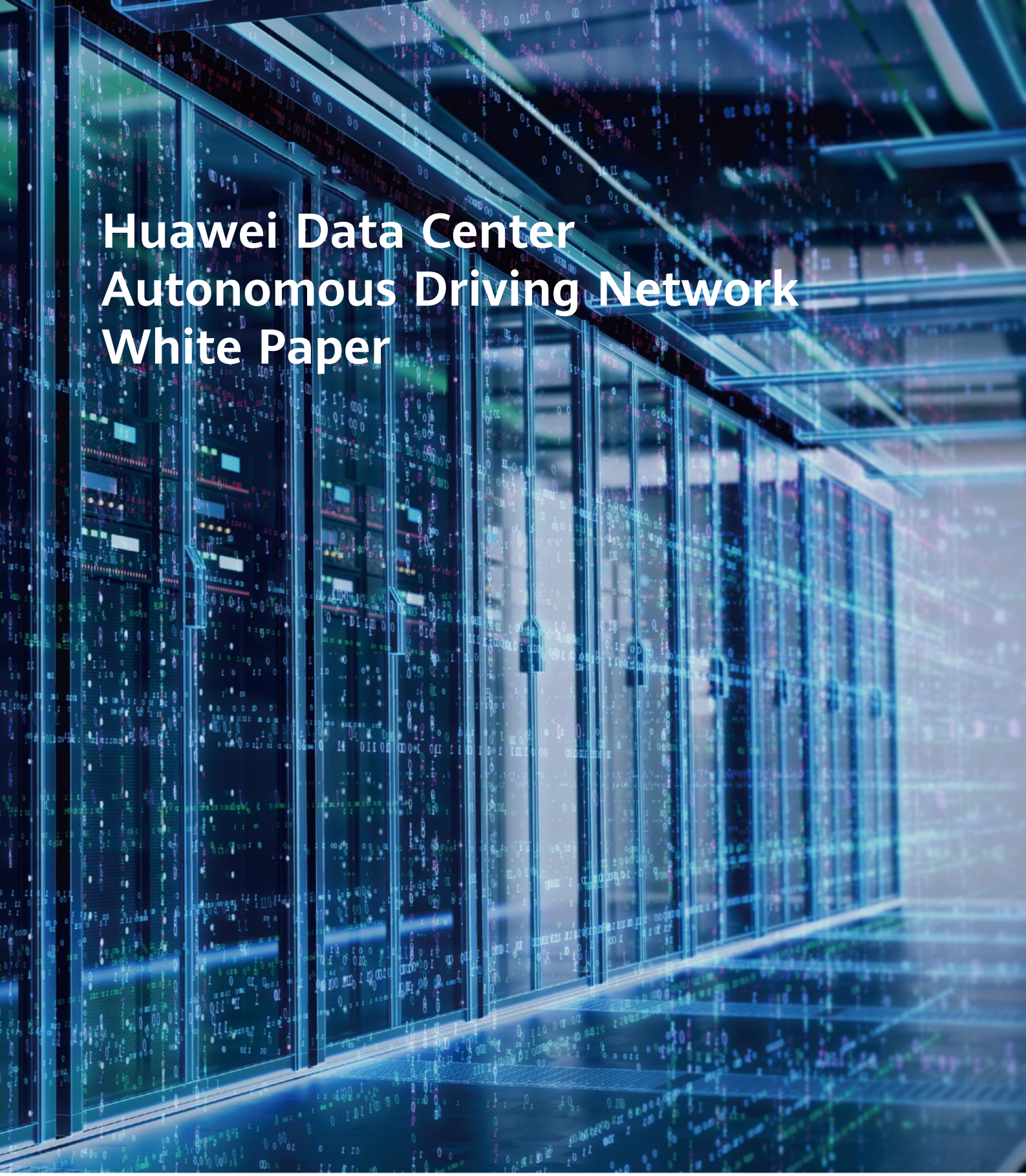


Huawei Data Center Autonomous Driving Network White Paper

HUAWEI

Contents
CONTENTS

Contents
CONTENTS

01

Driving Forces of Autonomous Driving Networks

Over the past decade, data centers (DCs) are undergoing radical development in their technologies and deployment methods. Such development can be summarized into three phases:

- **DC 1.0:** the first phase that is dominated by data center consolidation. This phase corresponds to the traditional two-layer architecture: STP + VLAN.

- **DC 2.0:** the second phase that advances DC 1.0 in higher resource sharing utilization and more flexible resource deployment via resource virtualization and dynamic service orchestration. In this phase, networks evolve into the fully connected overlay architecture.
  In particular, DC 2.0 outperforms DC 1.0 in the increasingly mature cloud computing technologies and large-scale deployment.
  In particular, DC 2.0 outperforms DC 1.0 in the increasingly mature cloud computing technologies and large-scale deployment.

- **DC 3.0:** the third phase aiming to better adapt to the explosively increasing service volumes in the Artificial Intelligence (AI) era. DC 3.0 stands out mainly for its super-large scale, distributed multi-region multi-center, higher requirements on the network architecture intelligence, and powerful integration of various branch-new technologies, such as container and Remote Direct Memory Access (RDMA), into applications.

The development outline of DCs signifies that DCs keep developing rapidly to catch up with and better support the service development pace. DCs are making process in line with high requirements over their openness, capacity, scalability, controllable costs, security, and stability, ultimately achieving a comprehensive and continuous improvement in various capabilities, such as flexible service adaptation, rapid application deployment, information exchange and sharing, distributed system expansion, and flexible load scheduling.

All these development trends have posed great impacts and proposed branch-new requirements on the scale, cost, planning and design, deployment and construction, maintenance and optimization, and operation management of DCs. The existing DC operation and management solutions cannot catch up with such development trends. Against this

backdrop, all parties in the industry have reached a consensus that a set of highly intelligent network management solutions must be listed on the top-priority agenda.

Thanks to our unremitting efforts in introducing key technologies and concepts such as AI, mathematical verification, and intent-driven network, we successfully build a set of autonomous driving network solutions for DCs. Amid our pursuit for comprehensive intelligence and automation, we are committed to iterative development of autonomous driving networks by phase, aiming to further evolve the networks into comprehensively intelligent and autonomous data center networks (DCNs).

1.1 Challenges Facing DCNs

- As the network scale increases, large enterprises and carriers confront many more difficulties in managing their networks. Manual network management has been far from meeting their service development requirements. Considering this, introducing an automatic network management and control system is time-pressing. Such a system can implement more secure and efficient service configuration automation and large-scale network orchestration than manual operations.

- Amid enterprises' pursuit for digital transformation, their requirements on network agility and availability keep increasing. In addition, the networks often change. Traditional O&M methods, however, are holding back the enterprises' digital transformation process. In this vein, the enterprises are urgently calling for an automatic network management and control system that can verify the network design implementation result in real time and discover network faults in a timely manner during network operating, thereby minimizing service interruption.

- Cloud applications need to be deployed across heterogeneous or multi-cloud infrastructures without sacrificing network service consistency. This practice solves the network management issues unique to heterogeneous environments and enables users to implement unified network management and control oriented at the service intent. In addition, device differences and private interfaces at the infrastructure layer are shielded, eliminating vendor lock-in.

- The enterprises' investment costs are limited. Currently, over the top (OTT) has great impacts on traditional industries. Amid this trend, enterprises are undergoing great competition pressure and urgently require higher efficiency. Network investments are also restricted by the input-to-output ratio. As a result, enterprises' pressures in reducing the operating expense (OPEX) gets greater. Against this backdrop, how to reduce labor costs and improve network performance are listed on the top-priority agenda of Chief Information Officers (CIOs).

1.2 Opportunities Facing DCNs

1.2.1 AI-Powered Network Assurance

AI, as a cutting-edge technology, can make machines as intelligent as humans. Nowadays, network O&M data, such as mass configurations, status data, alarms, and logs, is increasing exponentially. Tens of thousands of or even tens of millions of network O&M indicators have been far from being effectively referenced by O&M personnel. In addition, improper network monitoring thresholds or alarm storms may even terribly interfere with fault diagnosis. How can we resolve these issues and more effectively use network data? AI holds the answer. AI-powered network data analysis helps us get a better grasp of network environment complexity. It already has been widely applied in various domains, such as network fault discovery, root cause locating, and network resource prediction, significantly improving the network O&M efficiency. The outstanding performance of AI in terms of network O&M has been widely recognized in the industry. As predicted by Gartner, the overall AI market share in the telecommunications industry will increase from US$315.7 million to US$11.3 billion in 2025, with a compound annual growth rate of 48.8%. Telecommunications carriers mainly apply AI into network operations, monitoring, and management, accounting for 61% of the total AI investments in the telecommunications industry.

1.2.2 Mathematical Verification

Mathematical verification, also called formal verification, is used to verify whether one or some formal regulations or attributes are correct through mathematics. That is, this technology uses strict mathematical formulas to verify and ensure consistency between the program behavior and expectations. This technology has been widely applied in correctness-hungry domains, such as unmanned aerial vehicles (UAVs), space vehicles (SVs), and operating systems (OSs). In financial service scenarios where DCNs are deployed to transmit critical application data, the loss upon network disconnections reaches up to US$6.89 million per hour. According to Gartner's statistics, 40% network incidents are caused by manual configuration errors. Therefore, many higher requirements are posed on network configuration correctness in such scenarios. Formal verification can meet such requirements. It can convert configuration file information and expected attributes to be verified (reachability, isolation, path information, and route blackholes between network nodes) into a series of logical formulas. The formulas then are calculated through mathematical solvers. This method is also known as network change simulation that can minimize configuration errors and improve the DCN availability.

1.2.3 Development Trends of Intent-Driven Networks

The intent-driven network is a closed-loop network architecture that is constructed and operated on the basis of a holography grasp of the network status, service intent, and AI. The concept of "intent-driven network" was first proposed

by Open Networking Foundation (ONF) in February 2015. Gartner released a relevant report in February 2017. This report defined the intent-driven network and predicted that the intent-driven network will be "the next big thing" in the network domain. As predicted, 1,000+ enterprises will deploy intent-driven networks by the end of 2020. The intent-driven network outperforms other networks thanks to its advanced network services and network operation methods via human languages. As defined, the intent constructs a network-wide declarative policy, so that the network can calculate the most suited solution on the basis of the expectations defined by network operators. A large number of heterogeneous devices and multi-cloud environments exist in the DC domain, which may bring mass device and environment differences. How can we shield such differences? The answer to the question lies in the intent-driven network. With such differences shielded, network administrators can focus on service requirements. In addition, the intent-driven network is a closed-loop system, which means that continuous network changes do not affect the delivered intent and the network needs to be proactively adjusted if the intent cannot be satisfied to ensure that the intent is not affected.

