



iMaster NCE-Campus Brochure



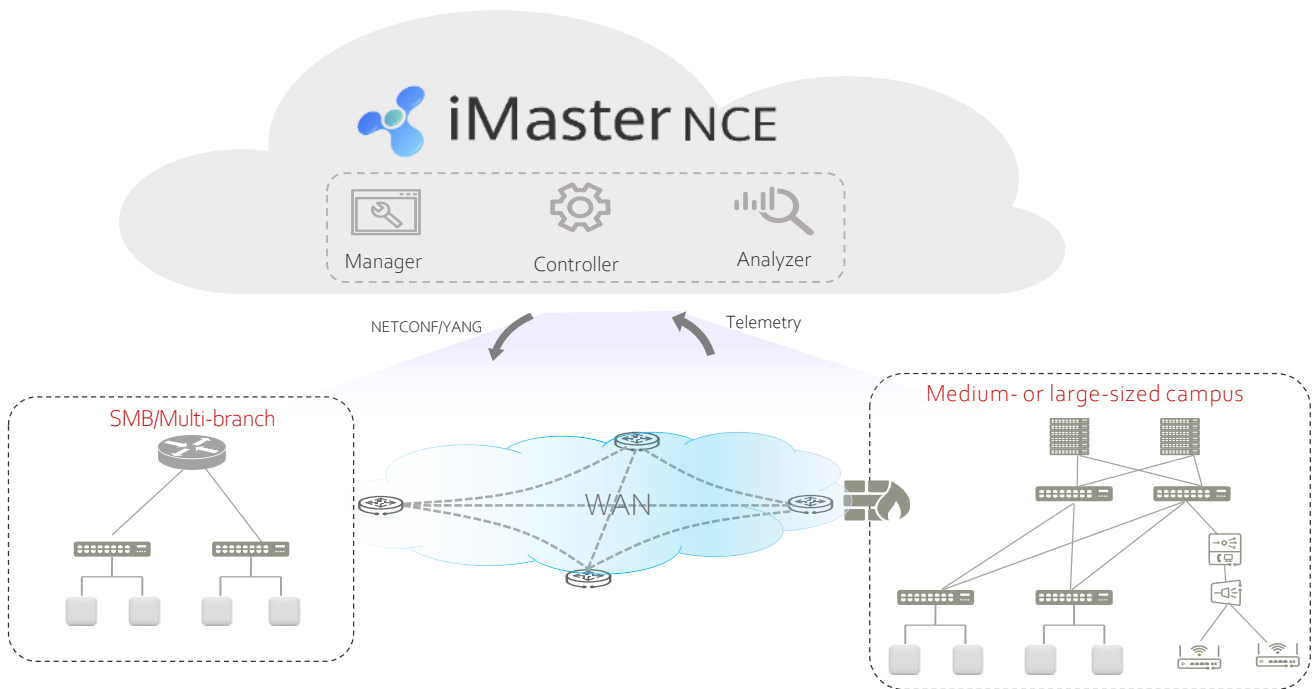
iMaster NCE-Campus Brochure

Product Overview

iMaster NCE-Campus is Huawei's next-generation autonomous driving network management and control system for campus networks. This first-of-its-kind intelligent network automation platform integrates management, control, and analysis functions, provides full-lifecycle automation of campus networks, and implements intelligent fault closure through big data analytics. These innovative features help enterprises reduce OPEX and O&M costs, accelerate enterprise cloudification and digital transformation, and achieve automated and more intelligent network management.

Solution Description

With the rapid development of enterprise services and comprehensive digital transformation of campus networks, campus networks are rapidly developing towards wireless, cloudification, and smartness. In this trend, a large number of innovative services such as BYOD, IoT, cloud UC, office, storage, VR, AR, and live TV are emerging, massive terminals are accessing the network, the network scale is growing exponentially, and various digital services frequently go online or are adjusted. However, the number of network administrators does not increase. If the administrators still manage networks using CLIs and scripts, networks will inevitably become a bottleneck for rapid service innovation and an obstacle for enterprise digitization. As the automatic management center of campus and branch networks, iMaster NCE-Campus is faced with multiple opportunities and challenges: how to accelerate network service deployment, how to provide reliable Service Level Agreement (SLA) guarantee, and finally how to improve user experience and service agility. In campus and branch network scenarios, iMaster NCE-Campus uses cloud computing, SDN, and big data analytics to implement automatic and centralized underlay & overlay management, provide data collection and analysis capabilities beyond traditional solutions, perform centralized control over access rights, QoS, bandwidth, application, and security policies of campus users, and enable service-driven virtual service provisioning in a simplified, rapid, and intelligent mode, transforming the network from an obstacle into an assistant for services.

