IP Network Digital Map

White Paper

Contents

03 Typical Usage Scenarios and Key Technologies /22

04 Industry Suggestions and Conclusions /46

05 References /49

06 Glossary /50

1 Trends and Challenges of IP Networks

1.1 Trends: IP Network Digitalization

Digitalization is being used to address all manner of challenges in today's world full of change and uncertainty. The need for digital development has become a global consensus. More than 170 countries have already formulated national digital strategies. According to McKinsey statistics, global digitalization is seven years ahead of schedule (10 years in the Asia-Pacific region). The pace of digitalization of communication service provider (CSP) and enterprise services is 20–25 times faster than expected. Hybrid work, hybrid education, and augmented social media and entertainment will become new norms.

As the foundation of digital infrastructure, network connectivity is playing an increasingly important role in advancing digital transformation across different industries. The total number of global connections may reach 200 billion by 2030, as networks evolve from connecting tens of billions of people to connecting hundreds of billions of things. New services such as next-generation human-machine interaction (AR/VR/XR), integration of housing and transportation, industrial interconnection, satellite broadband interconnection, and artificial intelligence (AI) computing, will emerge and create new requirements for network connections. A potential direction is a green network featuring native intelligence, holographic visualization, deterministic experience, high security and reliability, and convergent awareness and automation.

From the perspective of CSPs, digital transformation presents huge opportunities in the 5GtoB and cloud-network convergence markets. At the same time, it increases their social responsibility for sustainable development. These changes create new requirements on the network and O&M capabilities of CSPs, spurring their construction of automated networks.

5G

5GtoB services create new requirements on network capabilities.
According to Keystone Strategy's report, the global 5GtoB market for CSPs will reach US$602 billion by 2025. 5GtoB services are becoming more sensitive to connection density, rates, delay, reliability, mobility, positioning accuracy, etc.

For example, a smart city requires a connection density of 100,000 to 1 million devices/km3, drones require 500–1000 km/h mobility, autonomous driving requires submeters-level positioning accuracy and an end-to-end (E2E) delay of no more than 5 ms, and industrial Internet requires 99.999% reliability. For network capabilities, 5GtoB services have three major requirements:

(1) One network meeting the highly differentiated connection requirements of millions of applications in a myriad of industries

(2) Online one-stop, on-demand, real-time, flexible subscription, provisioning, and change

(3) E2E deterministic service-level agreements (SLAs) that can be promised and guaranteed

Cloud

Cloud-network convergence moves massive data to the cloud.

Gartner predicts that in 2023, end users worldwide will spend as much as US$ 591.8 billion on public cloud services, a 20.7% increase over the previous year's US$490.3 billion. In the past two years, cloud-network convergence has become an important choice for enterprises seeking cloudification. Vertical industries have three requirements on cloud-network capabilities:

(1) Enterprises need to be able to use a global private or public network to quickly migrate massive data to the cloud while guaranteeing data security.

(2) One-point access to one or multiple clouds needs to be implementable for any service anywhere. Cloud-network business must be able to achieve integrated provisioning, integrated operation, and integrated service.

(3) The distributions and dynamics of global cloud-network computing power need to be perceivable and predictable in real time, and computing power needs to be intelligently scheduled to meet the differentiated requirements of industries and enterprises on convenience, quality, cost, security, etc.

Green

Green economy relies on energy saving and emission reduction on networks.

The European Union (EU) has estimated that the global ICT industry accounts for 5%–9% of electricity consumption and over 2% of greenhouse gas emissions. Energy saving and emission reduction have become the top priority for global CSPs striving to reduce costs and fulfill social responsibilities. For energy saving, the following capabilities are indispensable: self-formulation of energy-saving policies in specific scenarios, self-configuration of parameters, and network-wide coordinated energy saving.

1.2 Challenges in IP Network Digitalization

Complex O&M for multi-vendor networks:

More than 80% of IP networks use devices from multiple vendors. Even devices supplied by the same vendor may have different models and versions. Furthermore, one device may use different protocols. The complexity of software and hardware on IP networks makes network visualization an industry-wide issue. The main industry challenges are:

(1) Completeness: It is difficult to realize multi-layer visualization, such as visualization across the physical, protocol, slice, and service layers. Moreover, individual layers cannot be visualized from all dimensions. For example, lack of visibility for the energy consumption of devices makes it difficult to optimize the network for energy saving.

(2) Real-time performance: The current minutes-level visualization is insufficient for detecting and closing network faults. If a network fault leads to service quality deterioration or service interruption, it often takes minutes to detect and rectify the fault. This affects user experience and increases the churn rate.

(3) Ease of use: CSPs need to deploy multiple systems, and each system has numerous user interfaces (UIs). Fragmented, discrete visualization greatly degrades user experience and affects O&M efficiency. For example, when a CSP has to run an OMC system, an integrated network management system (NMS), an SDN controller, and a traffic system, this results in low O&M efficiency.

Severe impacts of risky configurations:

IP networks carry a wide array of services. For example, a CSP's IP backbone network has more than 2000 NEs and carries services for hundreds of millions of users. A tiny route configuration error can have a profound impact on the network, causing huge economic losses to a CSP. The longer the down time, the higher the costs. In extreme cases, essential services may be affected. This is why configuration has become a top concern for CSPs. In one instance, services on the entire network of the Canadian communications company Rogers were once interrupted for 37 hours, affecting more than 30 million customers and incurring direct economic losses of over US$190 million. All of this was the result of just one incorrect routing policy, which caused a sharp increase in the number of routes on backbone network devices and ultimately exhausted memory resources.

Difficulty in guaranteeing service experience through best-effort forwarding:

Statistical multiplexing and best-effort forwarding are core features of IP networks. Routing protocols perform calculations based on reachability, and devices forward packets hop (device) by hop. There is no global view of the entire network. As such, the network is prone to local congestion, increasing both delay and packet loss rates. Gaming and live streaming services are extremely sensitive to delay. They require delay to remain stable at the milliseconds level. In contrast, video and big data transmission services demand elastic high bandwidth. They require the network to provide high-bandwidth paths at the Gbit/s level. Ever-changing service requirements make the native disadvantages of networks even more prominent. Manual work is time-consuming and produces unsatisfactory results. On one CSP network, service detours resulted in high service delay and poor user experience. In two months, O&M personnel could only analyze and optimize 84 NEs and 8 paths in one area.

1.3 Technological Innovations Solve Native Problems

1.3.1 Digital Twin Network

With the development of new technologies such as 5G, IoT, and cloud computing, the scale of networks, number of connections, and network loads are increasing rapidly, making network O&M more and more challenging. The high reliability requirements of industry users on CSP networks and the high costs of trial-and-error make it difficult to achieve cost-efficient network operations and innovations. Digital twin technology can address these issues by using the network digital twin as the basic network O&M platform to reduce trial-and-error costs, accelerate innovations and iterations, and improve intelligent network O&M.

A digital twin network is a virtual mirror where physical network entities are rebuilt digitally and interacted with in real time. The digital twin network has almost the same network topologies, services, and traffic data model as the physical network. As a refined full-lifecycle, multidimensional duplicate of the real physical network, it provides a digital verification environment for O&M of the physical network.

With the digital twin network platform, network change operations such as adjustment, maintenance, and optimization can be fully tested and verified, and the operation solutions can be continuously evaluated, modified, and optimized based on feedback, with minimal impact on the physical network. The digital twin network also records its own status and behavior in real time and supports history tracking and playback so that pre-verification can be completed without affecting network operations, thereby greatly lowering the trial-and-error costs.

Unlike traditional simulation technologies, the digital twin network is not a static snapshot of the physical network; rather, it is updated in real time based on physical network status. With the help of AI technologies and self-learning, the digital twin network will evolve by itself based on feedback and provide higher authenticity and reliability.

1.3.2 IPv6+

Different vertical industries tend to customize and diversify their IP network connections in areas like delay, bandwidth, and service availability. IP networks are evolving to IPv6 at a quickening pace to accommodate massive basic connections. At the same time, IP networks are using a series of solutions and capabilities (e.g., slicing, SRv6, IFIT, centralized management & control, and intelligent analysis) to address higher-level challenges (e.g., differentiated quality assurance, security isolation, programmability, awareness, refined service, and intelligent management) and realize network as a service (NaaS).

SRv6

As one of the core technologies of IPv6+, SRv6 combines network programmability with centralized management and control to provide multi-factor path computation (based on bandwidth, delay, metric, etc.), fast optimization upon faults, and optimization upon SLA deterioration. It delivers differentiated service assurance and provides an innovation platform to meet the service needs of the 5G and cloud era.

Slicing

Network slicing facilitates resource isolation and provides deterministic, differentiated quality assurance for services. The convergence of FlexE slicing and Flex-channel slicing technologies not only implements multi-purpose networks and accelerates private network construction, it enables on-demand slicing and provision of high-quality private lines to specific tenants. E2E slice lifecycle management simplifies slice deployment, visualizes slice quality, and supports lossless scaling, helping CSPs monetize "slicing as a service".

IFIT

IFIT stands for In-situ Flow Information Telemetry. Unlike traditional measurement technologies, IFIT performs in-situ measurement on a per-packet basis, which greatly improves the accuracy of service SLA measurement. Combined with intelligent analysis, IFIT supports automatic hop-by-hop measurement of service degradation in addition to E2E SLA measurement, thereby locating the links suffering from quality degradation and enabling refined service operations.

The emergence of IPv6+ presents a better choice for NaaS. IPv6+ helps make network data and capabilities available and embeds them into CSPs' service systems and service processes, achieving automatic deployment and intelligent O&M.

1.3.3 AI + Big Data

From AlphaGo to ChatGPT, AI technologies have made many notable breakthroughs recently, and AI is accelerating its integration with the industry. The ever-increasing scale of networks, heterogeneous network technologies, and human-centered O&M are all increasing the burden on CSPs. At this point in time, AI is coming into play on telecom networks. It is accelerating the adoption of human-machine collaboration during telecom network operations and is playing an active role in telecom network planning, construction, maintenance, and optimization. Typical scenarios include network risk forecast, network traffic forecast, intelligent root cause analysis (RCA), and user package recommendation.

In the future, network environments will be more complex and erratic, emergencies will be more unpredictable, and data complexity and magnitude will hit record highs. Service scenarios will span clouds, networks, and edges, encompassing diverse industries, fields, and autonomous domains. There will be a great variety of tasks, deciding factors, and noise interference. To achieve full autonomy, IP networks must possess closed-loop autonomy through full-lifecycle self-learning, self-adaptation, and self-evolution. These capabilities will enable machines to autonomously conduct analysis, make decisions, and intervene in networks. Self-learning and evolutionary AI will be the key to achieving this.

In continuous evolution of AI models, big data is a must. Big data technology is critical for CSPs seeking to build an intelligent O&M system, improve network construction capabilities, and create more O&M benefits. By combining AI and big data technologies, CSPs can efficiently detect network-wide resources in real time, optimize network resources online, locate network faults quickly and accurately, and implement automatic, intelligent E2E network management, design, and operations. On top of that, as network O&M big data is continuously injected into operational systems, network graphs, and network elements (NEs), and as analysis models are optimized, network O&M can be upgraded intelligently and iteratively to make networks smarter than ever. For example, one CSP established an IP network resource utilization analysis model built on AI and big data technologies. This model continuously optimizes network resource utilization and performs predictive analysis so as to intelligently schedule network resources across areas and time segments. By doing so, the model effectively guarantees end user experience, improves network O&M efficiency, and reduces O&M costs.

1.3.4 SDN

Since its inception, software-defined networking (SDN) has not wavered in popularity. In the beginning, SDN was centered on an innovative network architecture featuring forwarding-control separation, centralized control, and network capability openness. Later, a development boom brought SDN from labs to live networks. We need to not only reimagine the network architecture, but redefine the network O&M process. We need to focus on service automation and O&M intelligence and build intent-driven adaptive networks to help CSPs achieve network cloudification and operation digitalization. These networks will have the following features:

Automation

Enabling autonomous driving networks (ADN) to automate full-lifecycle network deployment and O&M.