1.3 Rising Momentum of Autonomous Driving Networks in the Industry

1.3.1 Industry Leaders Are Vigorously Planning Autonomous Driving Network Implementation

Financial service:

Industrial and Commercial Bank of China (ICBC): is comprehensively planning the construction of Artificial Intelligence for IT Operations (AIOps), aiming to construct an intelligent O&M ecosystem. ICBC constructed a cloud O&M system oriented at large-scale DC clusters in the second half of 2017. This practice enhances automatic and refined O&M of cloud-based applications, and lays a solid foundation for the implementation of intelligent O&M. In the future, ICBC will keep on advancing the intelligent O&M construction, ultimately evolving intelligent O&M into autonomous O&M in the banking industry. All these practices help ICBC construct an intelligent, open, sharing, efficient, and convergent intelligent banking system. In particular, the data center autonomous driving network solution is an important part of this system.

Carrier:

China Unicom: proposed an intelligent network strategy — CUBE-AI. This strategy focuses on 5G + AI, intelligent network O&M, and industry innovations, and aims to boost the development of network intelligence and service intelligence via innovative technologies, build typical AI applications, and move towards autonomous driving networks.

China Telecom: announced China Telecom CTNET2025 Network Architecture White Paper, signifying a comprehensive startup in intelligent network re-construction and an innovative evolution from on-demand, self-help, and elastic networks into automatic closed-loop and intent-driven networks. In a short term, China Telecom aims to reduce the service provisioning time by 50% to 90% and service interruptions by 50%.

1.3.2 Top Standard Organizations Are Proactively Promoting Autonomous Driving Network Standards

- **Telecommunication Management Forum (TMF)**: announces the white paper — *Autonomous Networks: Empowering Digital Transformation For The Telecoms Industry*. This white paper defines for the first time standards of autonomous driving network's different levels, and figures out that the domain ideal for implementing the autonomous network is DCN.
- **European Telecommunications Standards Institute (ETSI)**: establishes the Experiential Networked Intelligence (ENI) group and Service Management Group (ZSM), which are dedicated to network intelligence research. In particular, the ENI group is committed to experience able intelligent networks, while the ZSM is committed to zero-touch network and service management. The ENI group, established in February 2017, aims to define a cognitive network management architecture that employs a "monitor-analysis-plan-execute" control model and adopts AI to provide customers with better network deployment and operation experience. This architecture centers on network awareness and analysis, data-driven decision-making, and AI-powered closed-loop control. Currently, ETSI has released "ENI Definition of Categories for AI Application to Networks" v1.1.1 that has been written into DCN intelligence level standards.
- **Global System for Mobile Communications Association (GSMA)**: released *AI in Network Use Cases in China Whitepaper*. In this white paper, GSMA clarifies that a highly intelligent automated network is required in the 5G era and networks are also moving towards higher intelligence and autonomy. In addition, a network architecture featuring layered autonomy and vertical collaboration is required for the implementation of the intelligent autonomous network, in order to gradually achieve fully autonomy of networks.

02

Interpretation of Huawei Autonomous Driving Network Strategy

Achieving the ultimate goal — fully autonomous networks inevitably requires a fairy long period of time. Strategically, we can divide this goal into different phases and achieve it phase by phase. Huawei has preliminarily defined the standards for each autonomous driving network level based on full consideration of communication network complexity, wishing to lay a solid foundation for all parties in the industry to reach a consensus on the autonomous driving network levels.

Levels		Features	Evaluation Dimensions						
			Execution	Monitoring	Analysis	Decision-Making	Loop-Closure	Scenario	Intent
L0	Manual Operation & Maintenance	Purely manual operation	Manual operation	Manual operation	Manual operation	Manual operation	Manual operation	*N/A*	Device CLI level
L1	Assisted Operation & Maintenance	Manual analysis and decision-making assisted by basic device CLI-level tools in a few scenarios	Manual operation dominated	System dominated	Manual operation	Manual operation	Manual operation	A few	Device CLI level
L2	Partial Autonomous Network	Static policy analysis and manual decision-making assisted by network model-level standard tools in some scenarios	System dominated	System dominated	Manual operation dominated	Manual operation dominated	Manual operation	Some	Network model level
L3	Conditional Autonomous Network	Basic loop-closure of dynamic policies assisted by system recommendation on the basis of dynamic policy analysis in specific scenarios	System	System	System	System dominated	System dominated	Majority	Network model level + service intent level
L4	Highly Autonomous Network	Automatic and comprehensive loop-closure of dynamic policies on the basis of service intent-level natural language in most scenarios	System	System	System	System	System	Most	Service intent level
L5	Full Autonomous Network	Full loop-closure in any scenario	System	System	System	System	System	Any	Service intent level

- **L0:** manual O&M. All dynamic tasks are performed manually.
- **L1:** assisted O&M. In a few scenarios, the system provides tools for users to help them simplify operations and improve the execution efficiency of recurring tasks on the basis of known repeated execution and monitoring tasks. For example, the system provides the GUI configuration wizard and batch configuration script or tool.

- **L2:** partially autonomous network. In some scenarios, the system provides intent interaction interfaces and assisted tools at the network model level, relieving users' dependency on the device CLI and lowering experience and skill requirements on the personnel. The system can perform network monitoring and analysis based on some predefined static policies. The network monitoring and analysis results then are used as a reference for manual decision-making.
- L3: conditionally autonomous network. In specific scenarios, the system provides intent interaction interfaces and tools at the service intent level, significantly lowering network experience and skill requirements on the personnel. In addition, the system can sense the environment changes, monitor the network, analyze root causes of network exceptions, and recommend closed-loop suggestions to assist users' decision-making using dynamic policies. This implements basic closed-loop management.
- **L4:** highly autonomous network. In most scenarios, users can interact with the system using natural languages at the service intent level. The system can sense environment changes in real time, predict and analyze potential network deterioration risks, rapidly analyze root causes of network exceptions, and dynamically adjust network parameters in an automated manner to rectify network faults and optimize the network. These practices help implement comprehensive closed-loop management.
- **L5:** fully autonomous network, which is the ultimate goal of DCN development. The system has full-lifecycle closed-loop automation capabilities across services and domains in any scenarios, truly achieving autonomous O&M.

  According to the five phases, we can see that the autonomous driving network is a multi-dimensional hierarchical strategy. It is not only the criteria for evaluating a network, but also the roadmap for gradually promoting the autonomous driving network.

03

Huawei Data Center Autonomous Driving Network Solution

3.1 Solution Overview

As a world-leading network solution provider, Huawei has been committed to providing customers with optimal experience. After years of unremitting efforts, Huawei has deployed more than 7,800 DCs. Amid this process, Huawei accumulates extensive experience in and gets in-depth understanding of automation and O&M services. In addition, thanks to its expertise in the DCN domain, Huawei ultimately achieves an in-depth combination of AI, big data, and automation with the DCN domain and releases the intelligent management, control, and maintenance system for autonomous driving networks oriented at DCN scenarios — iMaster NCE-Fabric.

iMaster NCE-Fabric aims to achieve fully autonomous driving of DCNs at L5, providing users with highly autonomous DCNs across the network lifecycle. That is, iMaster NCE-Fabric is centered on user intent (including network construction intent, service intent, and network intent) across the network planning, construction, maintenance, and optimization phases. On this basis, iMaster NCE-Fabric automatically implements network deployment in line with user intent and provides feedback over whether the intent execution results meet user expectations. The following provides three scenarios to describe outstanding functions of iMaster NCE-Fabric across the network lifecycle:

Scenario 1: network planning and construction

A customer needs to construct a DC with a specified number of servers.

① The customer can use iMaster NCE-Fabric right after purchasing it with no extra configuration.
② The customer inputs network planning intent and sets the network reliability requirements (high, medium, and low).
③ iMaster NCE-Fabric automatically plans the network based on the input intent and provides an appropriate network solution and network planning simulation results.
④ The customer confirms the final network planning solution. (The network planning solution can be modified.)
⑤ iMaster NCE-Fabric then automatically completes network construction, executes acceptance test cases, and provides network construction results.

Scenario 2: service change in the network maintenance phase

In financial service scenarios, customers often propose service communication requirements. For example, a financial service customer needs to permit the access from its application A (branch wealth management app) to application B (the risk control system of the HQ).

① The business department inputs the intent.
② The service system invokes the corresponding service template for access between internal applications.
③ iMaster NCE-Fabric automatically decomposes the intent into network change solutions and provides simulation evaluation results.
④ The service system or administrator confirms the final network change solution.
⑤ iMaster NCE-Fabric automatically delivers network configurations and provides service acceptance reports.
⑥ If any problem occurs during acceptance, iMaster NCE-Fabric performs a rollback immediately.

Scenario 3: monitoring and analysis in the network maintenance phase

A customer wants to maintain the network in a convenient and more effective way.

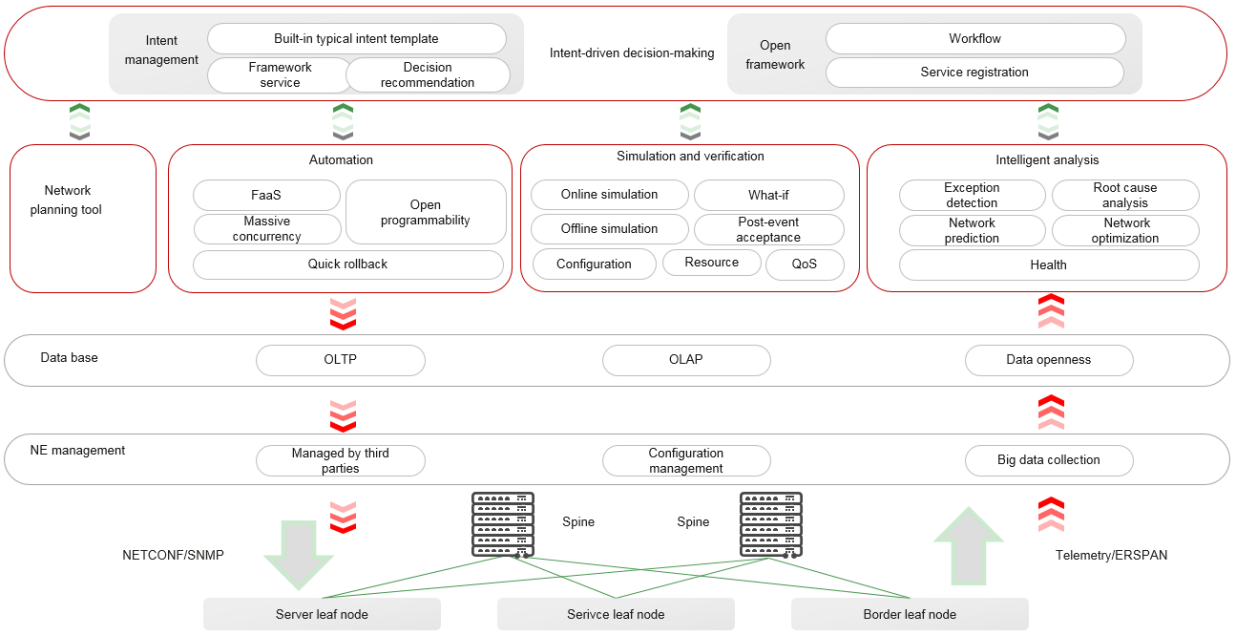
① iMaster NCE-Fabric continuously monitors the network, predicts network faults or deterioration, and proactively reports fault loop-closure or network optimization solutions.
② The administrator confirms the final solution and fault rectification impacts. The system then delivers the solution.
③ iMaster NCE-Fabric automatically optimizes the network to eliminate network faults or deterioration.
④ iMaster NCE-Fabric proactively detects network exceptions, such as device faults, port faults, out-of-date versions, and password expiration.
⑤ iMaster NCE-Fabric automatically submits recommended device upgrade and replacement solutions based on the detected exceptions and provides risk assessment.
⑥ The administrator confirms the final device upgrade and replacement solutions.
⑦ iMaster NCE-Fabric automatically performs device upgrade and replacement and generates corresponding reports.
⑧ If the upgrade or replacement fails, iMaster NCE-Fabric performs a rollback immediately.