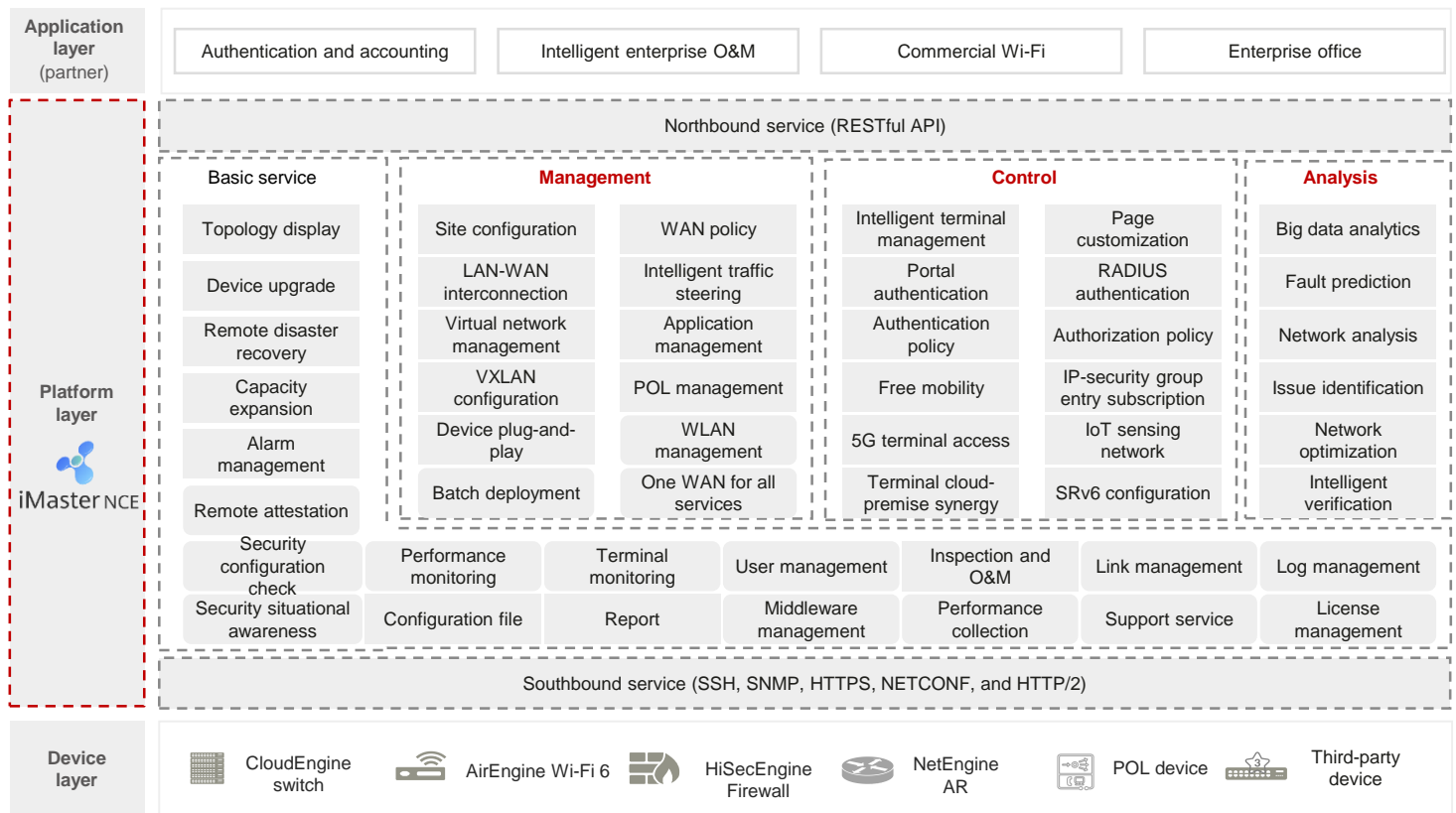


As the intelligent management and O&M center of the campus network, iMaster NCE-Campus covers large- and medium-sized campus networks, SMBs, multi-branch interconnection networks, and IP+POL device convergence networks. It has the following key capabilities:

