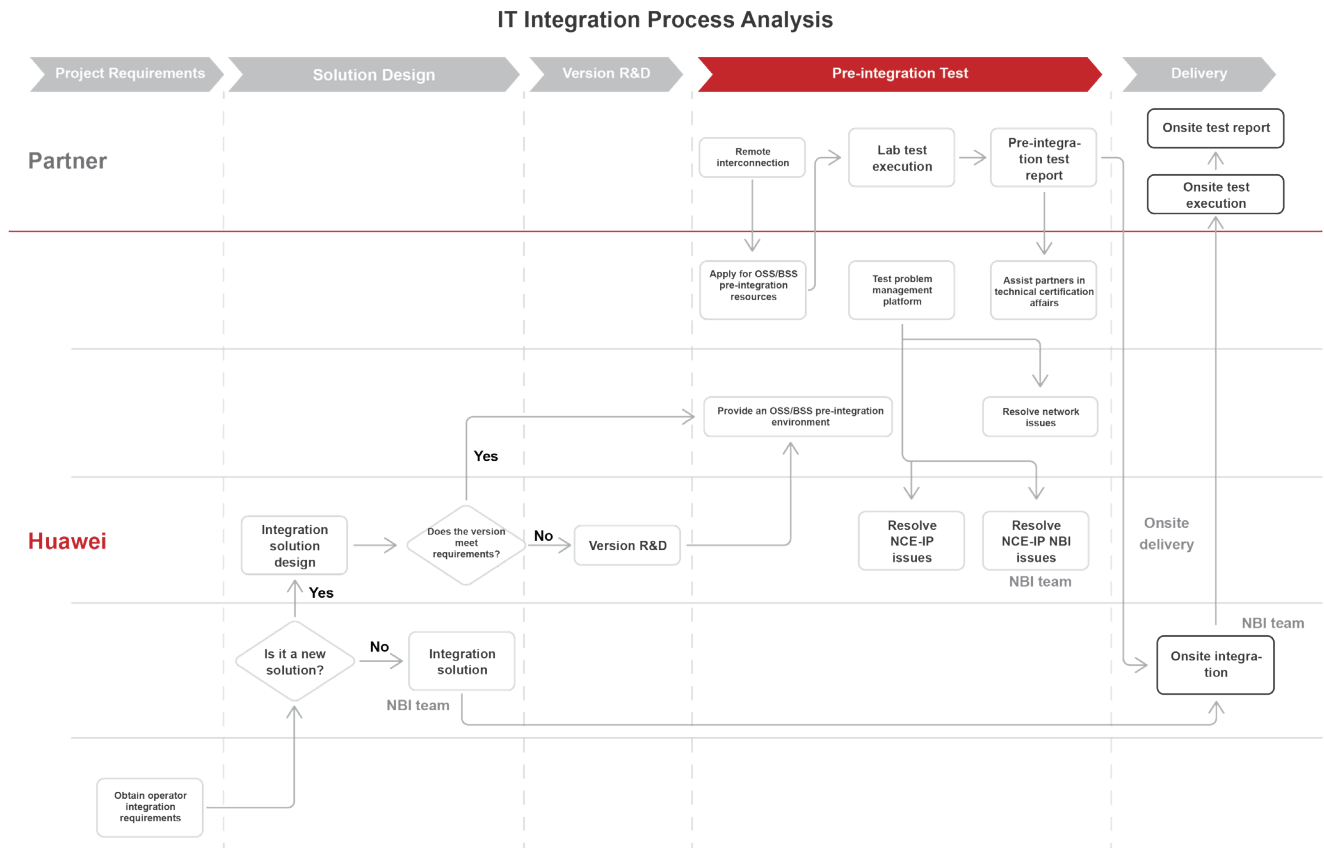


Figure 4-3 Huawei's OSS/BSS integration process

Huawei's integration lab is a one-stop unified portal where users can gain OSS/BSS integration experience, study the intelligent cloud-network solution and OSS/BSS success cases, or apply for resources for interconnection testing. Once a successful test has been completed, the system automatically generates an integration test report.

||| 4.3 IT Architecture and Integration Practices

Thanks to the OSS/BSS integration ecosystem, OSS/BSS and ICT vendors can quickly streamline OSS/BSS service processes while operators can efficiently develop cloud-network convergence capabilities for intelligent cloud-network projects. Following successful interconnection and certification with numerous industry vendors – such as Nanjing Staryea Network Technology Co., Ltd. and Hongxin Information Technology Co., Ltd. – Huawei iMaster NCE has already been successfully deployed in market projects.

China Telecom Ningxia, in particular, is committed to providing users with an e-commerce cloud network service experience. By regarding networks as the foundation and clouds as the core, China Telecom Ningxia aims to integrate both in order to achieve cloud-driven network scheduling. Based on an integrated authentication solution, iMaster NCE has been quickly interconnected with provincial OSSs/BSSs, making China Telecom Ningxia the first operator to deploy slicing and SRv6 technologies across the entire government & enterprise network. In this way, China Telecom Ningxia implements multi-cloud interoperability for the education, healthcare, and law-enforcement sectors. Its one-stop cloud network service capability enables industry customers to subscribe to an extensive set of cloud-network products through a unified online portal.



05 Summary

A core motivation behind Huawei's three-layer intelligent cloud-network architecture (namely, network infrastructure layer, intelligent management & control layer, and network operation layer), NaaS capabilities, and OSS/BSS integration solutions, is to cooperate with operators, OSS/BSS partners, and industry alliances to deliver integrated cloud-network scheduling as well as consistent cloud-network experience for thousands of industries in the cloud era. Huawei also aims to assist operators with their transformation from traditional ICT services to future-proof DICT services, fueling breakthroughs in emerging technologies across all areas of society.



06 References

1. TM Forum: Business Process Framework (eTOM)
2. IETF: IPv6 Application of the Alternate Marking Method
3. Expert Committee on Promoting Large-Scale IPv6 Deployment: SRv6 Technology and Industry White Paper
4. China Telecom: Technical White Paper on Cloud-Network Convergence in 2030
5. Alibaba Cloud: Cloud Networking White Paper
6. Huawei Intelligent Cloud-Network Solution White Paper

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Industrial Base Bantian Longgang

Shenzhen 518129, P.R. China

Tel: +86-755-28780808

www.huawei.com

Copyright©Huawei Technologies Co., Ltd. 2021. 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.

Trademark Notice

 HUAWEI, HUAWEI and  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.