The overall architecture of iMaster NCE-Fabric is similar to that of Gartner's digital twin network, and includes three layers:

① Bottom layer: unified data base (transaction + big data)
② Middle layer: network planning tool, automatic control module, and simulation and verification module, and intelligent analysis module
③ Upper layer: intent-driven decision-making module

The service flow of iMaster NCE-Fabric is as follows: The intent-driven decision-making module identifies user intent,

converts it into corresponding network intent, and sends the network intent to the automation module and simulation and verification module for network configuration deployment and change simulation and verification, respectively. The intelligent analysis module performs big data analytics based on the real-time network data and sends the analysis result to the intent-driven decision-making module to determine whether to perform configuration changes. iMaster NCE-Fabric provides key functions required across the network planning, construction, maintenance, and optimization phases.



The intent-driven decision-making module functions as the brain of autonomous driving networks and also signifies the improvement from L2 to L3 of autonomous driving networks. This module is intent-centric and can effectively organize network planning and design, configuration automation, intent simulation and verification, intent monitoring and analysis, fault rectification, and network optimization, achieving automatic loop-closure of intent across its lifecycle.

- Intent definition: network services externally offered and routine network operations from the network administrator's perspective. These services and operations are provided across the DCN's lifecycle and include network planning (new site construction, capacity expansion, and device replacement), network construction (device go-online and application go-online), service changes (mutual, internal, and external connection services), and routine network monitoring and analysis (exception identification and fault rectification). iMaster NCE-Fabric provides some built-in intent templates.
- Intent framework service: full-lifecycle intent management, for example, user intent identification, intent template recommendation, intent simulation and verification, automatic intent delivery, intent monitoring, and exception-triggered configuration rollback; automatic recommendation of service restoration solutions, service impact analysis, and configuration delivery, acceptance, and rollback on the basis of the fault- or network health analysis result.
- Intent openness: Besides some built-in intent templates, iMaster NCE-Fabric also provides a set of simplified and easy-to-use framework featuring great intent openness. Users can perform customized development of intent templates through GUIs. In addition, the developed scenario-based APIs can interconnect with the customer's trouble ticket system and NMS, and be integrated into the customer's IT environment.

The automation module functions as the core of autonomous driving networks at L2. Its dominant capabilities include Fabric as a Service (FaaS), openness, high performance, and high reliability.

- FaaS: iMaster NCE-Fabric is oriented as part of the overall network management system. It may be interconnected with various cloud platforms in the northbound direction, such as OPS, UI, and Kubernetes, and be interconnected with network devices in the southbound direction, such as switches, routers, and third-party value-added service (VAS) devices. Considering this, one of the keys of the automation module is to shield various differences and enhance scalability by abstracting northbound and southbound common models. In addition, FaaS provides dynamic network path calculation oriented at compute resources, and can automatically calculate and deploy east-west and north-south paths based on the specified location of compute resource such as VMs, bare-metal machines (BMs), and containers.
- Openness: iMaster NCE-Fabric constructs northbound and southbound openness on the basis of northbound and southbound common models.
- High performance: The automation module is fundamentally responsible for converting northbound models into southbound models, and is efficiency-centric. The module can process 10,000 northbound service requests concurrently within 1 minute. This capability is mandatory in container cloud and telco cloud scenarios.
- High reliability: The automation module also focuses on guaranteeing (southbound and northbound) end-to-end data consistency and quick rollback capabilities without sacrificing the system performance.

Simulation and verification module: As a highlight of autonomous driving networks at L3, this module concentrates on constructing a digital twin based on the physical DCNs, performing digital simulation on the execution of the critical user intent, verifying the expected intent execution results, and checking whether intent execution affects other services. This further ensures reliability of customer networks. Simulation and verification is oriented at the following scenarios: network planning verification, physical network verification, logical network verification, and fault rectification and verification. The core capabilities of this module include simulation and verification of online and offline configurations, post-event acceptance, and what-if:

- Simulation and verification of online configurations: Before automatically delivering network configurations, the simulation and verification module obtains southbound configurations, simulates intent execution, and verifies the intent execution result on the basis of the dry-run capability. The intent execution verification indicators include connectivity and impacts on the surrounding services.
- Simulation and verification of offline configurations: The simulation and verification module is decoupled from the surrounding modules. It can be independently deployed or integrated with customers' network systems. In addition, this module implements simulation and verification of the specific intent based on the user-imported topology, full configuration, and incremental configuration.
- Post-event acceptance: After converting the intent into network configurations, the simulation and verification module delivers these network configurations and verifies the configuration results through algorithms or dialing tests.
- What-if: This module helps users complete scenario-specific simulation rehearsal on the basis of the digital twin simulation environment, such as NE capacity expansion, NE go-offline, link interruption/switchover, and routing policy adjustment.

Intelligent analysis module: As one of the cores of autonomous driving networks at L3, this module implements network health analysis, quick exception discovery, and root cause locating on the basis of big data analytics-powered digital twin bases.

- **Health:** five-layer evaluation model concentrating on the device, network, protocol, overlay, and service; this model oriented at five dimensions: performance, capacity, status, security attack, and connectivity.
- **Quick exception discovery:** abnormal KPI, abnormal flow detection, and abnormal log.
- **Root cause locating:** locating the root cause from a large number of alarms based on the knowledge graph and machine learning, and reporting the root cause to the intent-driven decision-making module.

Data base: including the transaction relationship database, big data database, and correlation between the two databases.

3.2 Intent-Driven Decision-Making Module

3.2.1 Pain Points

Service network provisioning is difficult to be agile and the change effect is uncontrollable.

- When new services need to be provisioned, network O&M personnel cannot figure out the network requirements of the new services and need to spend a lot of time in communicating and clarifying with the service team. As a result, service network provisioning is difficult to be agile. In addition, network requirements vary depending on the service team and service. A single system cannot adapt to all services.
- If a network fault occurs, network O&M personnel cannot determine the fault impact and how to quickly rectify the fault and restore services.
- The network personnel also get difficulties in determining whether the current network resource capacity meets the requirements of the new services, whether the network usage is appropriate, and when to expand the network capacity.

3.2.2 Functions and Customer Benefits

The intent-driven decision-making module considers the intent management module as its core and provides the following functions:

- Intent identification
- How to convert the intent into network configurations
- Pre-event simulation and verification of the intent

- Post-event intent monitoring and diagnosis
- Fault rectification upon an intent assurance failure

The intent-driven decision-making module provides built-in intent templates that are commonly used in DCs. In addition, to better adapt to different user requirements, this module provides open programmability. In this case, users can customize new intent templates and assemble existing intent templates through workflows to form a new intent template. As the intent-driven decision-making module gets much more intelligent, the system gets stronger in identifying the intent. This also signifies that users need to enter fewer parameters. For example, 10 parameters are required to execute an intent originally. With this module configured, however, the number of parameters required decreases significantly because this module will automatically supplement some parameters on the basis of user-entered information (for example, three basic parameters), system status, actual network topology, and historical operations of users. In addition, the intent-driven decision-making module recommends intent templates that users may use based on the digital twin data. For example, the port capacity of a DC is insufficient and needs to be expanded. The existing switches in a DC are rather out-of-date and need to be upgraded. The system licenses are about to expire and need to be updated.

How does the intent-driven decision-making module monitor intent execution and perform intent loop-closure after the intent is delivered? The key to this question lies in the module's event-condition-action (ECA) management framework for intent loop-closure. The ECA management framework can implement loop-closure of the intent regardless of whether the intent is built-in or customized. The basic principle of the intent-driven decision-making module is as follows: After an intent is delivered, the module drives the intelligent analysis module to monitor the events defined by the ECA management framework. When a defined event occurs, the intelligent analysis module notifies the intent-driven decision-making module of executing the corresponding action based on the condition. Executing actions may bring risks. Therefore, the intent-driven decision-making module will evaluate risks of different actions using the decision-making algorithm. The process also involves the simulation and verification module. When the risk exceeds a certain threshold, the system provides different actions and simulation verification results for users so that users themselves can select the final action based on their requirements. If the risk level is low, the system automatically executes the action and checks whether intent loop-closure is completed. The system also records detailed logs of this automatic closed-loop event. Users can view the logs at any time.

The intent-driven decision-making module also provides the proactive network optimization function. As many more services are transmitted on the network, the network resource usage may not be optimal. With this in mind, the intent-driven decision-making module provides some network optimization suggestions on the basis of the digital twin data for reference. For example, the intent-driven decision-making module detects that loads between leaf nodes on the current fabric network are unbalanced. That is, some leaf nodes get busier in transmitting the sharply increasing traffic volume, while the traffic volume on some other leaf nodes is light. Against this backdrop, the module recommends that some servers connected to these busy leaf nodes be migrated to the idle leaf nodes to achieve load balancing. This example is only for reference because this suggestion is provided only from the network perspective. In actual scenarios, full

communication with the computing department is also mandatory before providing a suggestion. Customer benefits of the intent-driven decision-making module are as follows:

- User intent-oriented automation: reduces network configuration parameters, simplifies network operations, and shields differences between heterogeneous networks. As predicted by Gartner, the service provisioning efficiency can be improved by 50%.
- Open and programmable framework: supports quick intent customization to adapt to different customer scenarios, achieving more comprehensive intent coverage.
- Pre-delivery intent simulation + post-delivery intent monitoring and assurance: reduces the network error probability and service interruption time. As predicted by Gartner, the O&M workload will be reduced by 50%.
- Intelligent assistant: implements prediction and notification of common DCN maintenance actions, relieving network administrators' workloads.
- Network optimization suggestions: is used as a valuable reference for network administrators, guaranteeing the DCN health.

3.3 Automation Module

3.3.1 Pain Points

Multi-system resources need to be interconnected through numerous models, and large-scale networks are slow to provision and difficult to recover once faults occur.

- Different service logic models are interconnected. In SDN DCs, networks need to be provided as services to interconnect with multiple upper-layer service provisioning systems, such as the OpenStack cloud platform, Kubernetes container platform, VMware vCenter, and Microsoft System Center. The service logic models of different platforms vary greatly. In this way, the automation module needs to translate multiple service logic models into network configuration models and automatically deliver the network configuration models to corresponding network devices.
- Different networking models are interconnected. For example, centralized and distributed gateways can be deployed on a fabric network, VASs can be connected in bypass, inline, or remote mode, and leaf switches can form a stack or M-LAG to ensure reliability. The automation module must be able to identify the networking models and deliver different network configurations based on the networking models.
- Different network devices are connected. A data center network is configured with different models of hardware switches, vSwitches, and third-party VAS devices. The automation module is required to uniformly manage and orchestrate them.