**Intelligence**

Collecting and perceiving network status in real time, automatically generating service policies based on big data, and achieving proactive maintenance and closed-loop optimization.
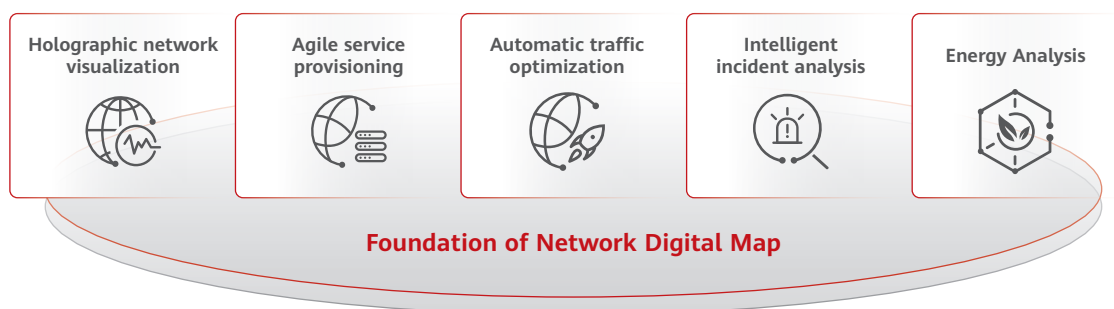
Self-adaptation

Leveraging AI and machine learning to build an intelligent network on which dynamic policies are automatically generated, thereby achieving network autonomy.
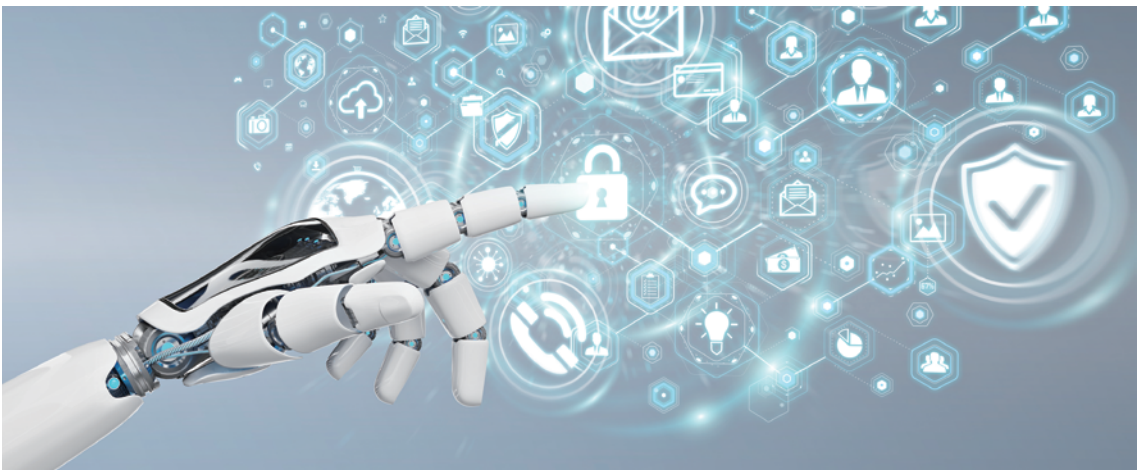
2 Target Architecture and Integration

2.1 Network Digital Map Overview

Digital transformation will be the focus of global development in the next decade. Driven by digital transformation, industries are accelerating their pace of cloudification. As different industries have different requirements for service SLAs, networks must provide agile and differentiated SLA assurance to meet diverse service requirements. Unfortunately, lack of visibility for network quality, makes it difficult to perceive service SLA changes. Furthermore, the current best-effort forwarding network is incapable of differentiated and automatic traffic scheduling and cannot meet the differentiated assurance requirements of industry services. To resolve these challenges, Huawei launched its futuristic Network Digital Map technology in Huawei iMaster NCE-IP.

| Holographic network visualization | Agile service provisioning | Automatic traffic optimization | Intelligent incident analysis | Energy Analysis |

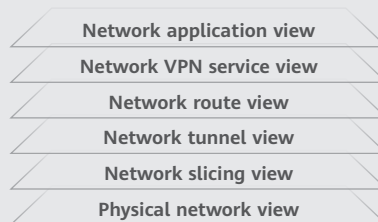**Foundation of Network Digital Map**

As a digital foundation for IP network intelligent O&M, Network Digital Map operates like a transit map to offer holographic network visualization, agile service provisioning, automatic traffic optimization, intelligent incident analysis, risk forecast, and full-lifecycle intelligent O&M, thereby continuously guaranteeing service SLAs and improving service experience.

- **Holographic network visualization:** Traditionally, network performance measurement relied on manual deployment. Low accuracy and efficiency were persistent issues for O&M personnel. Using standard protocols such as BGP-LS and BMP, Network Digital Map collects data about physical resources, slices, tunnels, routes, VPN services, and applications on multi-vendor devices in real time. The map's framework for distributed network performance collection presents multidimensional indicators of ultra-large networks such as delay, bandwidth, packet loss, and energy consumption in real time. This helps customers obtain a clear view of the entire network and identify service detours or other problems.

Network application view
Network VPN service view
Network route view
Network tunnel view
Network slicing view
Physical network view

Multiple views

- **Physical network view:** Drawn based on physical network connections, this layer automatically places network nodes based on their GIS coordinates. The statuses of NEs and Layer 2 links are associated with their alarm conditions. Users can zoom in and out on multi-level topologies and enjoy an automatic topology layout.
- **Network slicing view:** Differentiated logical networks are offered to different tenants by means of hard slicing and soft slicing. Not only are the slice topologies displayed, but the statuses of NEs and links on slice networks are also displayed and associated.
- **Network tunnel view:** This layer provides views for the RSVP-TE, SR-TE, and SR-Policy tunnels on the physical or slice networks, displays the statuses and paths of E2E tunnels, and supports latency circle rendering, path precomputation, and optimization history playback.
- **Network route view:** This layer displays the information and prefixes of IGP and BGP routes on networks.
- **Network VPN service view:** With an E2E VPN service view, this layer displays basic VPN information, peer connections, and forwarding paths.
- **Network application view:** Associated with upper-layer applications such as network traffic, routes, and energy consumption analysis, this layer uniformly analyzes and displays network-wide applications, and supports network traffic optimization and scheduling.
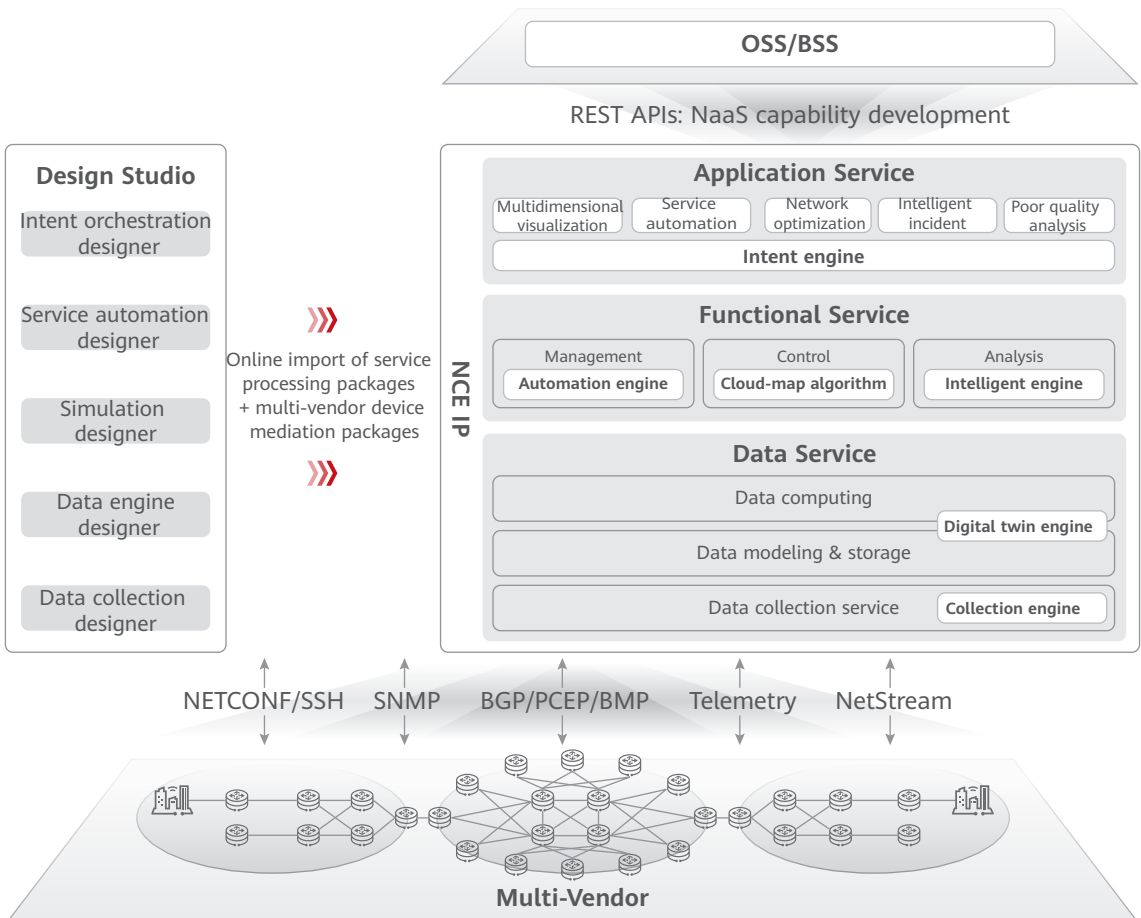
Network Digital Map displays multidimensional information, including:

Multiple dimensions

- **Status:** When there is a network fault, the IGP protocol on devices immediately performs convergence and floods the updated link status. The BGP-LS protocol then reports the information to the controller, and the controller sets the corresponding links as down.
- **Bandwidth:** Network Digital Map displays bandwidth utilization data for links and color-codes the links based on the bandwidth utilization ranges set by users.
- **Delay:** Network Digital Map displays delay data for links and color-codes the links based on the delay ranges set by users.
- **Cost:** Network Digital Map displays TE metric data for links and color-codes the links based on the TE metric ranges set by users.
- **Packet loss rate:** Network Digital Map displays packet loss rate data for links.
- **Energy:** Network Digital Map displays energy efficiency and real-time power for NEs.
- **Availability:** Availability is automatically assessed based on link fault frequency to reflect the stability of network links.

- **Navigation-like path computation:** Optimal paths are computed to match service intents. The intelligent cloud-map algorithm can finish path computation in mere seconds while taking 20+ factors into account. It can detect poor service quality in seconds, locate root causes in minutes, and complete automatic optimization in minutes to meet differentiated SLA assurance requirements.

- **IP traffic scheduling:** Currently, most IP networks use best-effort forwarding, which makes them prone to congestion in the event of a traffic surge. Manual traffic balancing takes more than 3 hours on average, resulting in poor user experience. Network Digital Map can detect IP network congestion in real time, and using BGP FlowSpec, it automatically optimizes and adjusts traffic paths, achieving minute-level SLA closed-loop assurance.

- **Highly stable IP network:** Network Digital Map provides the "intent verification" and "BGP route analysis" capabilities to detect incorrect network changes in advance and intercept potential major network accidents, helping service providers build secure, reliable, and highly stable IP networks.

- **Green IP network:** Network Digital Map provides the "energy analysis" capability that makes energy consumption visible, manageable, and optimizable on the entire network.

2.2 Target Architecture

OSS/BSS

REST APIs: NaaS capability development

Design Studio

Intent orchestration designer

Service automation designer

Simulation designer

Data engine designer

Data collection designer

Online import of service processing packages + multi-vendor device mediation packages

NCE IP

Application Service

| Multidimensional visualization | Service automation | Network optimization | Intelligent incident | Poor quality analysis |

Intent engine

Functional Service

| Management | Control | Analysis |
| Automation engine | Cloud-map algorithm | Intelligent engine |

Data Service

Data computing — **Digital twin engine**

Data modeling & storage

Data collection service — **Collection engine**

NETCONF/SSH   SNMP   BGP/PCEP/BMP   Telemetry   NetStream

Multi-Vendor

As a network management and control system and the core bearer of Network Digital Map capabilities, Huawei iMaster NCE-IP provides a complete family of open APIs for OSSs/BSSs as well as a rich set of simple and easy-to-use UIs for system administrators and network O&M personnel. iMaster NCE-IP connects to devices through various protocols to manage and control network operations.