- **Automatic network deployment:** automated network deployment, automated virtual network service provisioning, automated LAN-WAN multi-branch interconnection, and automated WAN interconnection.
- **Service policy automation:** mass user authentication, intelligent terminal management, 5G terminal access, IoT sensing network, hierarchical QoS scheduling, intelligent verification.
- **Intelligent O&M:** real-time experience visibility, fault locating in minutes, and intelligent network optimization

Key Components

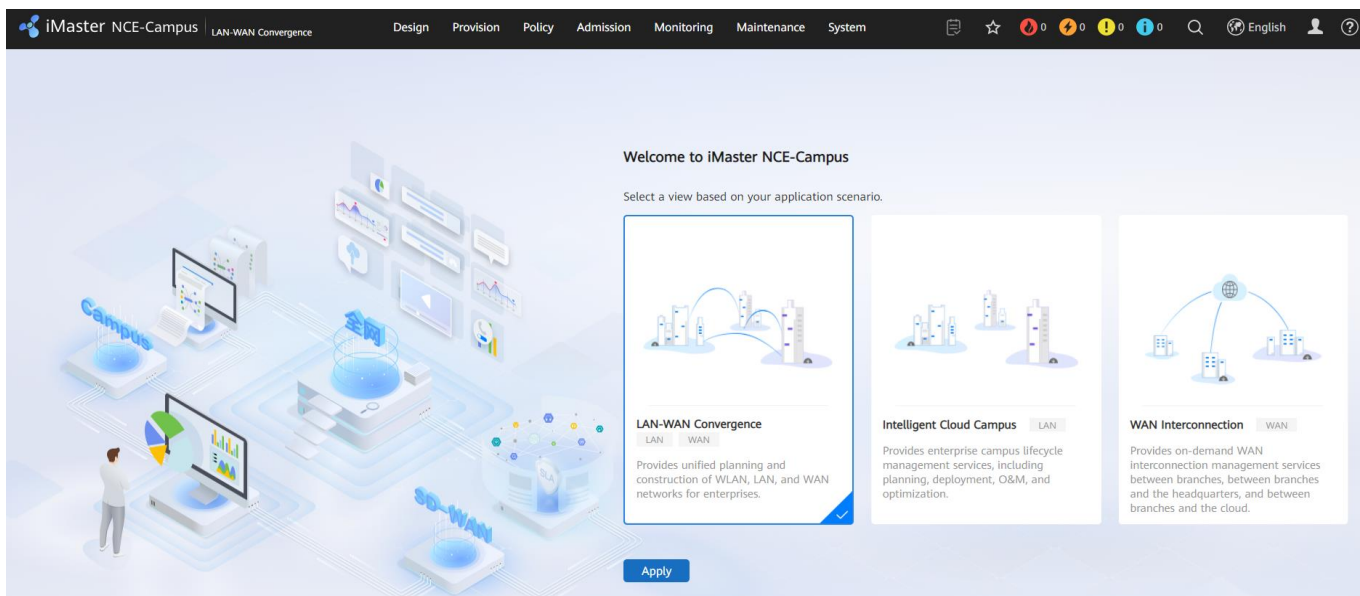
Based on the cloud computing and distributed architecture design, iMaster NCE-Campus adopts the service-oriented module design and supports distributed deployment. The overall architecture of iMaster NCE-Campus consists of four components, basic services, management, control, and analysis.