- The scale of data center networks is increasing continuously. A typical fabric network can connect to a maximum of 2,000 servers and 200,000 to 50,000 VMs. The speed of concurrent provisioning of compute resources on the upper-layer platform is being accelerated. For example, Kubernetes can concurrently provision 10,000 containers per minute. As such, the automation module must be able to adapt to high-speed service provisioning.
- A data center network changes frequently. If an error occurs during the change, rapid rollback is the quickest method. The automation module needs to manage all configuration changes to implement snapshot-based rollback.

3.3.2 Functions and Features

The automation module of the autonomous driving system receives instructions from upper-layer systems and intent-based decision-making systems, converts the instructions into device configurations, and completes service network provisioning and network changes. The automation module provides the orchestration capability of the automation to implement mapping between intent models and network models, thereby converting the intent to network configurations. Configurations are submitted in two phases. In the first phase, the automation module decomposes the network models into specific device configurations. However, the configurations are not delivered to devices but is transmitted to the simulation and verification module to check the impact of the new configurations on the live network. The simulation and verification module verifies the following contents: manual input items and items automatically generated by the automation module based on the delivered intent and change records. After the verification is successful, the automation module delivers the configurations to devices. This prevents incorrect configurations. Of course, simulation verification also consumes resources. Users can determine whether the current configurations need to be simulated and verified based on site requirements. The low-risk intent configurations can be delivered without simulation and verification. The automation module provides the following functions:

- Southbound and northbound openness: The automation module provides Fabric as a Service (FaaS), including underlay and overlay configurations in a fabric, which provides a unified entry for all changes. FaaS provides open expansion capabilities based on a unified model and provides a unified northbound model for upper-layer systems and a unified model for lower-layer devices. FaaS also provides open programming capabilities and performs specific configurations on NEs of heterogeneous vendors to decompose upper-layer intent into configurations.
- High reliability: The automation module provides the network snapshot function. All network changes are stored with corresponding historical records. When an error occurs on network change, the changes can be quickly rolled back to reduce the network interruption time. In addition, the automation module provides the southbound and northbound data consistency verification function to ensure end-to-end data consistency and further enhance reliability.
- High performance: The automation module supports a large number of concurrent requests, among which the number of concurrent northbound requests reaches 10,000 per minute, matching needs of high-speed service delivery of the upper-layer systems.

3.4 Simulation and Verification Module

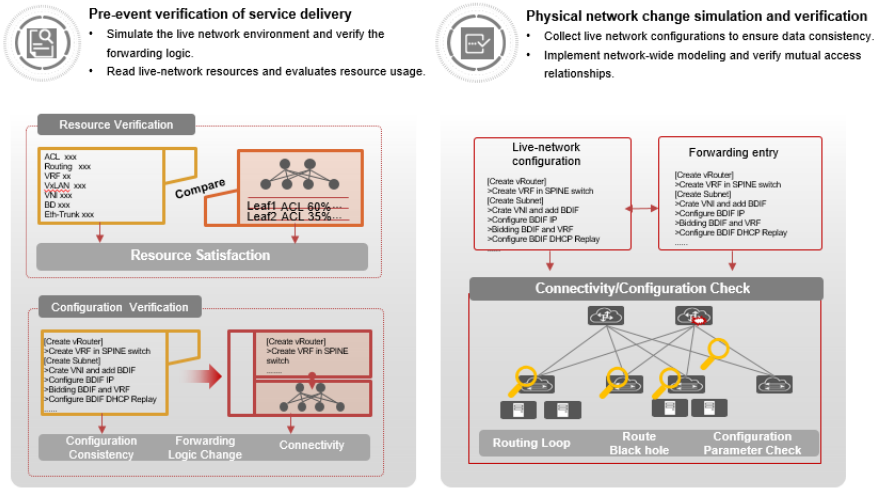
3.4.1 Pain Points

For cloud data centers, cloud services must be always online, which is the most concerned issue of customers. However, nearly half of faults on data center networks are caused by configuration changes. Device simulation involves a high cost and consumes many resources, which is difficult to quickly respond to service requirements. There are the following disadvantages:

- **Service faults caused by changes**: According to Gartner statistics, 40% of network accidents in the data center field are caused by manual configuration errors. The network management department takes an average of three days to assess the risks of a network change, but the accuracy is only about 70%.
- **High simulation cost**: Devices in a data center network have complex functions and various models. Traditional simulation is costly because it needs to simulate different functions of different devices and complex routing protocols. In addition, different device models have different implementation mechanisms, making simulation more difficult.
- **Resource-consuming and slow response**: Simulation of devices on the control plane consumes a large number of compute and memory resources. When multiple devices are simulated, the time consumption increases exponentially and the response is slow.

3.4.2 Functions and Customer Benefits

Simulation and verification, as a key technology of Huawei data center autonomous driving system iMaster NCE-Fabric, plays an important role in planning and design, automatic decision-making, expert recommendation, and fault rectification. It provides pre-event simulation analysis of decisions and the intent to verify their feasibility and impact, and also supports offline simulation analysis on physical network changes and planning, helping quickly identify potential risks based on the service intent. It has the following advantages:



- **Physical network change simulation and verification:** Supports data modeling for managed physical networks and displays the overall network status on the GUI. The system checks new physical configuration parameters of the network to automatically discover faults on network connectivity, routing loops, and routing blackholes. No manual intervention is required.
- **Pre-event verification of service delivery**: Analyzes resource usage for the service intent, and automatically calculates the resource consumption of current services and the overall resource status of the current network. In addition, it checks whether the service intent configurations conflict with the current services and simulates and verifies the configurations, helping users analyze impacts and make decisions. It can also simulate the complex access control policies on a data center network. For example, PBR-based SFC and microsegmentation, simplifying management of these access control policies.
- **Efficient and fast**: Supports lightweight simulation, which occupies few resources and is easy to deploy. The verification and simulation module of iMaster NCE-Fabric has built-in OSPF and BGP algorithms commonly used by data center networks. It uses the binary decision diagram (BDD) to build a graphical connection model of the network and implement fast and efficient verification. This meets requirements on data simulation of different scales. BDD is a data structure that is used to represent a Boolean function and can efficiently perform intersection, union, and difference calculation of Boolean functions.
- **Openness and collaboration**: Supports online and offline simulation and verification. The simulation and verification module can work with other modules of iMaster NCE-Fabric. This module extracts a set of models irrelevant to device models. In the future, the simulation and verification module can be applied to third-party devices.

3.5 Intelligent Analysis Module

3.5.1 Challenges

With the development of cloud-based DCs, network resource pooling and network service automation bring more convenience to users. However, they also bring challenges to proactive, real-time, and large-scale network O&M. As a result, the traditional O&M system cannot ensure consistent service experience or fault location. The challenges are as follows:

- **Proactive:** In SDN scenarios, services need to be provisioned quickly and dynamically. For example, if logical networks are created and deleted as required, network or service configuration changes frequently. Frequent configuration change increases the fault probability. The O&M system must be able to proactively and intelligently detect faults, and use big data analytics and experience databases to help users quickly locate and rectify faults.
- **Real-time:** The O&M system can detect microburst exceptions on a network in a timely manner. For example, an enterprise customer complained that its lightweight network had the issue of transient packet loss and suspected that there were millisecond-level traffic bursts. However, these issues cannot be detected or optimized through the minute-level SNMP mechanism.

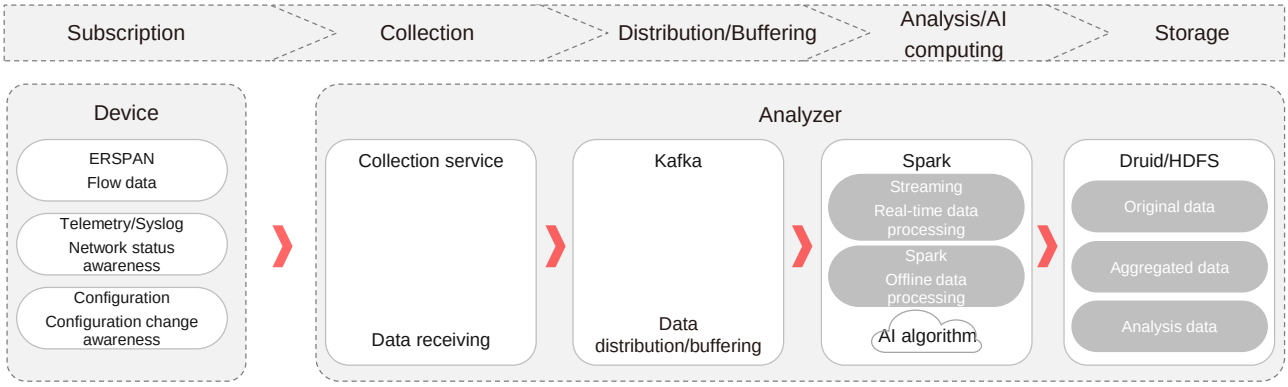
- **Large-scale:** Large-scale management involves the following aspects. On one hand, managed objects are extended from physical devices to VMs and the NE management scale is increased by dozens of times. On the other hand, the device indicator collection granularity is improved from minutes to milliseconds to meet real-time analysis requirements, and the data volume is increased by nearly 1000 times. For active awareness and troubleshooting of issues, the system needs to collect and analyze network device indicators, and analyze the actual forwarding service flows, further increasing the data scale.

The traditional O&M management system is challenged by the preceding three features of SDN network O&M. According to a survey conducted by the Enterprise Management Associates (EMA) on over 100 enterprises, about 70% of customers are concerned about whether the existing network O&M system is applicable to SDN scenarios.

Faced with the preceding O&M challenges (proactive, real-time, and large-scale) in the SDN scenarios, the overall O&M architecture needs to be changed to make the SND network easy to use.

3.5.2 Functions and Customer Benefits

The intelligent analysis module uses Telemetry technology to collect data on the data plane, control plane, and management plane in all scenarios in real time, uses the distributed architecture to perform real-time and offline computing, and uses intelligent algorithms to analyze and display network data, processing of millions of packets in seconds. Different from the traditional resource status monitoring mode, the analysis module detects the fabric network status and application behavior status in real time, comprehensively evaluates the network health, and identifies, locates, and rectifies faults in minutes.



- **Network health analysis and proactive fault prevention**: The analysis module establishes a detailed evaluation and health analysis system from five dimensions (device, network, protocol, overlay, and service), builds a comprehensive network monitoring and evaluation system, and periodically pushes evaluation reports. Compared with the traditional system which uses fixed thresholds, the analysis platform uses the machine learning algorithm to detect network behavior changes. Based on historical network data, the analysis platform uses the Gauss process regression

algorithm to automatically learn dynamic baselines of KPIs from multiple dimensions, such as devices, cards, ports, and optical modules, and update the baselines every day, implementing intelligent detection of network exceptions. In addition, the analysis platform constructs multi-event association analysis based on dynamic correlation between KPIs. It detects behavior changes in the network sub-health phase in a timely manner, and predicts and prevent faults before they occur.