- Using management protocols such as NETCONF, SSH, and SNMP, it configures devices, queries status, and receives alarms.
- Using control protocols such as BGP, PCEP, and BMP, it collects network topology and route status information, and controls tunnel paths.
- Using performance/status protocols such as telemetry and NetStream, it collects network traffic, delay, and other data to analyze network status.
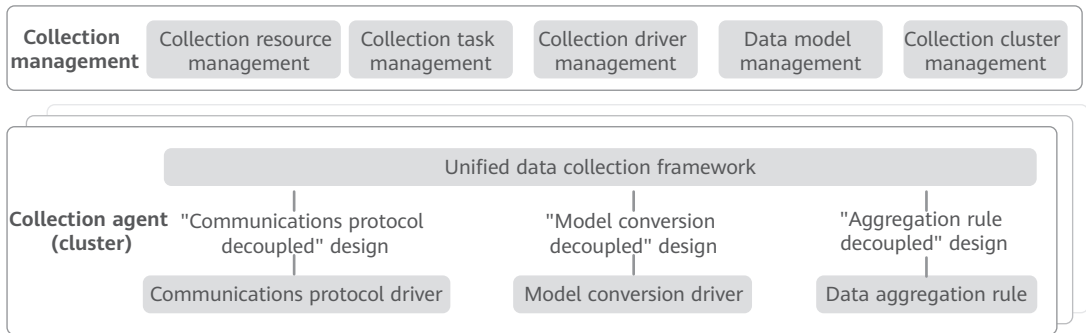
Network Digital Map has the following core capabilities:
- **Openness:** Full-stack support for service customization allows CSPs to customize service orchestration, open interfaces, configure third-party devices, collect data, and adapt device behaviors and capabilities simply by loading service driver packages online.
- **Digital twin:** A big data platform enables the map to create digital duplicates for network services, NE configurations, status, performance, etc. The map also supports data-based analysis, computing, and presentation.
- **Multi-service capability:** The map supports wildly diverse services, covering the entire network lifecycle (network planning, construction, maintenance, and optimization). It provides a complete set of network management, control, and analysis capabilities.
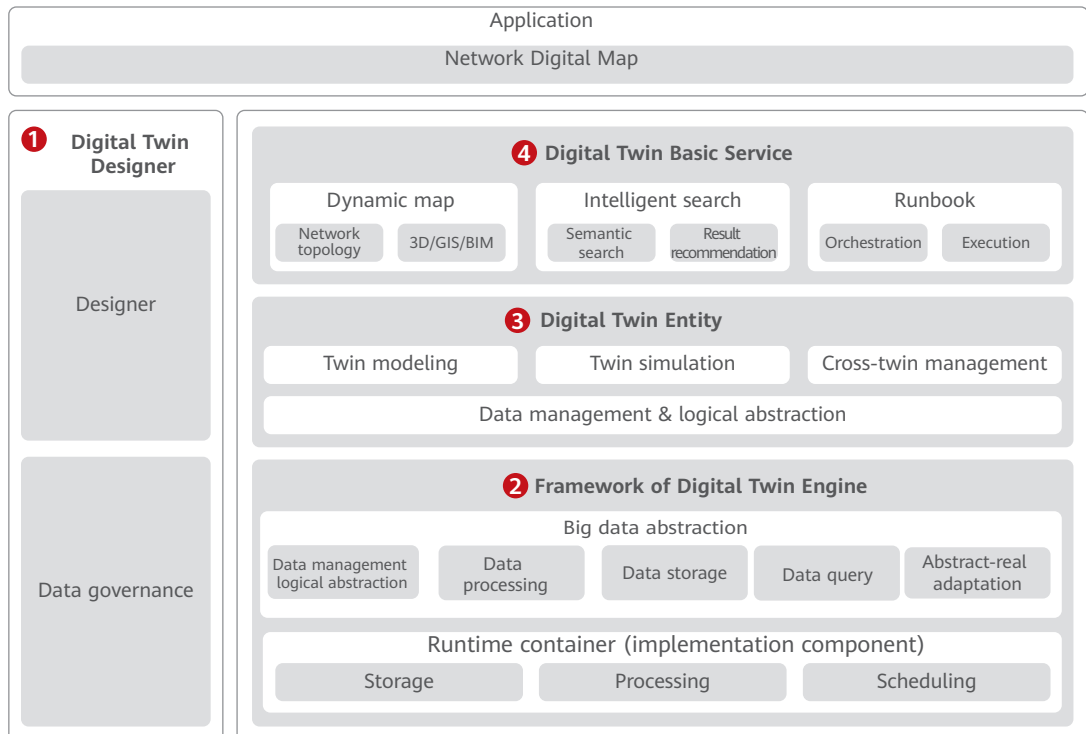
To bolster these core capabilities, a "functional engines + service definitions" approach spanning all three layers (data service, functional service, and application service) of iMaster NCE-IP is used to unify system quality attributes such as openness, scalability, reliability, and security, and continuously iterate new features. Functional engines include:
- **Data collection engine:** This engine projects physical network data into the digital world. To this end, it collects raw network data through a host of protocols (NETCONF, SSH, telemetry, BMP, NetStream, etc.). For large networks, it employs a distributed data collection framework to collect data concurrently. Once data is collected, the engine aggregates the data, converts the basic format, and writes the results into the digital twin engine for subsequent data analysis and presentation.
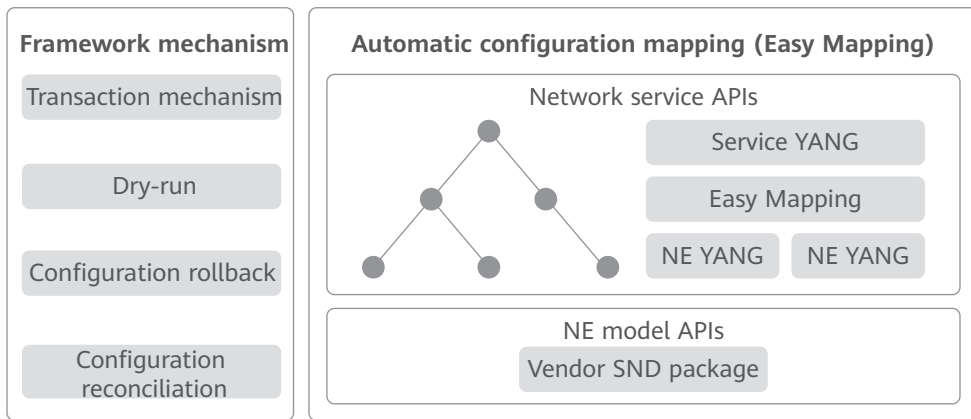
Collection management	Collection resource management	Collection task management	Collection driver management	Data model management	Collection cluster management

Collection agent (cluster)	Unified data collection framework		
	"Communications protocol decoupled" design	"Model conversion decoupled" design	"Aggregation rule decoupled" design
	Communications protocol driver	Model conversion driver	Data aggregation rule

- **Digital twin engine:** This is the engine that converts the physical network into a digital one. The digital twin engine provides core data services, including big data–centric storage services of different data types (typically online transaction processing [OLTP] and online analytical processing [OLAP]) and aggregation and computing services of different data types. Furthermore, the engine maps logical data models to storage models (and manages these mappings), processes the time series of data objects, manages data associations, etc. To the outside world, it supports data services like data query, data search, and data orchestration. The target architecture of the digital twin engine consists of four parts: Designer, Framework, Entity, and Basic Service.
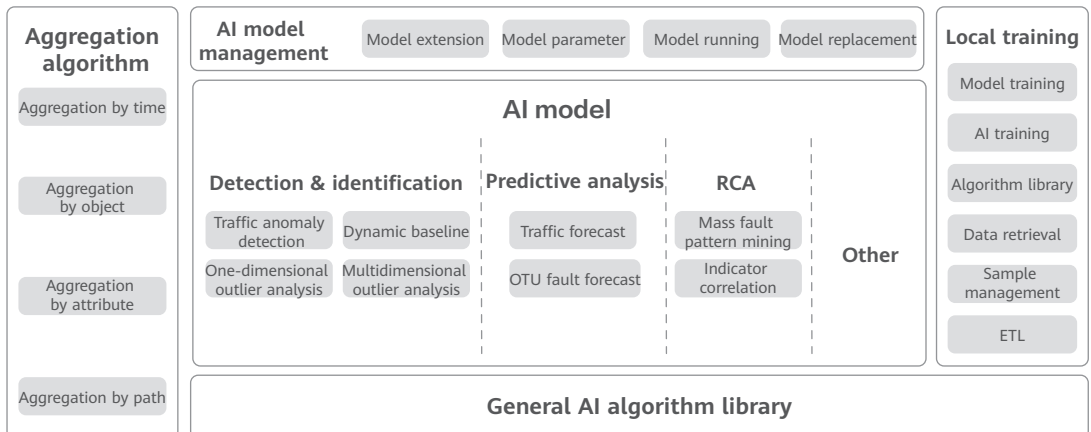
Application
Network Digital Map

❶ Digital Twin Designer	❹ Digital Twin Basic Service		
	Dynamic map	Intelligent search	Runbook
Designer	Network topology / 3D/GIS/BIM	Semantic search / Result recommendation	Orchestration / Execution
	❸ Digital Twin Entity		
	Twin modeling / Twin simulation / Cross-twin management		
	Data management & logical abstraction		
Data governance	❷ Framework of Digital Twin Engine		
	Big data abstraction		
	Data management logical abstraction / Data processing / Data storage / Data query / Abstract-real adaptation		
	Runtime container (implementation component)		
	Storage / Processing / Scheduling		

Designer	Provides a simple and scalable dimension/relationship/fact table modeling system by referring to modeling theories in the industry, and builds a unified model management and design tool to simplify product development and visualize network data modeling.

Framework	Provides real-time and trusted network data, as well as optimal data processing/storage/query capabilities.

Entity	Provides common data service capabilities. In particular, the simulation service provides unified NE configuration, NE inventory, NE behavior, and network models to which network data is mapped. iMaster NCE-IP provides Network Digital Map, which not only completes device-centric protocol simulation based on unified models, but supports customized verification plug-ins based on common verification algorithms. Using these tools, CSPs can quickly customize the simulation service. Within the digital mirror of the physical network, Network Digital Map builds multiple digital mirror branches, based on which the effects of changes are verified.

Basic Service	Provides NetSearch to achieve semantic-/intent-based intelligent search, associated information recommendation, and dynamic high-fidelity (Hi-Fi) segment topology on GIS, support fast network fault diagnosis, and improve O&M efficiency.

- **Automation engine:** In model-driven mode, this engine uses YANG to define network service models at the network service layer and NE configuration models at the NE layer. The Easy Mapping framework automatically converts network models into NE models and provides reliability capabilities such as dry-run, configuration reconciliation, configuration rollback, and transaction mechanism to achieve automatic service configuration.

Framework mechanism

Transaction mechanism

Dry-run

Configuration rollback

Configuration reconciliation

Automatic configuration mapping (Easy Mapping)

Network service APIs

Service YANG

Easy Mapping

NE YANG   NE YANG

NE model APIs

Vendor SND package

- **Intelligent engine:** This engine provides a fundamental AI algorithm library and facilitates service computing with intelligent applications such as traffic anomaly detection and identification, traffic forecast, and mass fault RCA. It can load and manage multi-application algorithm models and supports a variety of computing applications. It provides a local training platform to quickly develop and import new algorithms based on live network data.

Aggregation algorithm

Aggregation by time

Aggregation by object

Aggregation by attribute

Aggregation by path

AI model management

Model extension   Model parameter   Model running   Model replacement

AI model

Detection & identification

Traffic anomaly detection   Dynamic baseline

One-dimensional outlier analysis   Multidimensional outlier analysis

Predictive analysis

Traffic forecast

OTU fault forecast

RCA

Mass fault pattern mining

Indicator correlation

Other

General AI algorithm library

Local training

Model training

AI training

Algorithm library

Data retrieval

Sample management

ETL

- **Intent engine:** This engine provides intent definition, closed loop, and workflow orchestration capabilities. With this engine, design and orchestration work can be completed on UIs in low-code mode, and atomic network interfaces can be orchestrated simply through drag-and-drop. Various service logic, workflows, and parameter transfers are visibly orchestrated online, with UIs and APIs generated automatically. For automatic service provisioning and automatic O&M scenarios, the engine divides workflows into two types: parameter mapping (provisioned through northbound interfaces) and event-triggered (triggered by network events). For example, the automatic service provisioning process usually checks the network status and detects any resource conflicts before configurations are delivered, and checks service connectivity and alarms after configurations are delivered. In some cases, however, automatic detection tasks and periodic inspection tasks need to be started after services are successfully provisioned. The intent engine consists of the following:

Design time	As the design environment of O&M workflows, the engine combines atomic APIs to meet closed-loop operations in specific O&M scenarios. In addition, it provides a commissioning environment for new workflows so that users can trace, commission, and modify workflows online, accelerating workflow development and rollout.

Run time	The engine includes a DSL interpreter, workflow engine, delivery/execution module, and workflow instance management module. The DSL interpreter loads workflow and action packages from 'Catalog' as required and parses them into a syntax tree. The workflow engine is a framework for workflow scheduling, workflow status management, and action execution/scheduling. The delivery/execution module delivers/executes actions based on the instructions received from the workflow engine. The workflow instance management module is used to manage the generated workflow instances. It allows users to query, retry, and roll back specific instances.
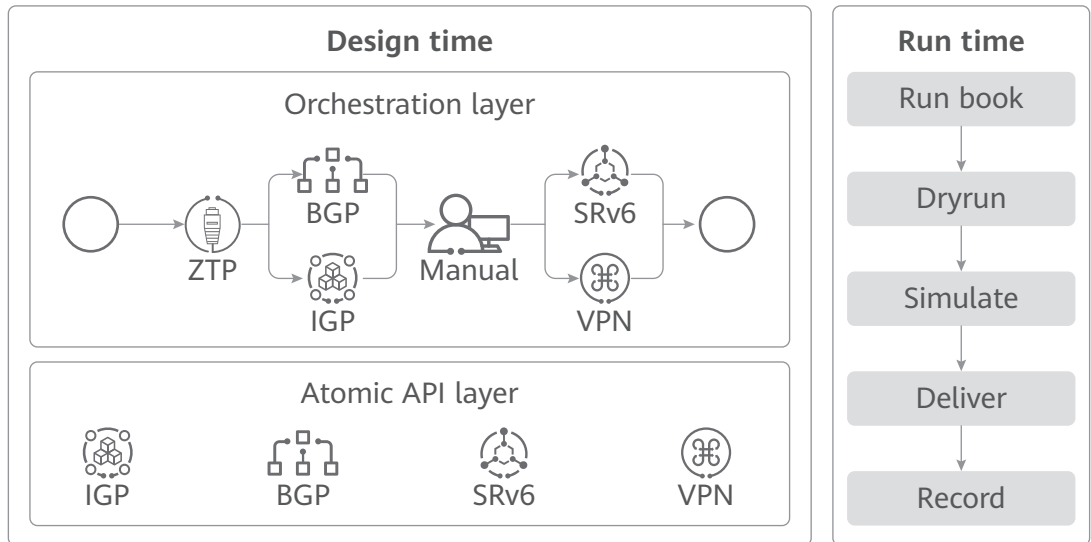
These engines provide many service applications of Network Digital Map, including service automation, configuration change simulation, multidimensional display of network topologies/tunnels/VPN services, BGP route analysis, service path discovery and restoration, and intelligent search. These engines accelerate service development and deliver unified experience and quality attributes.