Benefits

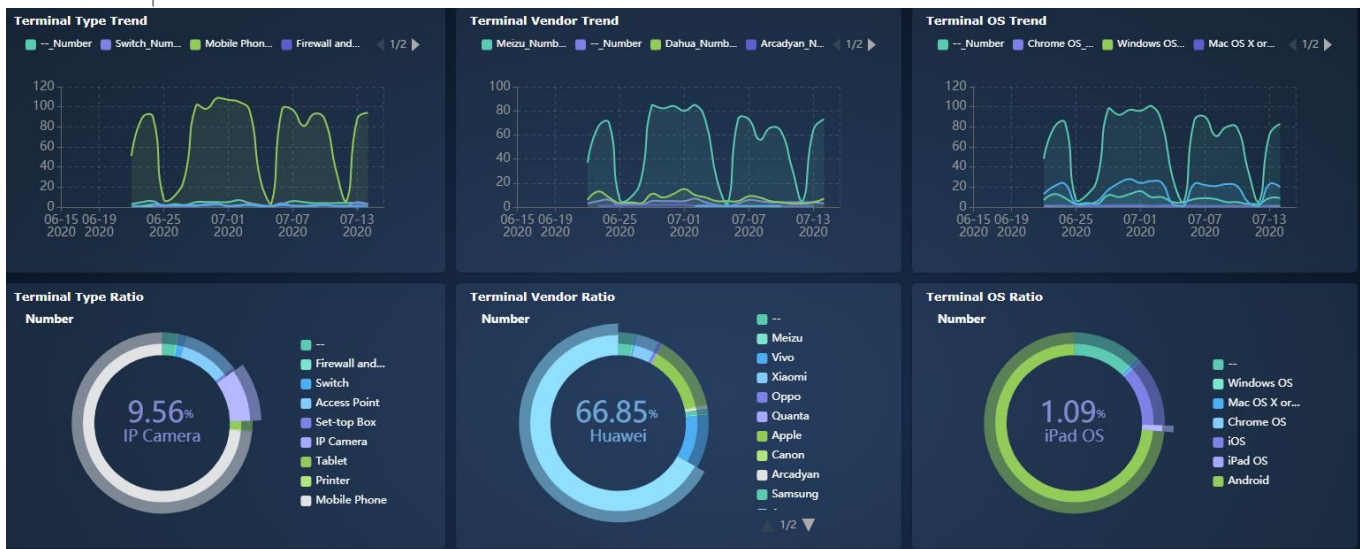
Automatic Network Deployment

- App-based deployment, DHCP-based deployment, and deployment through the registration query center and ZTP-based deployment of POL devices: Devices are plug-and-play and networks are provisioned within minutes, greatly simplifying network deployment and shortening the construction period.
- End-to-end automated VXLAN network deployment: service isolation, one network for multiple purposes, and a wide range of networking models (such as centralized gateway and distributed gateway), enabling more flexible and efficient network adjustment and capacity expansion.
- Multi-branch interconnection: LAN and WAN network devices are centrally deployed, managed, and monitored, guaranteeing services in an end-to-end mode while reducing O&M costs and improving O&M efficiency.
- Campus networks, WAN access networks, and backbone networks are managed in a unified manner. WAN-based path navigation is provided based on SRv6, maximizing network resource utilization.