- "1-3-5" troubleshooting and fault locating in minutes: Based on over 30 years of O&M experience and thousands of fault cases, Huawei sorts out over 75 fault cases, covering 85% fault scenarios. On the one hand, the analysis platform continuously carries out DC attack-defense drilling to accumulate fault knowledge and improve fault locating efficiency. On the other hand, the analysis platform uses AI to build network knowledge graph. Currently, the root causes of typical faults can be located within 3 minutes.
- Network-wide full-flow analysis and visualized application behavior exceptions: The analysis platform collects and analyzes TCP packets forwarded on the network, displays application interaction relationships and quality, and white-boxes network traffic. The Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm is used to perform clustering analysis on application flows on the network, restore the hop-by-hop forwarding paths of packets and the forwarding traffic and delay of links, and construct multi-layer association and analysis capabilities from service flows, forwarding paths, to network services, presenting application behaviors and network quality to users in a structured manner.

3.6 Data Warehouse

The data warehouse is used to collect historical data of iMaster NCE-Fabric and network data of other systems, for example, configurations of devices that are not managed by iMaster NCE-Fabric or manually delivered by users, and information about server status and network status. The collected original data can be used as the data source for data mining and AI learning. For example, iMaster NCE-Fabric learns the impact of historical network configurations on network operating and provides an optimal network planning solution. It then uses the data warehouse to further process the original data to obtain modeled data in tree structure. Modeled data helps compare historical data and display results, enhancing the automatic driving capability. For example, snapshot-based rollback can be performed at any time or in any range without saving the snapshots. Users can customize multi-dimensional data views based on the modeled data and detect the differences between the configurations of managed devices on iMaster NCE-Fabric and the actual configurations and report alarms.

3.7 User Experience

3.7.1 User Experience Pain Points of Traditional O&M Systems:

- Due to the increase of network scale and complexity, errors may occur when network administrators (users for users)

manually perform network changes on the system. Currently, more than half of network exceptions are caused by network changes.

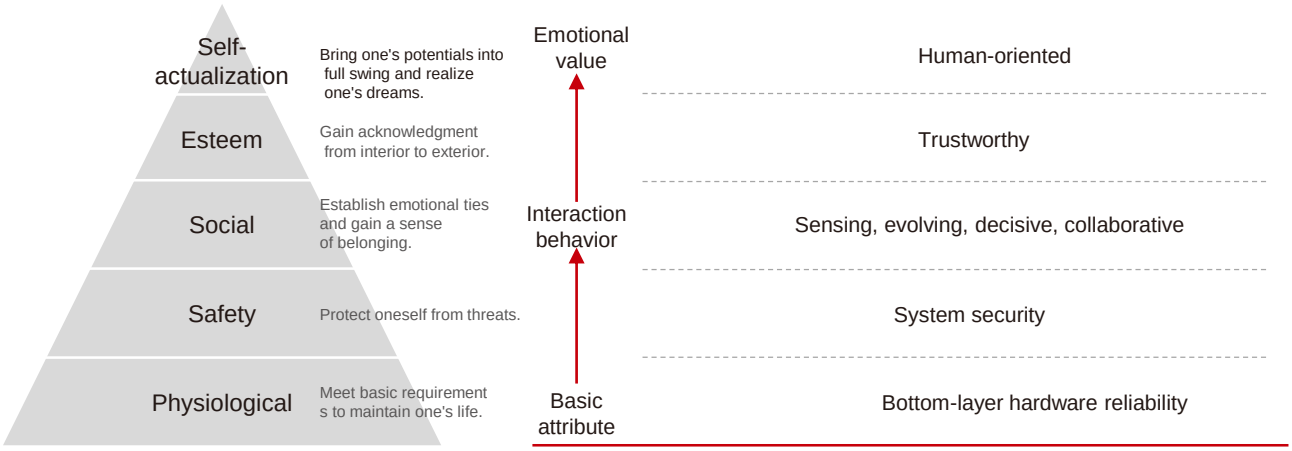
- Capacity expansion requires manual operations and verification in the system. Therefore, the correctness of configured resources cannot be ensured, which may cause configuration errors and conflicts.
- In financial service scenarios, especially for core services, faults must be detected and located within minutes. It is difficult for users to detect and locate faults based on manual experience.

3.7.2 Data Center Network Autonomous Driving System:

The intent-driven autonomous driving system integrates intent-driven decision-making (quick and intelligent recommendation of fault rectification solutions and intent-based full-lifecycle loop closure), simulation (digital twin-based simulation experience), and intelligent analysis (unified monitoring and quick fault discovery and locating). This gradually reduces the proportion of manpower in O&M operations.

In the future, the autonomous driving system will interact with users as an independent individual to help users work efficiently, accurately, and intelligently. This improves network quality and O&M efficiency, and improves O&M experience of users.

The autonomous driving system complies with core elements of user experience: Sensibility, Decidability, Evolvability, Collaborability, Trustability, and Humanability (6-Abilities).



Maslow's hierarchy of needs

DCN autonomous driving intelligent model

Sensibility: Provides channels such as information text, 2D/3D images, natural language conversation, and tactile vibration for users to perceive system behaviors.

Decidability and Evolvability: Learns independently and helps users perform inference and decision-making.

Collaborative: Provides intelligent identification and prediction capabilities, enabling users to interact and collaborate with each other to complete DCN management.

Trustability: Builds a trustworthy autonomous driving system through trustworthy appearance, behavior, and emotion.

Humanability: Ensures that system behaviors respect human rights and ethical norms and behavior decision-making complies with human values to reduce users' privacy concerns and build a secure AI system.

3.7.3 User Experience Improvement Points and Customer Benefits:

- The autonomous driving system detects and identifies the user intent (such as service provisioning) through natural language. The system simulates and verifies the deployment solution to ensure solution feasibility, and recommends solutions for users, helping users make decisions and complete service provisioning. Further, if the recommended solution of the system is gradually trusted by users, the system may be allowed to independently determine and deliver the solution. As a result, users' investment in service provisioning is reduced and the correctness of service provisioning is ensured.

- The autonomous driving system detects the capacity expansion requirements and plans a capacity expansion solution that has been simulated and verified based on the resource usage on the live network. This helps users determine the most appropriate solution to ensure successful capacity expansion. After the capacity expansion, the system automatically verifies the capacity expansion and outputs the result so that users can know the progress and result of the capacity expansion. In this way, a large quantity of manual operations and verification during capacity expansion are avoided. That is, an effective capacity expansion solution can be quickly determined, and correctness of configuration resources can be ensured, thereby avoiding configuration errors and conflicts in advance.

- The autonomous driving system can proactively detect the status of various services and the entire network, quickly identify and locate events, and intelligently recommend fault rectification plans that have been simulated and verified. Some events can be configured to be automatically completed by the system. Users only need to sense the progress and result. This frees them from heavy network O&M workload.

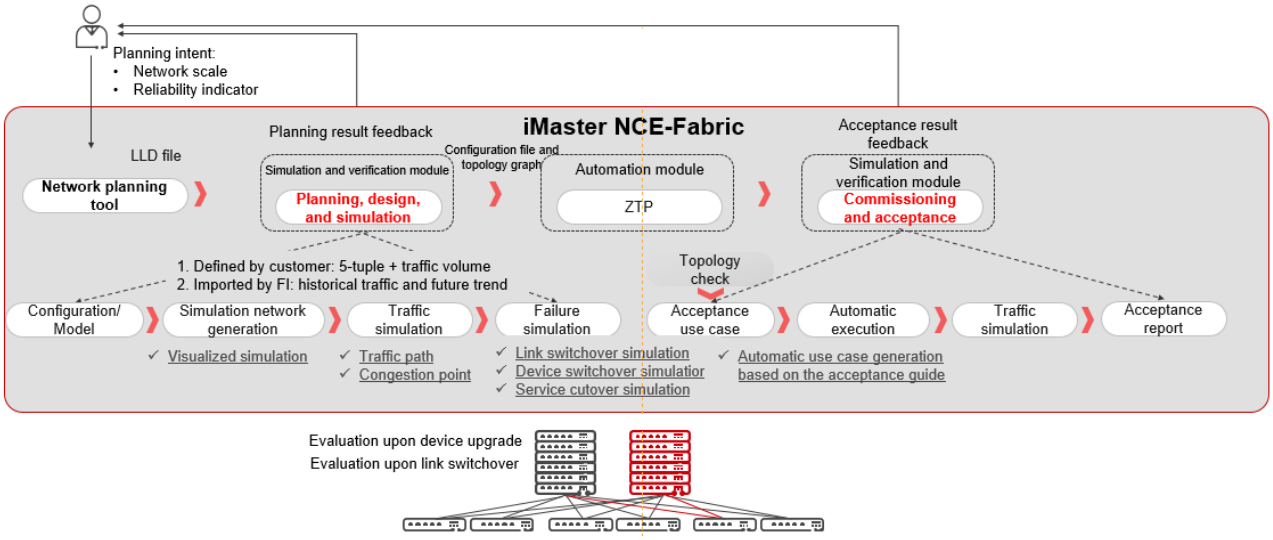
04

Typical Application Scenarios of Huawei Autonomous Driving Network

4.1 Planning and Construction: Planning, Design, Simulation, and Automatic Acceptance

4.1.1 Scenario Description

In the planning phase, the network department needs to design the DCN architecture, device selection, and system collaboration based on service requirements of the data center to be constructed, such as the planned service volume, security, network performance, technology evolution, and long-term capacity expansion. In the construction phase, the network administrator needs to complete hardware installation and testing, software installation, and joint commissioning based on the low level design (LLD), and output an acceptance report.



4.1.2 Pain Points

1. In the planning phase:

- Professionals are required to plan the networking solution, including the connections between border nodes and external networks, the oversubscription of leaf and spine nodes, and connections between leaf and spine nodes, involving heavy workload. The operations are inefficient and error-prone, and difficult to be verified.
- No actual device or networking is deployed in this phase. The network administrator analyzes only the number of servers that can be deployed on the network, server access reliability, and network access path theoretically. The network performance after construction cannot be evaluated intuitively, and whether planned services can be carried on the network cannot be ensured.

2. In the construction phase:

- Configuration files need to be imported to spine and leaf nodes one by one, which is time-consuming.
- A large number of test cases need to be manually executed to verify whether the network meets the planning requirements, consuming a lot of manpower and time.