2.3 Data Model

Traditional NMSs are riddled with data silos and huge volumes of redundant data. When data flows across different network function units, it needs to be converted many times. For example, when an inventory system sends data to a performance analysis system, both systems convert the data once with their own models. In the future, the digital twin will serve as the one and only source of system data at each layer. This will greatly reduce data redundancy and inconsistency, as well as the extra overhead of transferring the same data across different subsystems. Therefore, network data models must be compatible and open enough to support multi-data access, heterogeneous storage, and real-time presentation in the twin.

The data involved in network twin modeling is classified into the following:

- **Static data:** includes configuration data (such as routing protocol configurations and service configurations) and inventory data (such as NEs, boards, physical ports, logical interfaces, timeslot resources, VLAN resources, and IP address pools).
- **Dynamic data:** refers to the data generated during network runtime, such as routes, tunnel paths, and protocol status.
- **Measurement data:** includes network alarms and performance indicators.

The preceding data is modeled in the following modes:

- **Managed object (MO):** This mode defines MOs and relationships between MOs.
- **Specification:** This concept comes from the Specification design pattern in the TM Forum SID. Specification data describes the invariant features of a specific type in a specific object class. Invariant means that the same specification data can be referenced by multiple instances, which saves storage space.
- **Historical fact:** This mode records events, performance, statistics, alarm logs, data change logs, and operation logs that have occurred in the system. This type of data is recorded in chronological order and cannot be changed (because they are established facts), but users are allowed to supplement and label historical fact data. The lifespan of historical fact data may be longer than that of the entities tied with the data. To correctly display historical fact data even after their entities are deleted, the historical fact data model maintains certain key entity attributes (e.g., names and addresses).
- **Role entity:** This concept comes from the Role Entity design pattern in the TM Forum SID. It aims to meet scalability requirements.

2.4 Network as a Service

CSPs are progressing digital transformation top down from strategic consulting to business planning, architecture design, operations management, organization optimization, etc. In this process, the main requirements are shifting from communications to information, and from connection/traffic operations to data operations. Network openness is an inevitable trend. Traditional OSS integration is characterized by large numbers of interfaces, complex parameters, long development periods, and high costs. This makes it difficult for CSPs to achieve rapid service provisioning and simplify O&M processes. CSPs are in urgent need of programmability, fast service rollout, open APIs, automatic O&M, and shorter integration TTM.

To address these needs, network as a service (NaaS) presents the following features:

Network-business decoupling

Network services are decoupled from customer businesses. Instead of designing a network service for each business, we must fully understand the business scenarios and network requirements before providing a network service that perfectly matches the business. In this way, one network can be used for multiple purposes to achieve rapid business growth without compromising network stability, flexibility, or agility.

Atomic network service

From a technical perspective, networks are divided into different layers and segments. Different networks use different technologies and solutions. However, from a service perspective, services need to be modularized and flexibly combined when necessary. That is, different atomic services need to be combined into a one-stop E2E service as required by users.

Standard network service

Only standardization can provide users with consistent services on-demand anywhere, anytime. Therefore, common standards must be defined to deliver standardized network services to users.

Network Digital Map provides NaaS interfaces to help CSPs centrally manage network resources for higher resource efficiency and O&M efficiency. They are also critical for implementing full-lifecycle automatic O&M, i.e., service automation, network optimization, and troubleshooting.

- **Resource management**

  Subnets, NEs, ports, IGP topologies, L3VPN services, L2VPN services, tunnels, slice resources, etc.

- **Service automation**

  Slice lifecycle management: slice instance initialization, change/modification, and monitoring

  SR-TE, SR-MPLS TE Policy, SRv6 Policy, cross-domain SRv6 Policy, RSVP-TE, L3VPN, L2VPN, etc.

  Service path precomputation

  Cloud-network package recommendation

- **Network optimization**

  Tunnel path optimization

  IP traffic optimization

- **Intelligent incident O&M**

  Alarm subscription, reporting, synchronization, acknowledgment, unacknowledgement, etc.

  Intelligent incident reporting

3 Typical Usage Scenarios and Key Technologies

3.1 Planning Phase: Network Configuration Verification

3.1.1 Scenario Description

Because IP networks carry a large number of cross-city, cross-province, and even cross-country data services, CSPs must be cautious about changing network configurations. Any mistakes can lead to huge losses. Regardless of how careful network maintenance engineers are, network configuration changes result in 80% of network faults. According to the "Network automation using AI and machine learning" report by the TM Forum, 43% of CSPs believe that manual configuration severely affects their service capabilities. Configuration has become a widespread concern of CSPs. CSPs want such an online configuration verification tool that can assess and verify the impact of network configurations in advance and successfully intercept incorrect configurations.
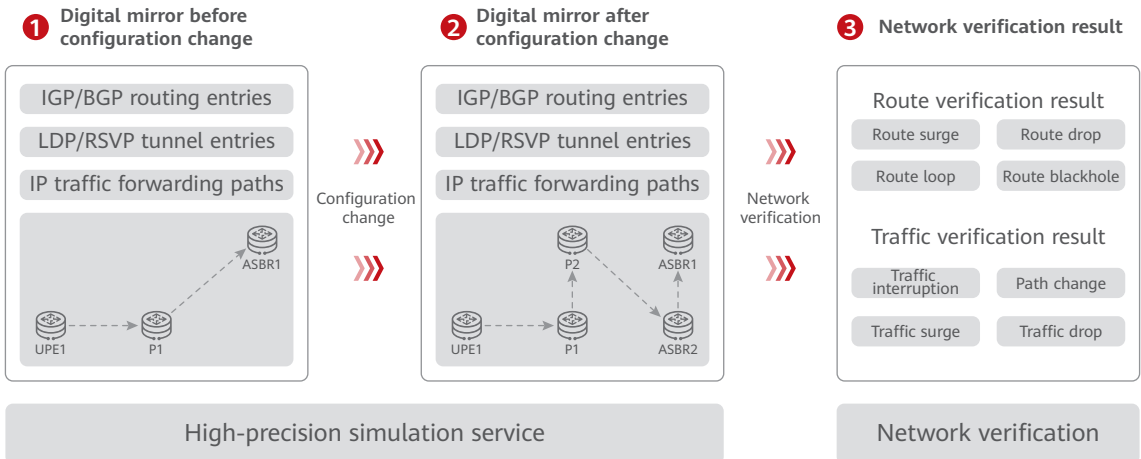
- **High-precision simulation:** Taking the configuration changes, interconnecting routes, and traffic of network devices as inputs, the engine simulates not only the statuses and behaviors of network protocols and traffic, but the routing and forwarding tables of network devices. This provides an authentic, objective basis for network change risk assessment.

- **Network verification algorithm:** Based on the routing tables, forwarding tables, and traffic loads of devices, control plane verification/data plane verification (CPV/DPV) is conducted to assess network risks according to certain rules. Control plane verification (CPV) can formally solve and verify changes in the number of control plane routes (sudden surges and drops), route reachability, and route reliability (blackholes and loops). Data plane verification (DPV) can formally solve and verify network forwarding plane paths. These two technologies complement each other to identify potential risks that may result from network configuration changes, thereby intercepting incorrect configurations.

3.1.2 Key Technologies

3.1.2.1 High-Precision Network Protocol Simulation

Network simulation is classified into non-real-time offline and real-time online simulation.

Offline simulation is mainly used for long-term network activities, such as network planning, network optimization, and network prevention. Simulation tools assist experts in verifying policy effectiveness to reduce implementation risks on the live network. This type of simulation is not frequently used and does not require extreme real-time performance.
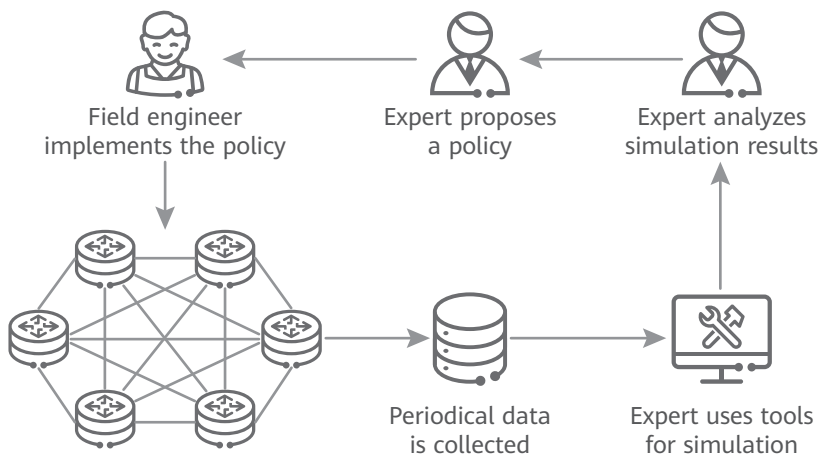
Online simulation is mainly used for network troubleshooting, emergency recovery, and network changes that must be detected in real time. As network automation continues to develop, users are increasingly sensitive to the time needed for closing network faults, self-service applications, etc. They expect these tasks to take minutes or even seconds. Real-time online simulation can solve this problem.

Simulation service
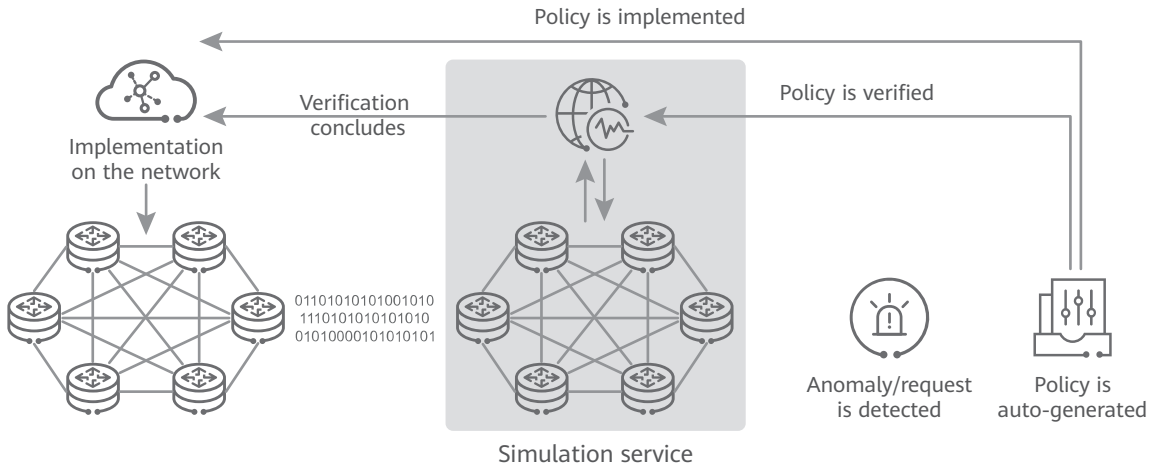
One of the main purposes of the online network protocol simulation system is to simulate the behaviors of device routing protocols based on NE configurations and then accurately generate NE protocol routing tables and global routing tables. These routing tables are the basis for verifying impact on networks. The simulation service must have the following capabilities:

- **Multi-vendor:** Supports joint simulation by mainstream vendors (such as Huawei and Cisco).
- **Incremental:** Simulates based on incremental configurations (such as configuration command snippets) to identify the impact of configuration changes on routes, traffic paths, and link loads in advance.
- **Routing protocol:** Simulates the behaviors of routing protocols and generates peer statuses, protocol routing tables, global routing tables, label tables, and tunnel tables for NE protocols (20+ mainstream routing protocols).
- **Traffic:** Models the behaviors of device forwarding planes based on routing and label tables, computes E2E paths for service flows and distributes flows to physical links based on the path computation results, thereby forming a simulated network-wide load map.