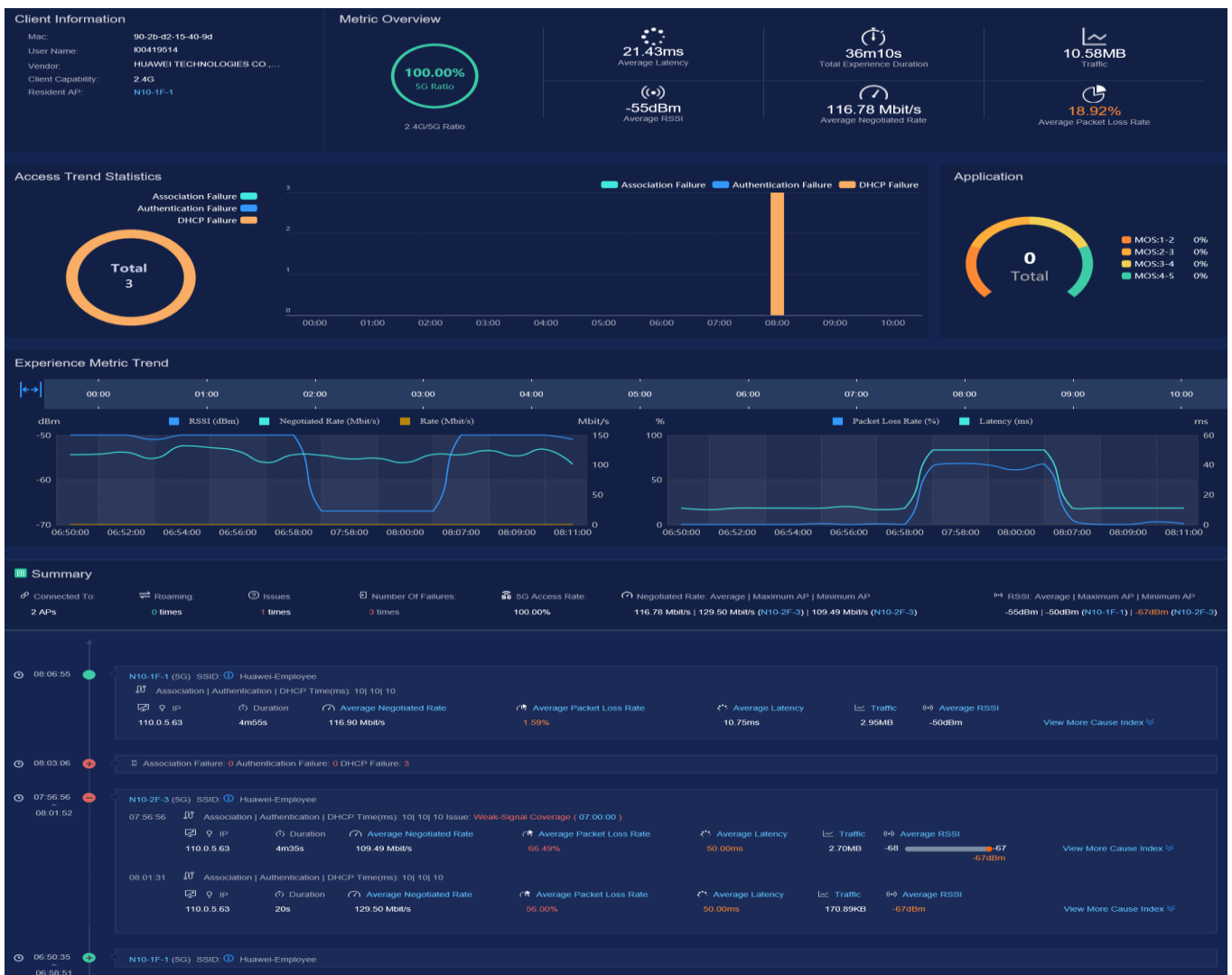
Service Policy Automation

- Massive network device management and user network access authentication: iMaster NCE-Campus supports multiple authentication modes, such as 802.1X authentication, Portal authentication, and social media authentication. Users are decoupled from IP addresses, and can access the network anytime and anywhere with consistent permissions. This ensures free mobility and consistent user experience, ensuring user experience while meeting permission control requirements.
- Built-in terminal fingerprint library: Multiple intelligent identification methods are combined to accurately identify terminal types. Massive IoT terminals are connected intelligently, and policies are automatically matched and delivered, making IoT terminals plug-and-play. Through continuous cloud-based training, a terminal identification fingerprint library that is locally downloaded and deployed can be expanded without limits in cloud-premise synergy mode.
- The IoT sensing network provides rapid and automatic network access for IoT terminals, simplifying and improving the security of IoT terminal access.
- Provide the 5G terminal access authentication capability, ensuring that 5G terminals can access enterprises' campus networks in a secure and reliable manner.
- Intelligent verification: Service rollout or changes may cause network segment or configuration changes. Intelligent verification can be performed to achieve error-free network changes.
- HQoS scheduling based on users and service priorities: Different policies are implemented for different users and applications, achieving more refined bandwidth policy control and effectively ensuring user access experience.



Intelligent O&M

- Real-time experience visibility for each application of each user in each area: With fault backtracking, quickly and intelligently demarcates faulty devices and analyzes root causes for poor quality.
- Continuously trained algorithm: Through proactive issue identification, fault locating in minutes, and intelligent fault prediction, identifies 90% of potential network faults and provides optimal rectification suggestions.
- Real-time wireless network channel conflict evaluation: performs predictive radio calibration, and compares gains before and after calibration, improving network performance by more than 50%.