4.1.3 Solutions

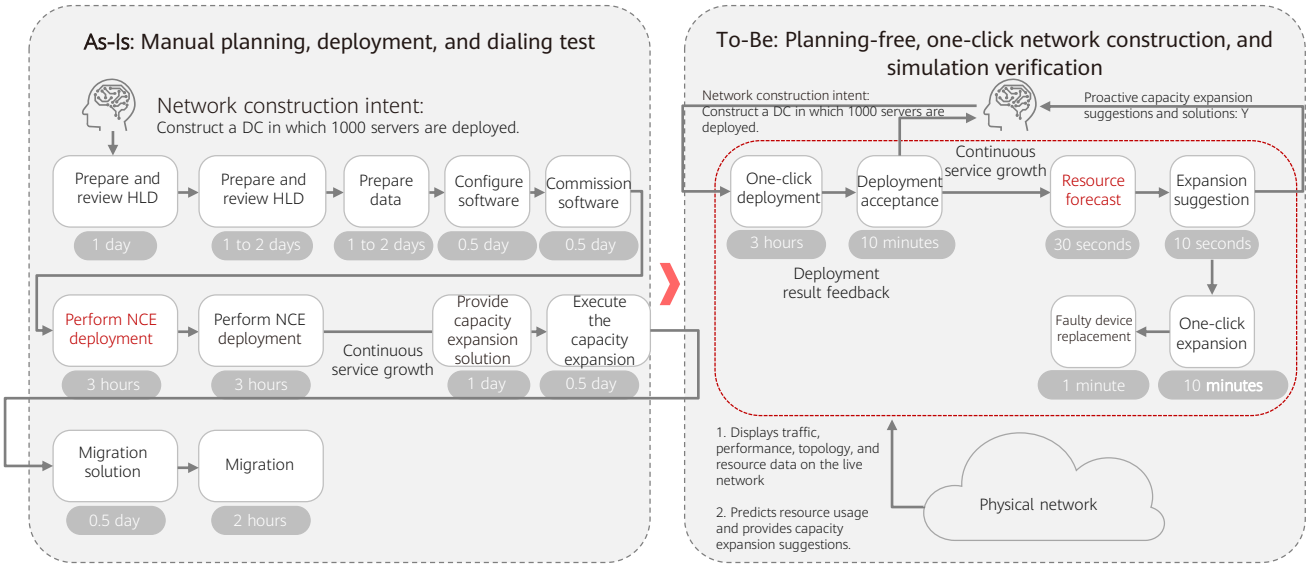
1. iMaster NCE-Fabric supports network planning (such as network scale and reliability indicators) and input of the network planning tool (LLD). The simulation and verification module of iMaster NCE-Fabric can automatically generate a simulation network using the digital twin technology. Traffic path simulation and network failure simulation can be implemented on the simulation network, such as reliability for link or device switchover. The visualized simulation result allows the network administrator to fully confirm the network planning results and adjust the network planning based on the detected problems until the simulation result meets the expectation. In this way, the problem that the evaluation is not intuitive and the verification is difficult has been resolved.

2. After the network administrator confirms the network planning results, devices only need to be powered on as planned. The ZTP deployment component of the automation module brings the devices online automatically. After all devices on the network go online, the simulation and verification module automatically generates acceptance test cases, executes the test cases for traffic dialing tests, and automatically generates acceptance reports. In this way, the device online efficiency is improved and the acceptance workload is reduced.

3. After the network is constructed, the intelligent analysis module of iMaster NCE-Fabric can also predict the network capacity and provide suggestions for network capacity expansion. In addition, when the analysis module detects a device fault, the system automatically migrates configurations of the faulty device to a new device.

4.1.4 Customer Benefits

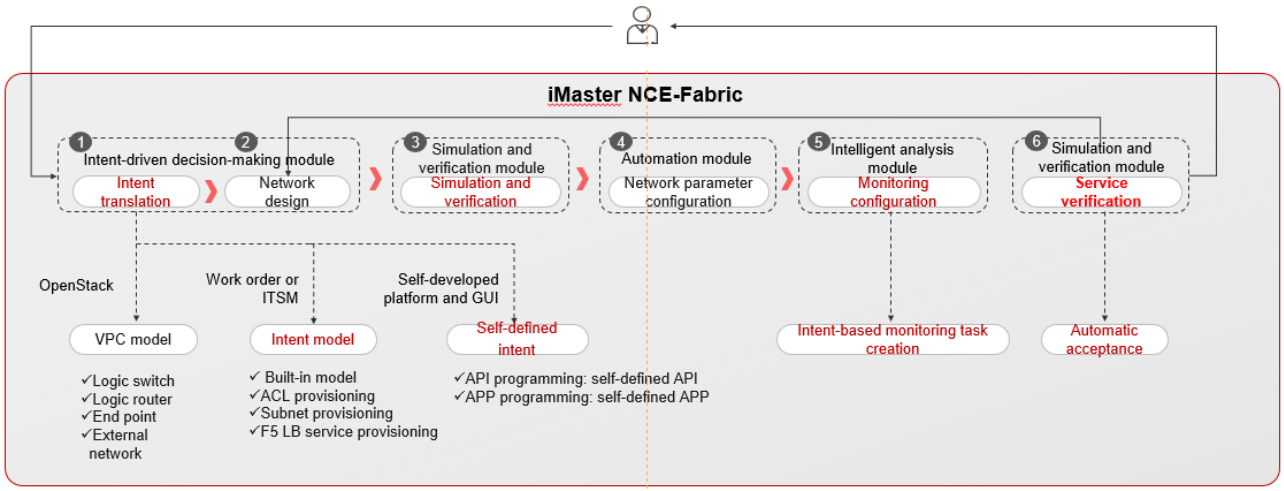
As shown in the following figure, iMaster NCE-Fabric eliminates a large number of manual operations, shortening the planning and construction time by 80%, reducing the planning error rate to less than 5% and rework, and improving the overall efficiency in the planning and construction phase. The system also proactively predicts device capacity expansion and device replacement upon exceptions.



4.2 Maintenance: Automatic Translation of Service Intent, Automatic Acceptance, and Rollback Upon Exceptions

4.2.1 Scenario Description

Scenario description: The system delivers network configurations based on network requirements raised by the IT or service department to complete service network provisioning required by users.



4.2.2 Pain Points

- Service network provisioning requirements are diversified, which cannot be covered by built-in functions. Network provisioning often involves fabrics and devices of different vendors. A single system cannot implement E2E automation, requiring a large number of manual operations.
- Network change risk is high. The manual operation accuracy is only 70% and misoperations may cause service interruption, resulting in high-risk network changes.
- The O&M monitoring capability is weak after the network is provisioned. The network department cannot know the actual network running status.

4.2.3 Solutions

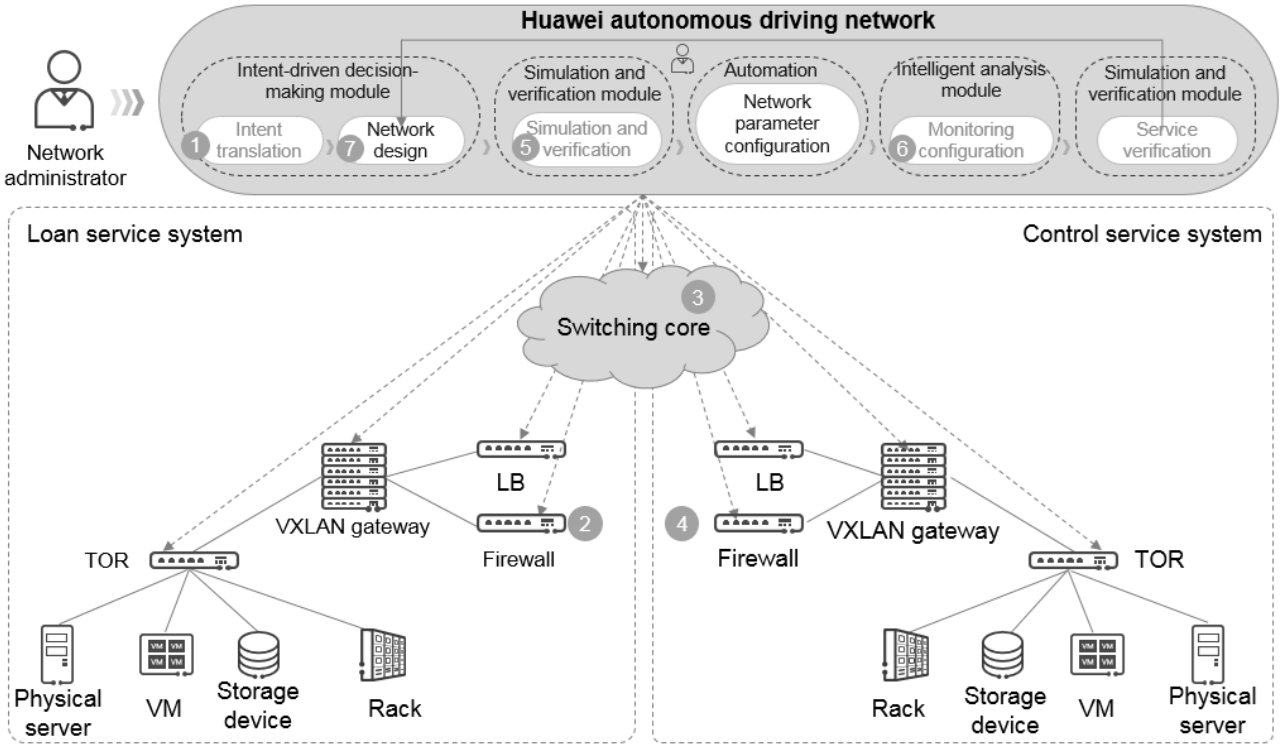
1. Based on the service provisioning intent, which is built-in or customized through open programmability, the intent-driven decision-making module of iMaster NCE-Fabric translates intent in a unified manner and designs the network. Finally, the intent is converted into configurations of multiple devices of different types (such as switches, firewalls, and LBs) on multiple fabric networks.

2. The simulation and verification module is used to simulate the network configurations generated in the previous step. Users can confirm or adjust the service provisioning intent based on the simulation result until the simulation succeeds. The automation module then decomposes and delivers the configurations to multiple devices, and ensures transaction-level consistency of service intent. All configurations should be delivered successfully; otherwise, they need to be rolled back. After the configurations are delivered, the intent-driven decision-making module decomposes and delivers service monitoring configurations to the intelligent analysis module and drives the simulation and verification module to verify the services.