3.1.2.2 Network Verification Algorithm

In the network verification phase, O&M personnel — after defining network verification intents and rules — use the digital twin system for strict intent verification and closure. They efficiently verify network problems and output a verification report. The network verification rules are:

- **Network-wide connectivity:** Layer 2/Layer 3 traffic exchange capabilities and Layer 2/Layer 3 traffic paths are verified.
- **Network-wide loop:** If a packet goes into/out of the same port that it went into/out of earlier during network forwarding, a loop arises in the port sequence of the packet.
- **Network-wide blackhole:** A blackhole refers to the situation in which an NE receives a route from other NEs but does not forward the route to other NEs.
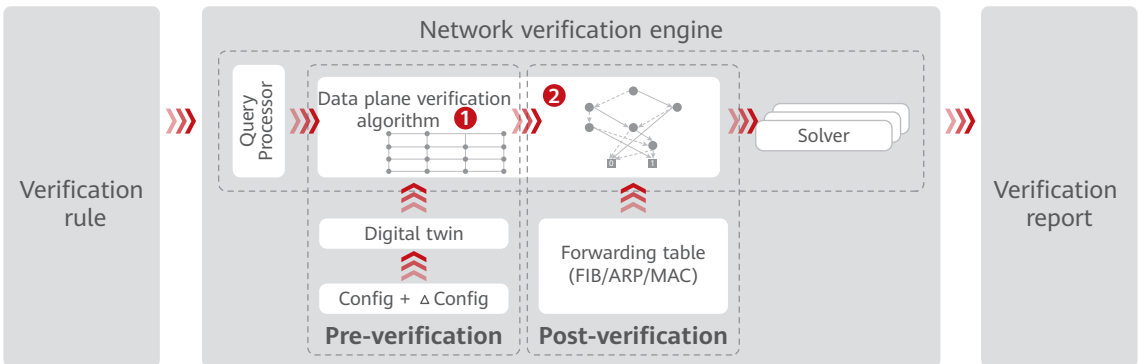
Key Technology

Efficient Graph Theory Verification Algorithm:
A correlated aggregation graph is created for each correlated equivalence class. The efficient graph theory algorithms — depth-first search (DFS) and header space analysis (HSA) — jointly compute paths to verify route reachability and loops.

3.2 Construction Phase: Service Automation

3.2.1 Scenario Description

CSPs and enterprises tend to deploy multi-vendor devices on their networks. Fast adaptation to multi-vendor devices and fast rollout of new services are the core competitive advantages of service automation. However, there are challenges in adapting to new devices and new services.

- The efficiency of adapting to new devices depends on vendor capabilities and response speeds. This results in slow device integration, low automation, and long provisioning periods, which are bottlenecks in E2E service delivery.

- The rollout of new services depends on the updates of OSS and controller versions, which creates problems such as insufficient API integration and high customization costs. These problems prolong the rollout periods of new services, which means service rollout cannot keep pace with flexible service scenario changes.
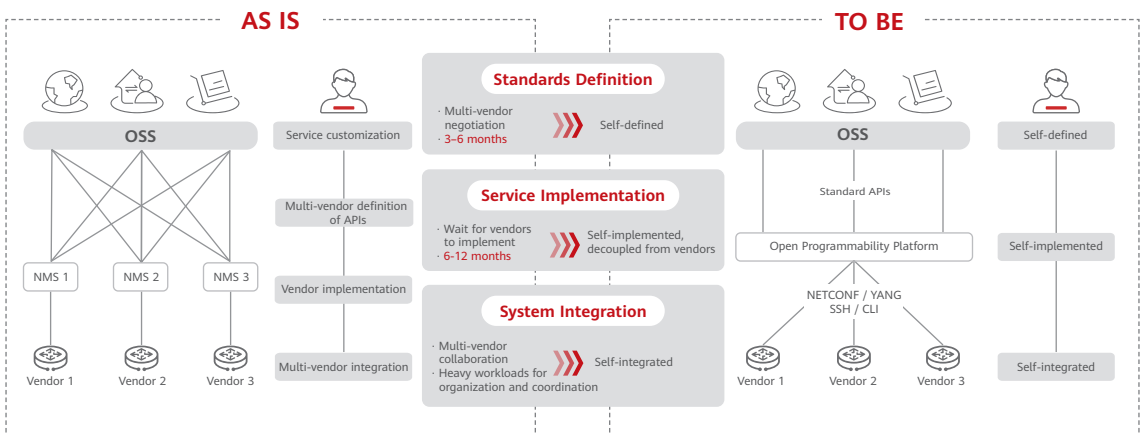
Network Digital Map in iMaster NCE-IP builds a high-performance and high-reliability automation engine to enable fast service provisioning on multi-vendor networks and address the challenges concerning service automation. It increases the efficiency of adapting to new devices by 90%, thereby shortening the device adaptation and management periods from months to days. The rollout periods of new services are shortened by 80%, from 6–9 months to 1 month.
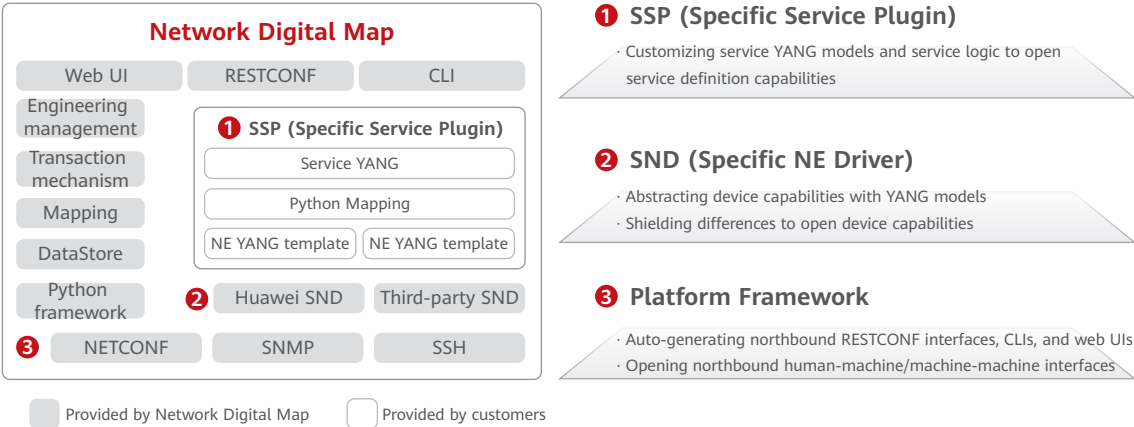

The automation engine consists of a design time and run time. The design time establishes mappings between service YANG models and device YANG models. These mappings are needed by the run time to provision services. Specifically, users write SSP and SND packages at the design time and load software packages at the run time, thereby quickly managing new devices and building new services.

- **Specific service plugin (SSP) package:** provides the data models required for completing a set of network-level service configurations.
- **Specific NE driver (SND) package:** provides data models for interacting with network devices. The data models contain YANG files that define device information, such as device types, vendors, connections, and features. By loading SND packages, Network Digital Map establishes connections with devices, queries data, and delivers configurations to manage devices.

3.2.2 Key Technology: Model-Driven Service Automation on Multi-Vendor Devices

The automation engine is a model-driven programmable framework with good scalability and plays a key role in multi-vendor service automation. After quickly managing devices, it automatically obtains configurations and generates NE-level atomic APIs. It allows users to customize service models based on YANG in order to generate network service APIs. With built-in decomposition, orchestration, computing, and backtracking algorithms, the Easy Mapping framework in the automation engine automatically decomposes network services into NE configurations and maps the configurations to NE-level atomic APIs.
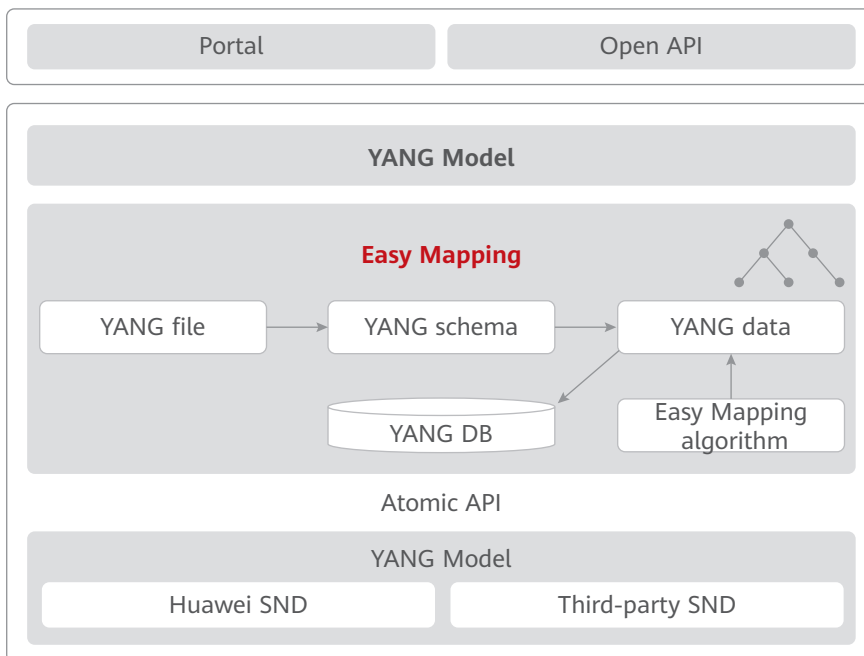
The automation engine has the following capabilities:

- Network Digital Map automatically generates not only northbound interfaces (NBIs), including CLI, RESTCONF, and web UI, based on the service and device models defined in the loaded software packages, but also southbound protocol packets (including NETCONF packets) based on the device models defined in the software packages. Network Digital Map also supports model-driven databases and automatically generates database entries based on YANG models.

- For service management, Network Digital Map automatically generates service creation pages based on service YANG models and implements Create, Retrieve, Update, Delete (CRUD) operations based on the mappings between service and device YANG models.

- For device management, Network Digital Map automatically generates NE management pages based on device YANG models and implements CRUD operations on NE resources, such as difference comparison, data synchronization, and configuration reconciliation.

- For NBIs, Network Digital Map automatically generates RESTCONF interfaces based on service and device YANG models and implements CRUD operations on services and NE resources based on the mappings between the two types of models.

- Network Digital Map uses a high reliability mechanism capable of configuration transaction, verification, and rollback to ensure that configurations are correct.

3.3 Maintenance Phase

3.3.1 BGP Route Analysis
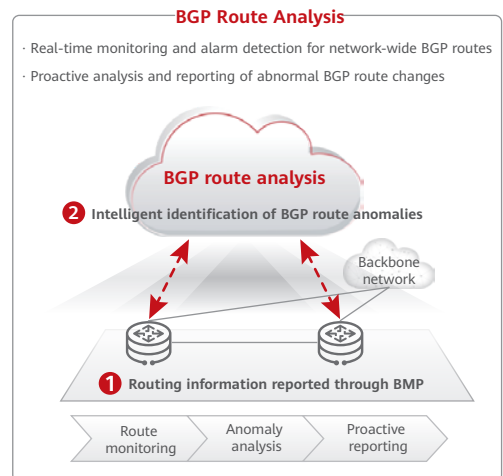
3.3.1.1 Scenario Description

Border Gateway Protocol (BGP) is a core system for exchanging routing information among autonomous systems (ASs) on the Internet. It is also the technical foundation for connecting global cyberspace. However, BGP security problems have become more frequent in recent years. BGP security problems are classified into the following types in RFC 7908:

1. Hairpin Turn with Full Prefix: (provider-to-provider) An AS learns a route from one upstream ISP and simply propagates it to another upstream ISP.

2. Lateral ISP-ISP-ISP Leak: (peer-to-peer) An ISP received a route from its non-transit ISP but leaks it to another ISP.

3. Leak of Transit-Provider Prefixes to Peer: (provider to peer) An AS leaks routes learned from its transit provider to a non-transit ISP (peer).

4. Leak of Peer Prefixes to Transit Provider: (peer to provider) An AS leaks routes learned from a non-transit peer to its own transit provider.

5. Prefix Re-origination with Data Path to Legitimate Origin: An AS learns a route from one upstream ISP and announces the prefix to another upstream ISP as if it is being originated by it.

6. Accidental Leak of Internal Prefixes and More-Specific Prefixes: An AS leaks its internal, more-specific prefixes.

These six types can be categorized into two groups:

- **Route leak:** A received route is forwarded to an incorrect BGP peer. This problem is related to the Internet architecture. A typical case was the Safe Host incident on June 6, 2019.
- **Route hijack:** The AS attribute of a learned route is tampered with or a more specific route belonging to other CSPs is generated, resulting in the route being advertised to other ASs. This problem is related to Internet governance. A typical case was the hijacking of Russian telco Rostelecom on April 1, 2020.

According to a report by Mutually Agreed Norms for Routing Security (MANRS), about 775 route hijacks and 830 route leaks occurred globally in 2021. Route hijacks and route leaks, whether accidental or malicious, severely affect the performance and service quality of the Internet. As such, visualization and security analysis of BGP routes, reporting and isolation of abnormal routes, and security verification of BGP configurations have become core requirements of CSPs and enterprises seeking a BGP route security system.

BGP Route Analysis

· Real-time monitoring and alarm detection for network-wide BGP routes

· Proactive analysis and reporting of abnormal BGP route changes

BGP route analysis

2 Intelligent identification of BGP route anomalies

Backbone network

1 Routing information reported through BMP

Route monitoring | Anomaly analysis | Proactive reporting

- **BGP route collection:** obtains BGP peer relationships and statuses in real time using BMP; collects the Adj-RIB-In, Adj-RIB-Out, and the Loc-RIB routes of BGP peers to show statistics on BGP peers and their routes.
- **BGP route visualization and analysis:** monitors all BGP routes (especially key routes); analyzes, collects, and displays temporal and spatial route changes (including routing prefix advertisement and withdrawal, and changes in route AS paths and source ASs) on each BGP peer to detect and report route hijacks, route leaks, and other anomalies; monitors key routes' performance indicators such as reachability and delay in real time; replays route path changes to quickly detect and rectify BGP route anomalies.