Specifications List

KeyFeature	Value
Simplified Network Deployment	<ul style="list-style-type: none"> Provides four PnP deployment modes: code scanning-free remote deployment, deployment through app-based barcode scanning, deployment through DHCP, deployment through the registration query center, deployment through the email and ZTP-based deployment of POL devices, to adapt to different network scenarios. GUI-based network planning and deployment and provision network services in minutes.
Automatic Virtual Network Service Provisioning	<ul style="list-style-type: none"> Visualized service configuration and GUI-based fabric planning, configuration, and provisioning. Supports service configuration visualization, topology-based virtual network configuration and monitoring, and real-time service provisioning status query. Automatically establish VXLAN tunnels through BGP EVPN. Supports centralized and distributed VXLAN gateway solutions, providing flexible expansion and high efficiency.
SD-WAN Convergent Management	<ul style="list-style-type: none"> Automatic deployment of HQ-branch and branch-branch lease line services: automatic configuration of all services including service policies, value-added services (VASs), and dynamic VPN connections, simplifying branch network deployment. Application experience-prior: Agile supports comprehensive traffic steering considering bandwidth and link quality. O&M and network-wide application traffic visualization: supports visualized management by application and link, network-wide status visualization, and real-time network status awareness, improving O&M efficiency.
Unified management of campus networks and backbone networks	<ul style="list-style-type: none"> Unified management of campus networks, WAN access networks, and backbone networks SRv6-based traffic steering for private lines such as MSTP, MPLS, Internet, and 5G WAN path navigation, maximizing network resource utilization
Multi-tenant Management	<ul style="list-style-type: none"> Adopts a three-level management model: The system administrator is responsible for platform-wide management and O&M. The MSP administrator can create tenants and provide construction and maintenance services for tenants. The tenant administrator is responsible for deployment and O&M of the local network; alternatively, the tenant administrator can authorize an MSP to manage tenant networks. Supports rights- and domain-based management. In the three-level management model, administrators can be set by role and site to secure network management. Services are invisible between tenants. Data of different tenants is isolated in an E2E mode and distinguished by tenant IDs in the database. In addition, only the corresponding tenant administrator can access data of a tenant. This ensures tenant data security to the most extent.

Key Feature	Value
User Access Authentication	<ul style="list-style-type: none"> Introduces new authentication protocol HTTP2.0, and can authenticate a large number of network devices and users using various access authentication modes, such as 802.1X authentication, Portal authentication, SMS authentication, and social media authentication. It also provides multiple user access control policies. Users decoupled from IP addresses, allowing users to access the network anytime, anywhere with consistent permissions. This ensures free mobility and consistent user experience, ensuring user experience while meeting permission control requirements. Provides the 5G terminal access authentication capability, ensuring that 5G terminals can access enterprises' campus networks in a secure and reliable manner.
Intelligent Terminal Management	<ul style="list-style-type: none"> Built-in terminal fingerprint library: Multiple intelligent identification methods are combined to accurately identify terminal types. Massive IoT terminals are connected intelligently, and policies are automatically matched and delivered, making IoT terminals plug-and-play. The IoT sensing network simplifies and improves the security of IoT terminal access. AI clustering for unknown terminal identification: Unknown terminals with similar fingerprints are clustered into one group, and then the administrator marks the terminal type. These unknown terminals then can be automatically identified.
Intelligent Verification	<ul style="list-style-type: none"> Snapshot comparison: obtains intuitive insights into configuration, topology, and table entry differences by comparing network snapshots at different time points. Insights into global IP subnet connectivity 100% digital modeling of the network environment and real-time, accurate simulation and verification of terminal access rights, enhancing network security and trustworthiness
Intelligent HQoS	<ul style="list-style-type: none"> HQoS scheduling based on users and service priorities: Different policies are implemented for different users and applications, achieving more refined bandwidth policy control and effectively ensuring user access experience.
Intelligent O&M	<ul style="list-style-type: none"> Provides GIS-based networking monitoring, network inspection, and health evaluation to monitor device alarms in real time and detect network conditions in advance for fault prevention. If a fault occurs, provides various fault locating methods to quickly locate and rectify the fault. Real-time experience visibility for each application of each user in each area: With fault backtracking, quickly and intelligently demarcates faulty devices and analyzes root causes for poor quality. Continuously trained algorithm: Through proactive issue identification, fault locating in minutes, and intelligent fault prediction, identifies 90% of potential network faults and provides optimal rectification suggestions. Real-time wireless network channel conflict evaluation: performs predictive radio calibration, and compares gains before and after calibration, improving network performance by more than 50%.
Capability Openness	<ul style="list-style-type: none"> Provides 600+ northbound RESTful APIs for user management, topology management, access authentication, service configuration, and performance monitoring. Leveraging such APIs, Huawei joins hands with 10+ partners to release 30+ industry, greatly simplifies integration with third-party systems and shortens the TTM of services.

Glossary

AR	Augmented Reality
IoT	Internet of Things
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
MSTP	Multi-Service Transport Platform
NCE	Network Cloud Engine
POL	Passive Optical LAN
SD-WAN	Software-defined networking in a wide area network
VR	Virtual Reality
VXLAN	Virtual extensible local area network