4.2.4 Example

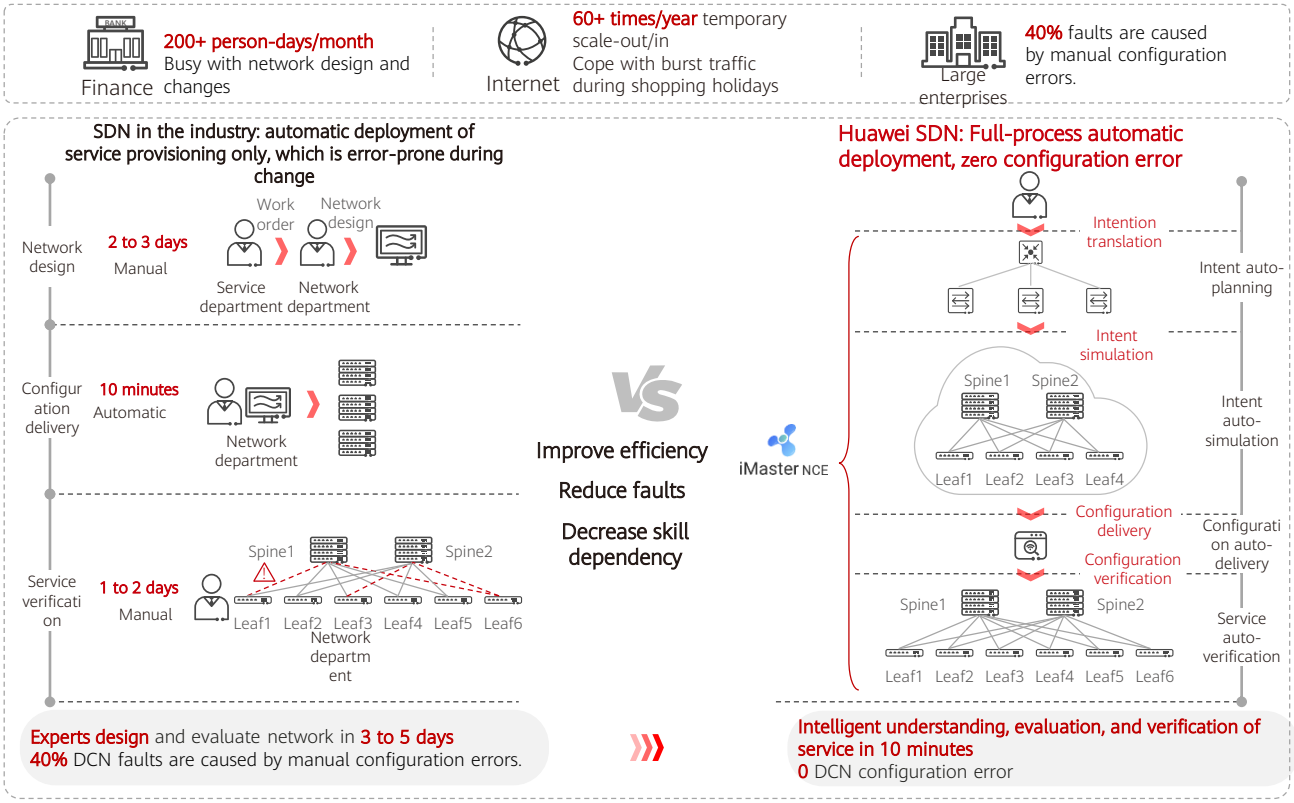
The following uses a financial DCN as an example to describe the service provisioning process. For example, the loan service system needs to access the risk control system. In iMaster NCE-Fabric, the network department only needs to deliver the mutual access requirements of services to the intent-driven decision-making module. The intent-driven decision-making module automatically performs the following operations:

:



- Query the IP addresses and port numbers of loan service and risk control systems and fabric networks where the systems are deployed.
- Configure an ACL with 5-tuple information on the firewall deployed on the fabric network where the loan service system is located. The source IP address is the IP address of the loan service, the destination IP address and port number are those of the risk control system, and the protocol is TCP.
- Query the fabric networks and switching core through which services are transmitted from the loan service system to the risk control system to ensure that the route is reachable. If no route is available, deliver the route in advance.
- Configure an ACL with 5-tuple information on the firewall deployed on the fabric network where the risk control system is located. The destination IP address and port number are those of the risk control system, and the protocol is TCP.
- In steps 1 to 4, configurations to be delivered are saved to the database. In this case, perform pre-event simulation for services on the entire network and check whether the simulation result is correct.
- Deliver services after the simulation result meets the expectation. After network configurations are delivered, deliver the service monitoring configuration, simulate traffic for dialing tests, and feed the results back.
- Trigger the fault closed-loop system if a service exception is detected

4.2.5 Customer Benefits

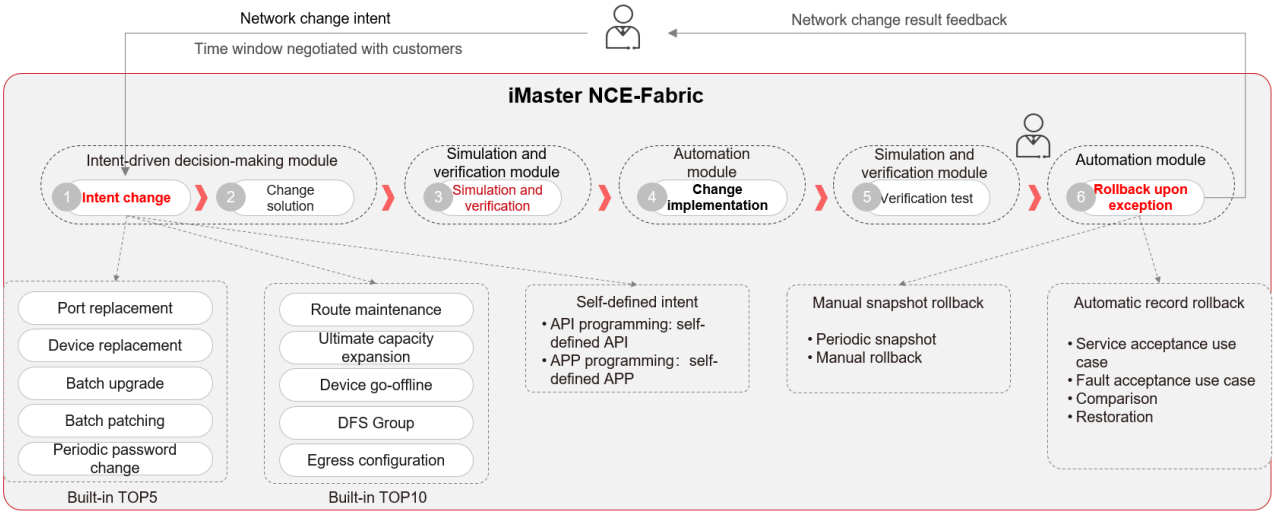


iMaster NCE-Fabric implements intent-driven network configurations, hides network implementation details, shields differences between vendors, achieving more agile service provisioning and simplifying network operations. As shown in the above figure, it takes three to five days to provision a typical traditional service, which is error-prone. After iMaster NCE-Fabric is used, it takes 10 minutes to provision a service and no configuration faults occur.

4.3 Maintenance: Built-in Common Network Change Intent and Quick Rollback Upon Exceptions

4.3.1 Scenario Description

Based on the live network services and network status, network personnel formulate and implement network change solutions (such as hardware replacement, software upgrade, and route switchover).



4.3.2 Pain Points

- The time for network changes is short and higher change efficiency is required. Currently, most network changes are performed manually, which is time-consuming (several hours).
- Misoperations may cause service interruption on the live network, and the accuracy of manual rollback operations is not 100%, resulting in high-risk network changes. In addition, it takes hours to recover service interruption caused by network changes.
- A lot of network change operations are performed on devices, which cannot be covered by the built-in function.

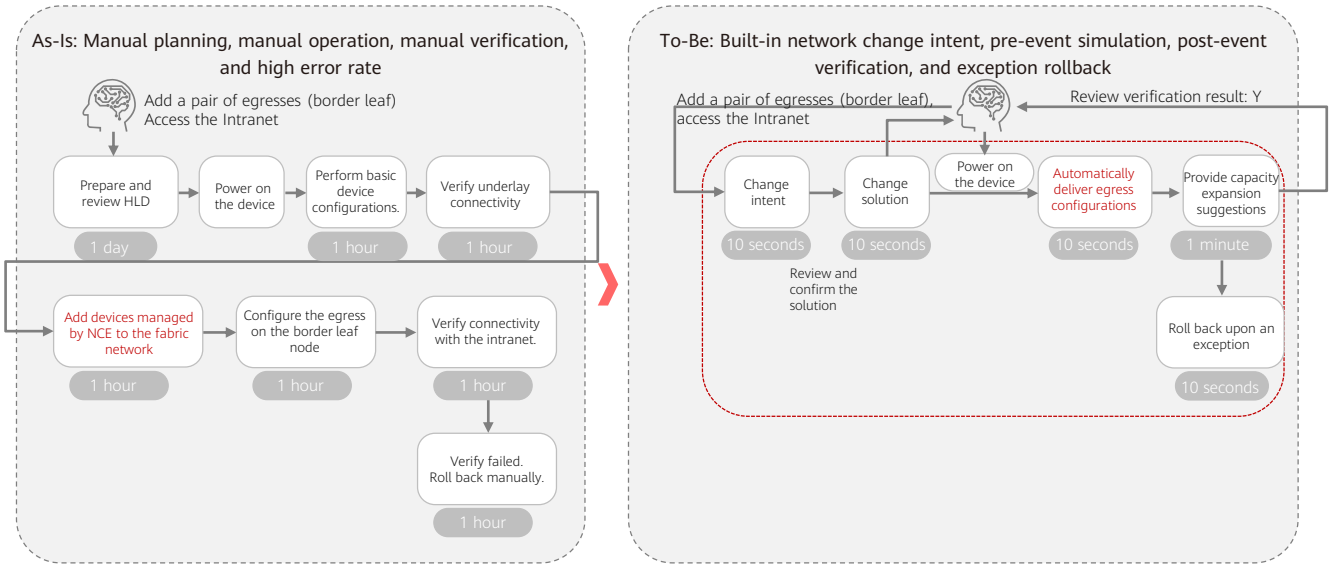
Different from network operations in the service provisioning phase, maintenance operations for network changes are proactively initiated by network personnel. Generally, network changes involve batch operations on devices, such as hardware replacement, software upgrade, route switchover, and network capacity expansion. iMaster NCE-Fabric provides optimal intent-driven operation experience upon network changes, and has built-in top 10 change operations commonly used in the data center. Other operations can be quickly adapted through open programming.

4.3.3 Solutions

- The intent-driven decision-making module decomposes change intents into network change solutions, specifies the devices and operations involved in the solutions, and inputs the operations to the simulation and verification module for simulation.
- The simulation & verification module displays the simulation result. After the result is confirmed, the automation module implements change solutions. If the simulation result does not meet the expectation, manually adjust the network to ensure that the network changes meet the expectation.
- After the changes are complete, the post-event acceptance component of the simulation and verification module performs a service dialing test and displays the test result. If the test result does not meet the expectation, the automation module performs rollback to the previous snapshot or the snapshot automatically recorded by the system to ensure that the system can quickly roll back to the status before the change upon an exception.