Perceivable global status	Using its powerful visualized O&M capabilities, Network Digital Map displays an accurate map of connections among global BGP ASs from the perspective of users. The AS topology view displays the directions and paths in which global Internet routes are advertised among ASs. The Network Digital Map topology shows information about BGP route peers, AS-advertised routes, and BGP route "peer down", as well as alarms for fluctuations in prefix advertisements by ASs. It evaluates global network quality in real time and detects route anomalies by analyzing AS path features. By monitoring the changes advertised by peers, Network Digital Map analyzes and replays suspected BGP route anomalies globally.
Traceable key routes	Key routes refer to the IP address segments owned by CSPs or users and those of popular Internet service providers (ISPs). In the existing Internet architecture, key routes have stable source ASs, AS paths, and route attributes that do not change significantly over long period of times. Key routes are monitored in real time. An alarm is triggered whenever a key route change occurs. On devices serving as integration gateways (IGWs) or provincial backbone egresses, routes change frequently every day. In addition, transient attacks make it difficult to trace and locate service quality problems. Network Digital Map supports minute-level anomaly analysis, speeding up abnormal route location and securing network borders. Key route changes are recorded in more detail. During fault location and demarcation, Network Digital Map allows users to view the lifecycle of a routing prefix through backtracking. By filtering key time points and attributes, users can efficiently determine the sources of anomalies. This facilitates subsequent interventions such as advertisement, isolation, and recovery. Key routes can be managed more flexibly. Network Digital Map can monitor anomalies by route for better management of key routes. Users can export historical routing information by day or month, facilitating long-term network change tracing and analysis.

- **BGP route configuration verification:** verifies BGP route configuration changes to forecast route changes and analyze the possibility of route leaks, reducing BGP security incidents caused by manual configuration mistakes.

3.3.1.2 Key Technology: Spatiotemporal Routing Algorithm

1. Building an AS Link Knowledge Base

The AS link knowledge base obtains the connections among global ASs to infer an AS topology, which constitutes the core statistical support for detecting and preventing path hijacks as well as a key input for detecting fake paths.

In building the AS link knowledge base, key technologies include activity calculation and link activity management. Based on a combination of spatial information (collected by edge routers) and temporal changes (recorded in the timeline), Network Digital Map designs the AS link lifecycle model, as well as reliability labeling and aging mechanisms. Then it adjusts parameters based on experience and practice so that the results can differentiate path hijacks from normal AS link updates.

The AS link knowledge base labels link activity in spatial and temporal dimensions.

2. Calculating Spatial Activity

Spatial activity measures the number of prefixes using an AS link. The more the prefixes, the higher the spatial activity of the AS link. Fake links usually exist in a small number of bad prefix advertisements. Therefore, the spatial activity is targeted at AS links generated by such prefix advertisements. If the activity value of an AS link at a specific time point is lower than the specified threshold, the link may be fake. In this case, a suspected path hijacking alarm is triggered, but further conclusions can only be made after temporal activity is also calculated.

3. Calculating Temporal Activity

Data sources are updated periodically. As such, each update is an independent discrete event, and the entire process is a time series process. For each AS link, the result of each discrete event is its spatial activity value. For links with uncertain activity, the activity value is 0. In addition, an observation time window needs to be set to calculate the temporal activity value of the AS link, which is the sum of the spatial activity values in the time window. If the average activity value of a link in the Active state is lower than the threshold over a period of time, its status is changed to Uncertain. If the average activity value of a link in the Uncertain state is lower than the threshold over a period of time, a path hijacking alarm is triggered. This situation is deleted if it reaches a preset aging time. Otherwise, its status changes to Active.

3.3.2 Network Congestion Analysis

3.3.2.1 Scenario Description

Packet loss on a mobile transport network affects the TCP throughput. When the packet loss rate exceeds a specified threshold, the TCP throughput decreases sharply. As such, the packet loss rate is an important indicator reflecting the transport network quality and has a significant impact on user experience. Network congestion analysis focuses on visualizing and troubleshooting base station traffic suppression. It offers a complete O&M solution that visualizes network-wide E2E traffic suppression and poor regional quality of service (QoS) status, and implements fast fault demarcation and location. Network congestion analysis uses the following measurement technologies:

- **Two-Way Active Measurement Protocol (TWAMP):** a standard measurement solution defined in RFC 6038. It is compatible with most routers and base stations. It deploys TWAMP test cases to measure the packet loss rate, delay, and jitter of a link from the source to the destination, monitor network service quality in real time, and assist in fault demarcation.
- **In-situ Flow Information Telemetry (IFIT):** a passive measurement technology that works similarly to IP flow performance measurement (IP FPM). It adopts the coloring mechanism (RFC 8321) to directly measure the performance of service packets and collects the actual values of performance indicators such as the packet loss rate, delay, and traffic rate on an IP network.

Network congestion analysis provides the following capabilities:

- **Network-wide E2E traffic suppression visualization:** displays the distribution of traffic suppression on a heatmap and visualizes network congestion points; prioritizes high-value areas; drills down to the problem base stations; provides precise capacity expansion suggestions.
  Network congestion analysis measures base station SLAs through TWAMP and IFIT. It calculates the suppressed traffic of a base station based on the collected packet loss rate and actual traffic, and determines whether the base station has poor QoS. Based on this analysis, the system visualizes E2E traffic suppression on the entire network and displays suppressed traffic in each region.
- **Fast fault demarcation and locating:** displays the packet loss distribution of base station services; restores the hop-by-hop path for a single base station service based on different time points; analyzes the impact of link SLAs and bandwidth on packet loss to implement accurate fault demarcation and location.

3.3.2.2 Key Technologies

1. Path Restoration Algorithm

Network congestion analysis uses TWAMP for congestion demarcation, restores the topology (E2E paths) through the Link Layer Discovery Protocol (LLDP), analyzes the root causes of congestion, and provides suggestions based on analysis results and expertise.

- Traceroute is used to trace the routes of packets for obtaining the inbound and outbound interfaces of involved NEs on the network.
- The Shortest Path Fast Algorithm (SPFA) is used to restore the shortest path in an AS. If load balancing is enabled, multiple equal-cost paths are restored.
- IFIT is used to automatically restore precise paths and analyze congestion/poor-QoS locations and root causes hop by hop, with optimization suggestions provided.

2. High-Precision SLA Measurement Technology

Network Digital Map enables high-precision and high-accuracy packet loss measurement through in-situ flow and per-packet measurement, implements microseconds-level delay measurement through real-time per-hop reporting with telemetry, and clusters mass network faults through big data analysis and AI algorithms, improving service experience.

- **In-situ flow measurement:** directly measures packets for the path information and delay, and supports measurement of a variety of services, such as auto-identified flows, custom flows (five-tuple or two-tuple), and VPN services.
- **Per-packet measurement:** measures packets one by one to accurately identify even tiny packet losses among massive data.
- **Per-hop diagnosis:** automatically triggered by poor-QoS flows, replays historical paths, measures per-hop SLAs, and performs KPI association analysis.
- **Seconds-level data collection through telemetry:** enables continuous data push when subscribed and efficient transmission using GPB. It is used by IFIT to report data in mere seconds to NCE for aggregation and calculation, achieving real-time data reporting and processing of massive data.
- **Big data analysis:** efficiently processes massive IFIT per-hop, per-packet data based on seconds-level query enabled by the data analysis platform.
- **AI intelligent analysis:** uses the clustering algorithm to accurately cluster poor-QoS events into mass network faults.
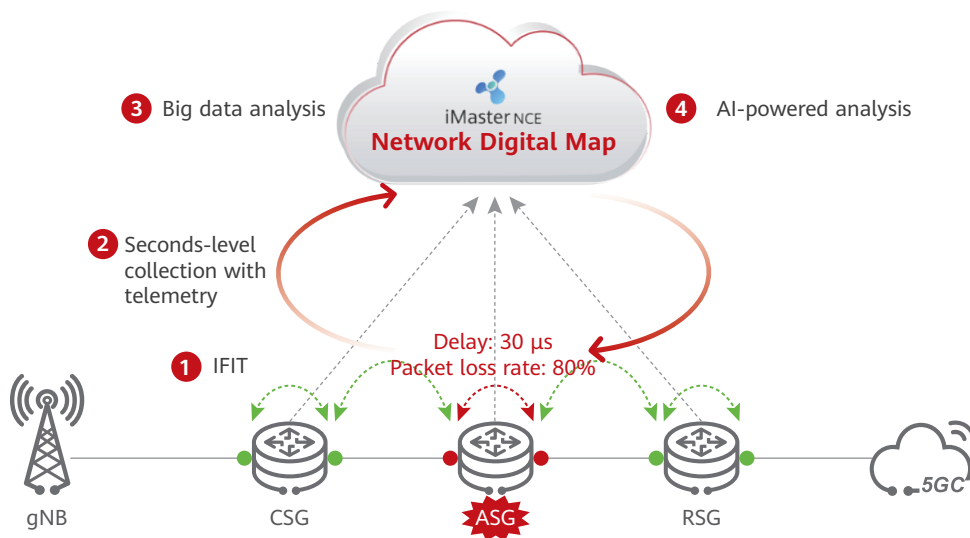
3. Ring Discovery Algorithm

In typical IP RAN networking, a network topology can be divided into the access ring, aggregation ring, and core ring. Unlike traditional traffic statistics by port and link, traffic statistics by ring helps accurately locate network bottlenecks and congested paths and provides a data model for bandwidth forecast. Due to frequent power-off and fiber cuts, insufficient fiber resources, and co-routing on the live network, a large number of non-standard networking scenarios exist, such as tangent rings, mesh rings, and rings in ring, resulting in difficult ring discovery.

The maximum-bandwidth-first algorithm for ring discovery delivers higher accuracy and is effective in non-standard networking scenarios.

- **Ring link algorithm:** uses a deep traversal algorithm to automatically identify links that can form a ring based on physical connections.
- **Tangent ring algorithm:** uses the maximum-bandwidth-first algorithm to preferentially home traffic on tangent links to high-bandwidth rings and make low-bandwidth rings level-2 rings.
- **Ring hierarchy algorithm:** uses a label-based role level identification algorithm to automatically identify the ring hierarchy.
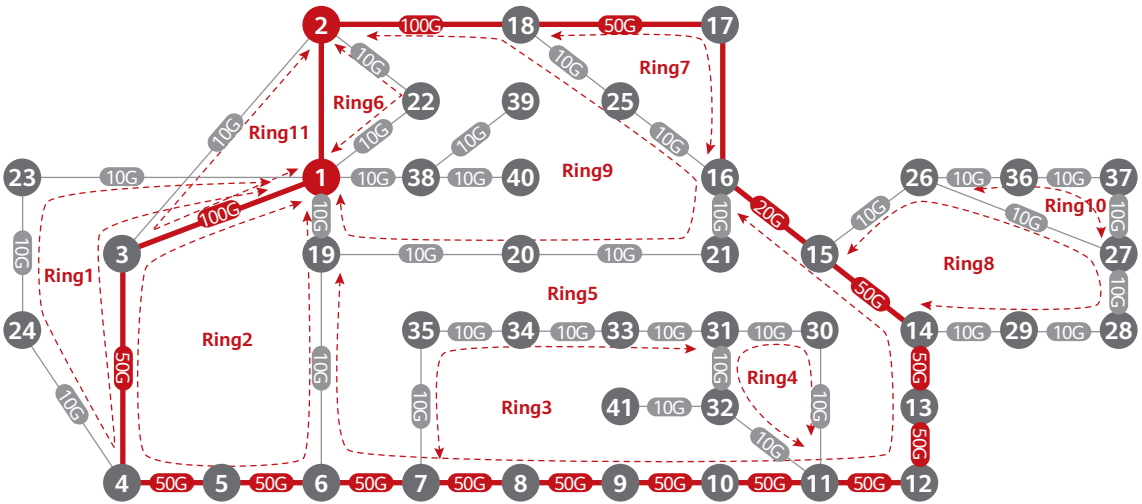
4. Suppressed Traffic Algorithm

After long-term network optimization, customers' wireless networks benefit less and less from network remodeling with the same level of investment. The transport network has become the network bottleneck, as opposed to the wireless air interface. The urgent issue facing customers is how to evaluate and remodel the transport network and release suppressed traffic. Network Digital Map analyzes the packet loss on transport networks based on the live-network base station suppression ratio and the packet loss rate statistics, identifies the base stations and links with KPI anomalies, and analyzes the causes of performance deterioration at fault points. In this way, it evaluates network quality in an E2E manner and analyzes the impact of transport networks on wireless traffic suppression, supporting network remodeling and improving customer benefits.

- **Suppressed traffic algorithm:** fits a suppressed traffic curve based on the traffic suppression theory and data collected from the live network.

$$\text{Traffic suppressed} = \sum_{t=0}^{n}(\text{Volume}_t^{3G} * SR_t^{3G} + \text{Volume}_t^{4G} * SR_t^{4G})$$

SR: suppression rate calculated based on the packet loss rate
Volume: total traffic within the hour t. t ranges from 00:00 to 23:00.

- **Network optimization suggestions:** precisely guide network reconstruction based on the diagnosis of transport networks using the suppressed traffic algorithm.

3.3.3 Intelligent Incident Analysis

3.3.3.1 Scenario Description

Currently, hardware, forwarding, and configuration errors on the network cannot be perceived clearly. Even when faults are perceived, there are no effective means to locate them. The inefficiency of checking massive alarm data prolongs service interruption times. For IP networks such as 5G transport and intelligent metro networks, Network Digital Map builds a fault propagation model based on O&M big data, AI, and expert knowledge and conducts continuous online self-learning. This reduces O&M costs, improves troubleshooting efficiency, and reduces dependence on experts.

Lower O&M costs	Network Digital Map clusters network events and alarms and performs association analysis to reduce redundant alarms, tickets, and thus O&M costs.
Higher troubleshooting efficiency	Network Digital Map clusters the events and alarms related to the same fault into one incident through association analysis by time and topology and identifies the root event, achieving "one incident, one ticket" and avoiding unnecessary ticket dispatching.
Less dependence on experts	Event clustering and RCA are based on massive O&M data, extensive expert knowledge, and AI algorithms. They can work automatically without experts, even for faults that are difficult to handle manually, facilitating comprehensive and quick troubleshooting.

3.3.3.2 Key Technology: AI-based RCA Algorithm

Network Digital Map introduces an AI-based RCA algorithm into its self-developed streaming framework to cluster alarms based on time and topology and identify root events in real time. It intelligently computes the correlations between faults, generates fault propagation graphs, and performs RCA, relieving O&M personnel from unnecessary or correlative events and improving troubleshooting efficiency.

Data collection and processing	The algorithm collects network alarms and mines temporal and spatial statistical features of alarm data to output an alarm-based high-dimensional dataset.

Online training

The algorithm provides data, model training, model generation, and model inference services to iteratively train event clustering models and fault propagation graphs, creating a more generalized and intelligent model.

Online inference

The algorithm clusters alarms and performs RCA in real time. It aggregates scattered alarms into groups of incidents based on cluster distance, with intermittent and repeated incidents compressed.

Impact analysis

Through expertise-based association analysis, the algorithm determines the impact on services, helping users identify major incidents that affect many services.
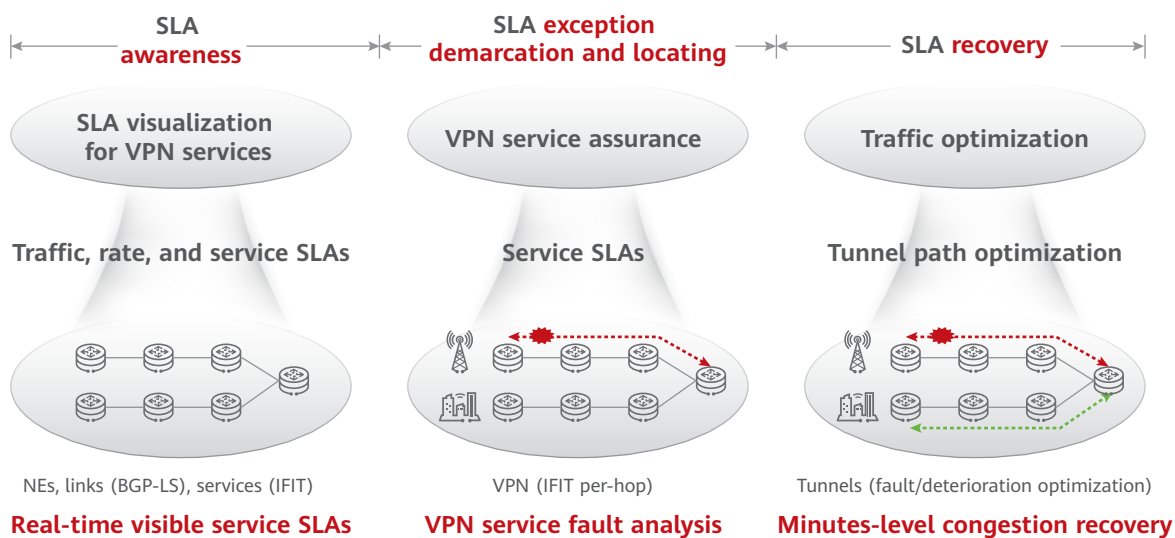

Events

Event clustering inference

Correlative

Inference based on the fault propagation graph

Result

Root cause

Updating of the association model

Updating of the fault propagation graph

| All events at 00:00 every day | Accumulation with existing project events | Re-inference of the (project-level) association model | Automatic feature extraction | Neural network model training |

Online incremental self-learning for smarter models

▣ 3.4 Optimization Phase

3.4.1 Intelligent Network Optimization

3.4.1.1 Scenario Description

1. Automatic Tunnel Path Optimization Preventing Network Congestion

Traditional telecom networks provide undifferentiated connection services, leading to resource waste on less demanding services and insufficient resources for demanding ones. To address this issue, IPv6+ networks need to offer differentiated network services based on service requirements to strike the best trade-off between resources and quality. Differentiated SLA assurance provides network connections with just enough bandwidth, delay, and availability for specific services. After network services run for a period of time, resource imbalance arises. Some links are overloaded while others are underloaded. Network Digital Map is designed to accurately detect service quality changes, quickly locate network quality deterioration points, and optimize service traffic in time to realize load balancing and improve network throughput, while fulfilling SLAs.

SLA awareness	SLA exception demarcation and locating	SLA recovery
SLA visualization for VPN services	VPN service assurance	Traffic optimization
Traffic, rate, and service SLAs	Service SLAs	Tunnel path optimization
NEs, links (BGP-LS), services (IFIT)	VPN (IFIT per-hop)	Tunnels (fault/deterioration optimization)
Real-time visible service SLAs	**VPN service fault analysis**	**Minutes-level congestion recovery**

- SLA awareness: uses BGP-LS to quickly detect network topology changes, including node and link faults as well as link bandwidth and delay changes; implements in-situ flow measurement through IFIT and seconds-level reporting through telemetry to accurately measure service SLAs and show network and service quality by layer.
- SLA exception demarcation and locating: automatically checks each hop with IFIT upon service quality deterioration; identifies faulty points in service forwarding paths; visualizes demarcation and location results in the network topology.

- SLA recovery: uses multi-factor cloud-map algorithms to recompute network paths based on the SLA exception demarcation and location results; re-optimizes network paths using technologies such as SR-TE and SR Policy to bypass the faulty points and satisfy service SLAs.

The multi-factor cloud-map algorithms can be classified into:

Multi-factor single-path algorithm	Computes the optimal path based on the specified policy, while meeting multi-factor constraints. Path computation policies include least TE metric, least IGP cost, minimum delay, maximum availability, and bandwidth balancing. Different policies can be applied to different tunnels to achieve the optimal network status. Path computation factors include bandwidth, delay, hops, packet loss rate, bit error rate (BER), availability, slicing, affinity (exclude-any, include-any, and include-all), explicit/excluded paths, and co-routing. These factors can work with each other to meet differentiated service requirements. In addition, backoff is supported. That is, the algorithm prioritizes the optimal path that meets all constraints. If no such path is found, the algorithm intelligently computes the path closest to the constraints.
Multi-factor multi-path algorithm	Adds constraint factors between paths in comparison to the multi-factor single-path algorithm. Such algorithms include the primary/backup path disjoint algorithm, tunnel path disjoint algorithm, and unequal cost multipath (UCMP) multi-segment algorithm.
Multi-factor multi-service algorithm	Schedules paths for multiple services in order to achieve network-level targets in throughput, cost, and delay. Such algorithms include the local optimization algorithm and global optimization algorithm. Users can specify links and tunnels for manual optimization, or perform global automatic optimization based on specified bandwidth thresholds, delay constraints, packet loss rate constraints, BER thresholds, etc.

To offer differentiated SLA assurance to different tenants, each service requires a tunnel, which means a 100x increase in the number of tunnels. To implement E2E control of network-wide paths, the controller must be able to manage a massive number of tunnels. Network Digital Map supports millions of tunnels and takes mere minutes to compute paths network-wide, even meeting future requirements of super-large-scale network management. E2E network management can be full realized through just one map.

2. Real-Time Scheduling of IP Traffic to Satisfy SLAs

Most CSPs' IP backbone networks run BGP for traffic forwarding. BGP does not consider factors such as network bandwidth utilization and costs during forwarding. Network SLA experience deteriorates when traffic congestion occurs on backbone networks or traffic imbalance occurs on the outbound direction of Internet data centers (IDCs) or inbound direction of metropolitan area network (MAN) egresses or integration gateways (IGWs). Traditionally, such problems were solved by manually optimizing IP network traffic, which was time-consuming, error-prone, and heavily reliant on engineer expertise. Network quality could not be restored quickly.

Network Digital Map introduces intelligent IP flow collection, analysis, and scheduling. It collects network topology, routing, and flow information in real time, and aggregates, analyzes, and displays the collected flow information from multiple dimensions, helping users identify key network bottlenecks and develop optimization solutions. It utilizes BGP FlowSpec to import specified IP flows to tunnels for traffic optimization, implementing IP flow–based SLA assurance.
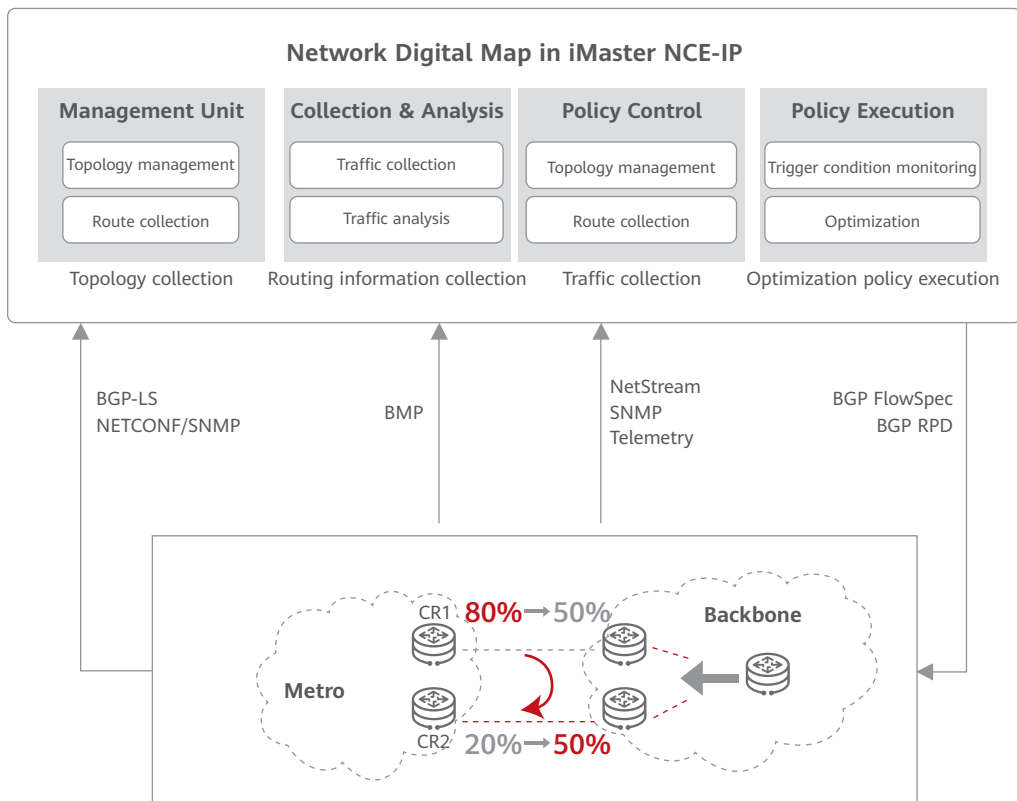
- **Real-time flow collection:** collects specific network topology in real time through BGP-LS; collects routing information in real time through BMP; dynamically collects traffic data on links and ports through NetStream/SNMP.
- **Multidimensional flow analysis:** automatically classifies, aggregates, and analyzes collected network traffic data to quickly generate predefined reports; generates Top N analysis reports in multiple aggregation modes, such as source IP address+destination IP address, source IP address+destination community, source IP address+destination AS, source community+destination IP address, source IP address, source community, destination IP address, destination community, and
- destination AS.

  Intelligent flow scheduling: intelligently spots key bottlenecks in traffic optimization and recommends optimization solutions based on multidimensional flow analysis; supports online preview of traffic optimization results to evaluate optimization benefits; converts traffic scheduling policies into BGP FlowSpec routes and delivers them to forwarders.

3.5.1.2 Key Technology: Multi-Factor Cloud-Map Algorithm

The multi-factor cloud-map algorithms of Network Digital Map obtain the network topology and bandwidth resources using BGP-LS, and perform unified management and path computation for network-wide tunnels. They aim to satisfy the SLA requirements of different tunnels with different priorities (that is, computing optimal paths for highest-priority tunnels and proper paths for lower-priority tunnels), achieving optimal bandwidth efficiency on the network.

Network Digital Map builds cloud-map algorithms based on the graph theory and operations research and optimization. The former is used for multi-factor path computation, and the latter is used for network flow scheduling. Network flow scheduling can be modeled as a linear programming problem. However, it is impossible to model all feasible paths between two points on the network, so column generation is introduced to incrementally compute feasible paths. The steps for column generation of linear programming are as follows.
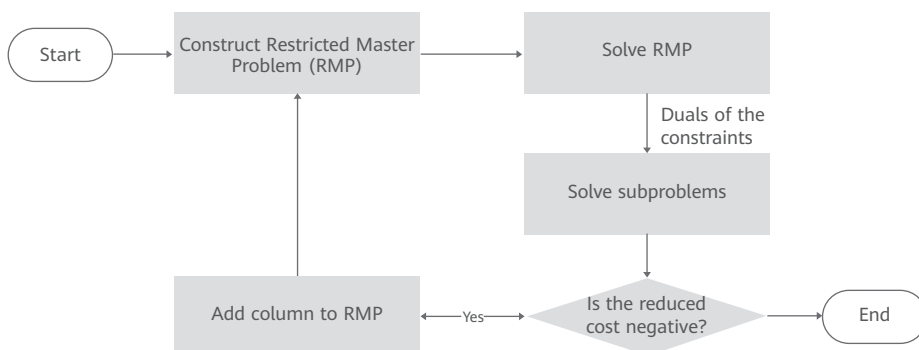
1. Construct a restricted master problem (RMP). That is, use a **multi-factor path algorithm** to compute the shortest path that meets the bandwidth requirements of each network flow. If no such path is found, a virtual path with an infinite cost is used to build a linear programming model.
2. Solve the RMP using a **linear programming solver** to obtain the dual variables of all constraints.
3. Compute new paths. Specifically, weigh links according to the dual variables and solve the subproblems, that is, compute the shortest path for each network flow by using a **multi-factor path algorithm**.
4. Refresh the new paths to check whether any of them have a negative reduced cost. If so, add them to the linear programming model and continue with step 2. If not, end the iterative column generation.

This process involves the following key technologies:

- **Multi-factor path algorithm**
  The multi-factor path algorithm in cloud-map algorithms consists of a series of atomic algorithms that solve specific problems. These atomic algorithms include classical problems such as max-flow min-cut, graph matching, graph search, and traveling salesman problems, as well as classical optimization methods such as Lagrangian relaxation and subgradient optimization. Based on the constraint factors configured for services, multiple atomic algorithms can be assembled into a multi-factor path algorithm to meet differentiated service requirements. Constraint factors are classified into single-point and E2E ones. Single-point constraint factors refer to those on a single node or link, such as bandwidth, affinity, excluded path, packet loss rate, and BER. E2E constraint factors refer to those on E2E paths, such as explicit path, delay, and hop count. The multi-factor path algorithm not only satisfies all the single-point constraint factors, but solves the NP-hard problems of E2E constraint factors.

- **High-performance large-scale linear programming solver**
  The linear programming solver in cloud-map algorithms is designed based on the typical characteristics of network flow optimization. It supports incremental solution, greatly improving solution performance.

3.4.2 Energy Analysis

In the context of the global energy crisis, countries are accelerating their journey to carbon neutrality. 29 CSPs around the world have signed to reduce carbon emissions by 45% by 2030. Currently, IP transport devices consume about 20% of the energy on the communications network, second only to base stations. Conventional NMSs mainly monitor alarm and performance as opposed to device power consumption. As such, power consumption efficiency is hard to analyze, and efficient scheduling of network power is often not possible. CSPs are unable to monitor the network and analyze data thoroughly in real time. Energy-saving policies then become difficult to formulate and execute. Energy View of Network Digital Map provides a way to visually manage and optimize the energy consumption of IP networks. It brings CSPs closer to their energy conservation and emission reduction targets and the goal of "green site, green network, and green operation."
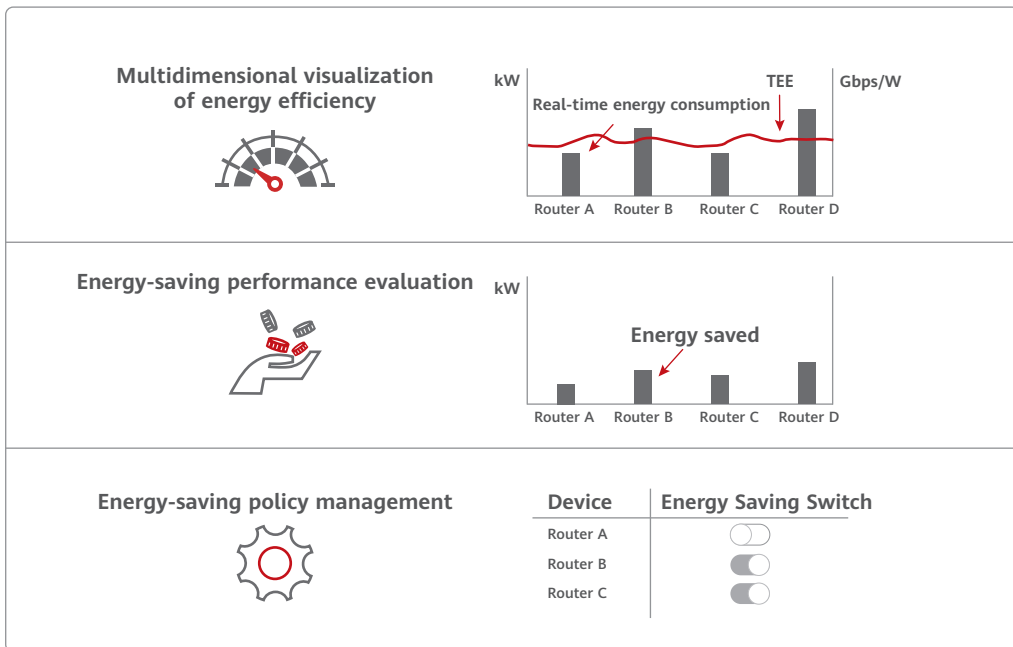
- **Multidimensional visualization of energy efficiency:** provides an energy monitoring dashboard to display power consumption data at the network and NE levels. By analyzing power consumption data from different dimensions, it facilitates the demarcation and location of power consumption issues by network departments. In addition, it forecasts the benefits of energy-saving devices to identify the energy-saving potential of the network, statistically supporting the formulation of energy-saving policies.

- **Energy-saving performance evaluation:** collects actual energy savings and outputs energy-saving benefit curves for devices; supports history comparison and analysis to evaluate the energy-saving benefits and quantify energy-saving performance.
- **Energy-saving policy management:** visualizes the energy-saving status of network-wide resources in real time; forecasts energy-saving benefits to quickly identify the resources with the highest energy-saving benefits to improve policy formulation efficiency; enables network-level energy-saving policy deployment using NETCONF/YANG and batch enablement of energy saving in one click to make policy delivery easy and efficient; updates the energy-saving status of devices in real time.

4 Industry Suggestions and Conclusions

◻ 4.1 Industry Suggestions

With the continuous development and evolution of cloud, computing, and networks, telecom CSPs will provide ubiquitous network services for industry applications such as smart cities, energy, public utilities, AR/VR, and Internet of Vehicles (IoV). Data will flow between different clouds, industries, and individuals at an unprecedented scale. As the infrastructure for data flows, IP networks — in addition to providing high bandwidth, deterministic delay, and secure and reliable intelligent connections — must respond to computing power scheduling requirements in real time to make the most out of global resources. This poses higher requirements on IP network O&M. With Network Digital Map being the basic platform, CSPs pursuing L4/L5 ADN must fully consider their own service and technical characteristics while working with industry partners to develop ADN level standards, the target architecture of multi-vendor management, southbound interface (SBI) standards, and service-oriented NBI specifications, and accelerate IP network O&M upgrade across industries.

Defining IP ADN levels and evaluation standards to propel industry development

Network Digital Map aims to build a self-fulfilling, self-optimizing, self-healing IP network and achieve intelligent network O&M. Reference standards and continuous evolution paths are indispensable. Although the TM Forum has defined the vision of L0–L5, what it provides is just a set of general standards, which need to be further refined based on the service, network, and technical characteristics of IP networks to define IP ADN levels and evaluation standards. Specifically, CSPs can draw from the TM Forum's hierarchical framework to define O&M scenarios for the IP network lifecycle (planning, construction, maintenance, and optimization), break down O&M processes and tasks based on the O&M scenarios, and refine the human and machine parts in each O&M task to form ADN level standards suitable for IP networks. When IP ADN level standards are ready, the industry can determine operable evaluation methods to facilitate evaluation of ADN levels.

For CSPs, the IP ADN levels and evaluation standards not only guide the intergenerational evolution of IP networks, but drive the cohesion of all stakeholders. The hierarchical evaluation system can be used to evaluate the live network, help formulate network O&M upgrade policies and plans, and boost business performance.

For suppliers, on the basis of full understanding of customer requirements, the IP ADN levels and evaluation standards will inform decision-making during capability planning and technology selection for Network Digital Map. This is conducive to continuous product evolution.

Defining an open target architecture and SBI/NBI standards to drive industry prosperity

Since their inception, IP networks have had open architectures. Many CSPs' IP networks are composed of devices from different vendors, and multi-vendor devices are often equipped with distinct interfaces, forcing many CSPs to define enterprise standards. However, such proprietary standards usually take months or even years from specification definition to product development, admission testing, and network deployment, which seriously impedes the digital progress of networks. It is therefore necessary to define a system architecture and SBI standards for Network Digital Map to enable multi-vendor management.

- **Open target architecture:** Network Digital Map is built on an open architecture. For multi-vendor scenarios, instead of performing a software upgrade to roll out new services, CSPs can simply customize plug-ins onsite to adapt to vendor differences.

- **Standard SBIs:** The SBI standards formulated for Network Digital Map help device vendors comply with the same interface standards during device development. In this way, devices from different vendors can be uniformly managed at a faster pace, preventing resource waste caused by repeated construction.

- **NaaS:** NaaS is the trend of the times. However, transitioning from individual pilots to full deployments requires industry-wide efforts and consensus on business drivers and gradual evolution. IP NaaS involves requirement modeling, service catalog definition, service design, etc. Network functions are built as atomic services to shield the complexity of underlying networks and make network capabilities available as services for users, achieving the best possible user experience, efficient operations, and sustainable business.

CSPs can use networks like services and integrate with upper-layer service systems conveniently and quickly. This lays a foundation for automation and intelligence, and greatly improves network service quality and O&M efficiency. Suppliers can use open system architecture and unified SBI/NBI standards to quickly meet customer requirements and guide the design and development of Network Digital Map products.

4.2 Conclusions

IP networks are the cornerstone of digital development and a vital nexus between things and applications. Amidst the digital transformation of a myriad of industries, IP networks are facing new requirements, such as massive IoT, ultra-large bandwidth, deterministic service, and security and reliability. To meet these new requirements, Huawei has launched Network Digital Map to build a highly intelligent, closed-loop, autonomous, and low-carbon digital O&M platform, to serve as the digital foundation for industries to go digital. Network Digital Map will assist CSPs in their transformation from traditional ICT services to future-proof DICT services, fueling breakthroughs in emerging technologies across all areas of society.

5 References

1. ADN Solution White Paper (Autonomous Driving Network), Huawei, 2021.
2. IG1218 Autonomous Networks Business Requirements and Framework, TM Forum, 2021.
3. IG1230 Autonomous Networks Technical Architecture, TM Forum, 2021.
4. IG1251 Autonomous Networks – Reference Architecture, TM Forum, 2021.
5. IG1252 Autonomous Network Levels Evaluation Methodology, TM Forum, 2021.
6. Wide Area Network as a Service White Paper, Huawei, 2022.
7. Intelligent Cloud-Network Solution White Paper, Huawei, 2022.
8. BGP Security in 2021, MANRS, 2022.

6 Glossary

Abbreviations	Full name in English
SRv6	egment Routing over IPv6
IFIT	In-situ Flow Information Telemetry
NaaS	Network as a Service
SLA	Service Level Agreement
TMF	TeleManagement Forum
SID	Tshared Information Model
ADN	Autonomous Driving Network
SDN	Software Defined Network
OLTP	Online Transaction Processing
OLAP	Online Analytical Processing
MO	Managed Object
IGP	Interior Gateway Protocol
BGP	Border Gateway Protocol
CPV	Control Plane Verification
DPV	Data Plane Verification
DFS	Depth-first Search
HSA	Header Space Analysis
SSP	Specific Service Plugin Pkg
SND	Specific NE Driver Pkg
BGP-LS	Border Gateway Protocol-Link State
BMP	BGP Monitoring Protocol
NetConf	Network Configuration Protocol
OSS	Operations Support System
EMS	Element Management System
IP Native	Internet Protocol Native
DC	Data Center
AI Native	Artificial Intelligence Native
5G	5th-generation Mobile Communications Technology