4.3.4 Customer Benefits

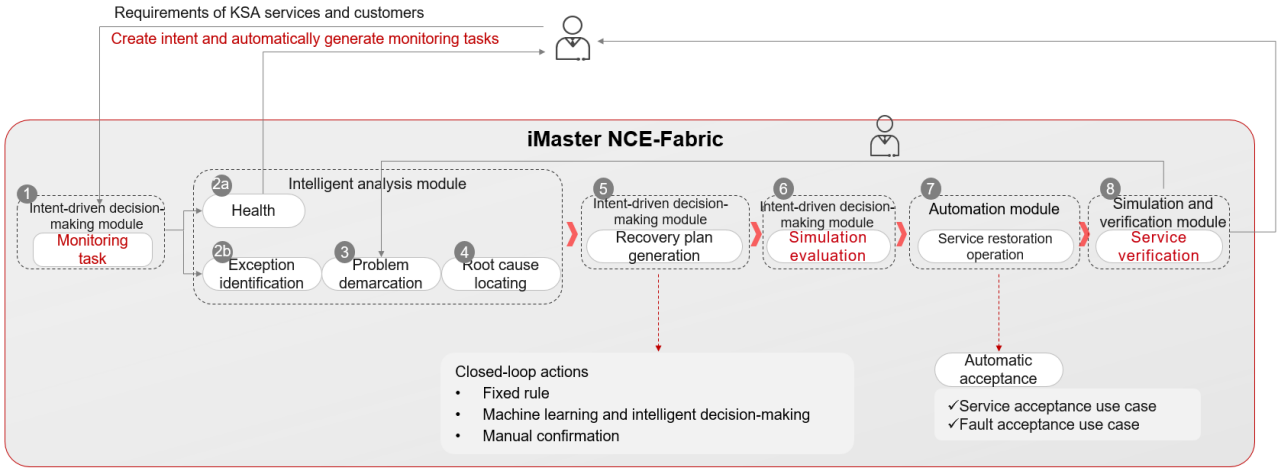
iMaster NCE-Fabric implements reliability simulation and automation of change operations, improving change efficiency and shortening the time required for common network changes in DCs from hours to minutes. In addition, the system quickly rolls back configurations after an exception is detected, minimizing the service interruption duration caused by change failures. The following figure shows the effect in the DC expansion scenario.



4.4 Maintenance: Intent-driven Network Monitoring, Implementing Fault Closed-Loop

4.4.1 Scenario Description

After network configurations are delivered or the network is changed, users monitor the network running status regularly. If a network fault occurs or performance deterioration is detected, users need to locate and rectify the fault, and verify fault rectification.



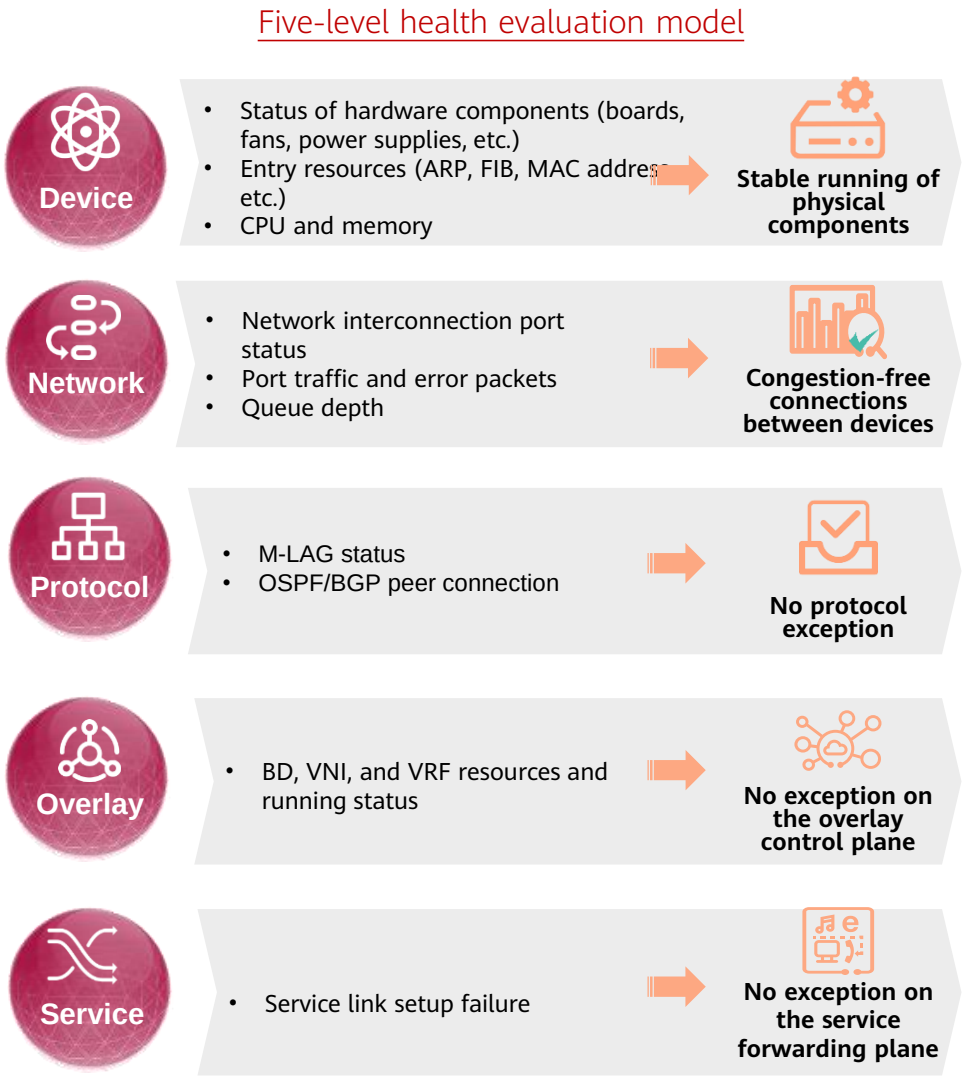
4.4.2 Pain Points

- The DCN is complex and involves a large number of devices. If a network fault occurs, maintenance personnel need to analyze a large number of alarms on devices in traditional O&M mode. It takes several hours to locate and troubleshoot the fault.
- The recovery plan is provided based on experience and reviewed by experts, so the accuracy rate is only about 70%.
- Fault rectification requires manual operations, which is inefficient and time-consuming. It takes 5 hours to rectify a fault on average.
- After the rectification operation is performed, maintenance personnel need to verify whether the fault has been actually rectified. Due to many verification points and low efficiency, it takes hours or even days to versify services.

Based on the monitoring rules and intent proactively delivered by users, the autonomous driving system can automatically generate monitoring tasks during service creation. It can also detect network exceptions in real time, locate and output root causes, and automatically rectify and verify the faults. The system aims to detect faults within 1 minute, locate root causes within 3 minutes, and automatically performs fault closed-loop within 5 minutes.

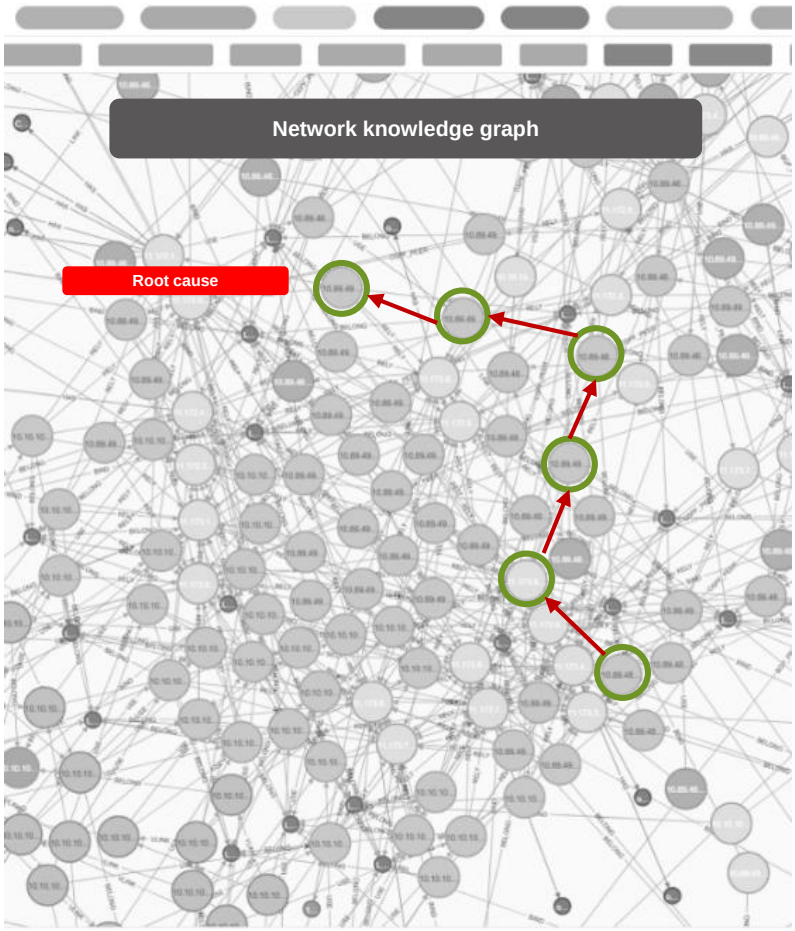
4.4.3 Solutions

1. The intent-driven decision-making module automatically creates a monitoring task based on service intents during network configuration delivery or network changes. (Users can view or create monitoring tasks.)



2. The intent-driven decision-making module delivers the monitoring task to the intelligent analysis module and performs big data analysis on collected TCP flows and Telemetry performance metrics through real-time and offline computing. In addition, the intent-driven decision-making module proactively detects possible issues on the fabric based on AI algorithms such as baseline exception detection and multi-dimension cluster analysis and the five-level model consisting of device, network, protocol, overlay, and service, and intelligently analyzes and identifies whether a network or an application has issues that occur on a large scale.

Network knowledge graph



3. Based on 30+ years of O&M experience and thousands of fault cases, Huawei sorts out 75+ fault cases, covering 85% of fault scenarios. On the one hand, the analysis platform continuously carries out DC attack-defense drilling to accumulate fault knowledge and improve fault locating efficiency. On the other hand, the platform builds network knowledge graph through AI learning and reasoning. Furthermore, after detecting a fault, the analysis module performs root cause analysis according to the knowledge graph of fault propagation, and reports the root cause to the intent-driven decision-making module.

4. The intent-driven decision-making module needs to generate a service recovery plan based on the root cause of the fault. For faults with clear closed-loop actions, the built-in fixed rule that describes mappings between root causes and service recovery plans is used. For faults with unclear closed-loop actions, the machine learning-based intelligent decision-making technology is used to intelligently recommend the service recovery plan based on historical records.

5. After the service recovery plan is generated, the simulation and verification module performs simulation and evaluation and displays the simulation result to the network maintenance personnel. The maintenance personnel select a service recovery plan and submit it to the automation module.

6. After the service recovery plan is executed, the simulation and verification module confirms the effect.

4.4.4 Customer Benefits

- Faults are automatically detected and root causes are located without manual operations, shortening the fault detection time from minutes to seconds and fault locating time from hours to minutes.

- Based on intelligent recommendation and decision-making, the system recommends the optimal service recovery plan, avoiding inaccurate fault solution formulation and shortening the closed-loop time from days to minutes.

- After the service recovery plan is manually confirmed, the system automatically executes the plan and acceptance test cases, shortening the verification duration from hours to minutes.

Huawei Technologies Co., Ltd.
Huawei Industrial BaseBantian, Longgang
Shenzhen 518129 People's Republic of China

TEL: +86 755 28780808
http://e.huawei.com

Trademarks and Permissions

Notice: