NMS Workshop

Arkadiusz Skubida

arkadiusz.skubida1@huawei.com

+48 515 549 519

HUAWEI

Content

Campusowe Systemy NMS

iMaster NCE Campus

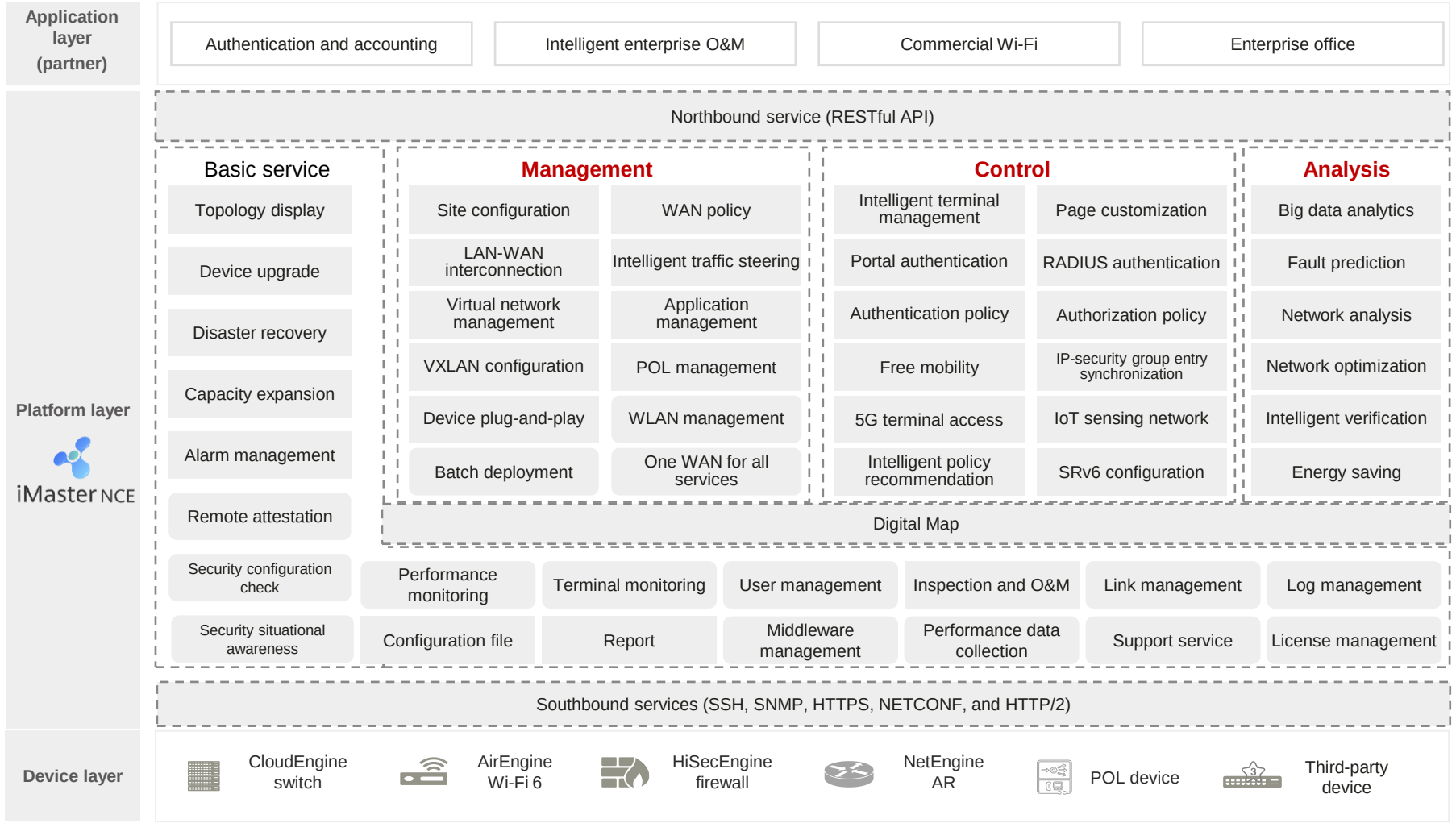
iMaster eSight

iMaster NeoSight

Podsumowanie + Q&A

HUAWEI

iMaster NCE-Campus Architecture



Northbound openness

- 600+ standard RESTful APIs in four types

High reliability

- Keepalive cluster node switchover upon faults
- Remote disaster recovery

Large capacity

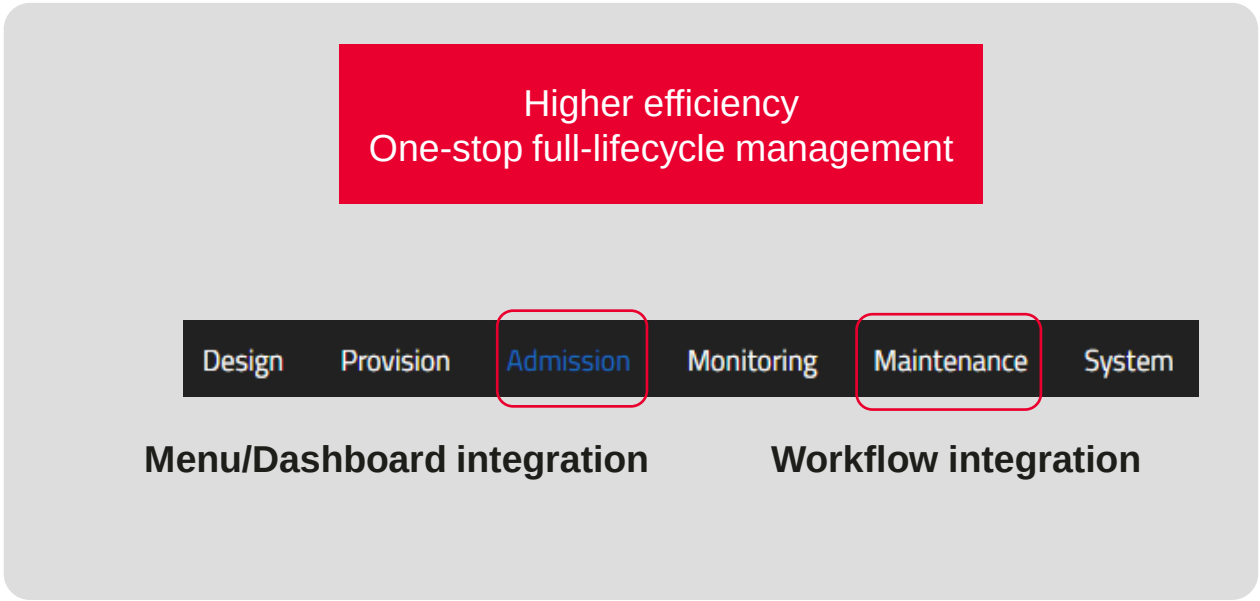
- Managing up to 200,000 NEs in a cluster

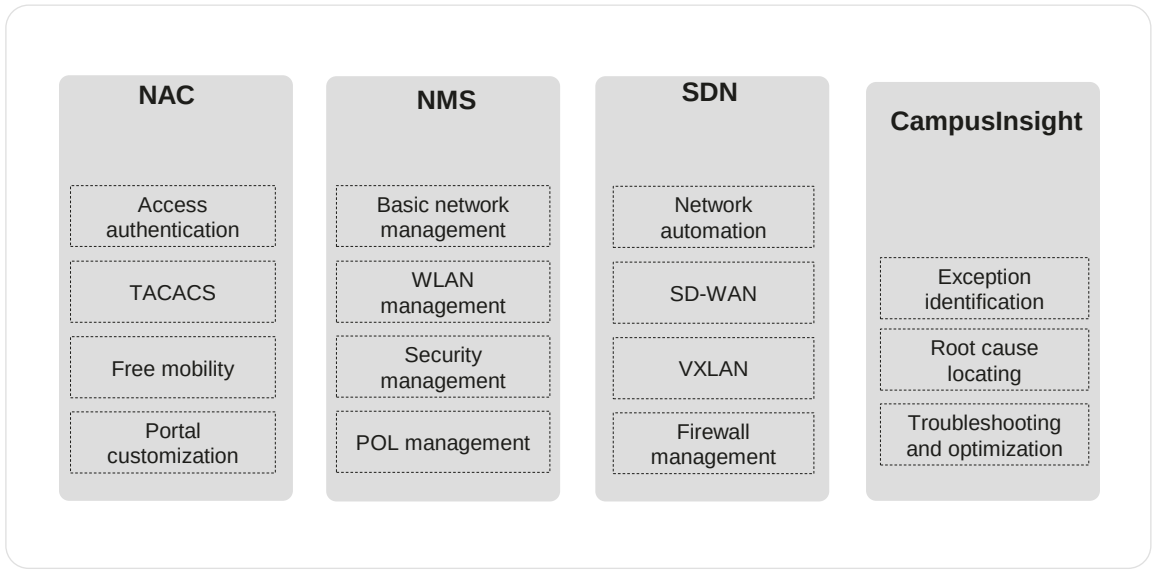
Southbound standard

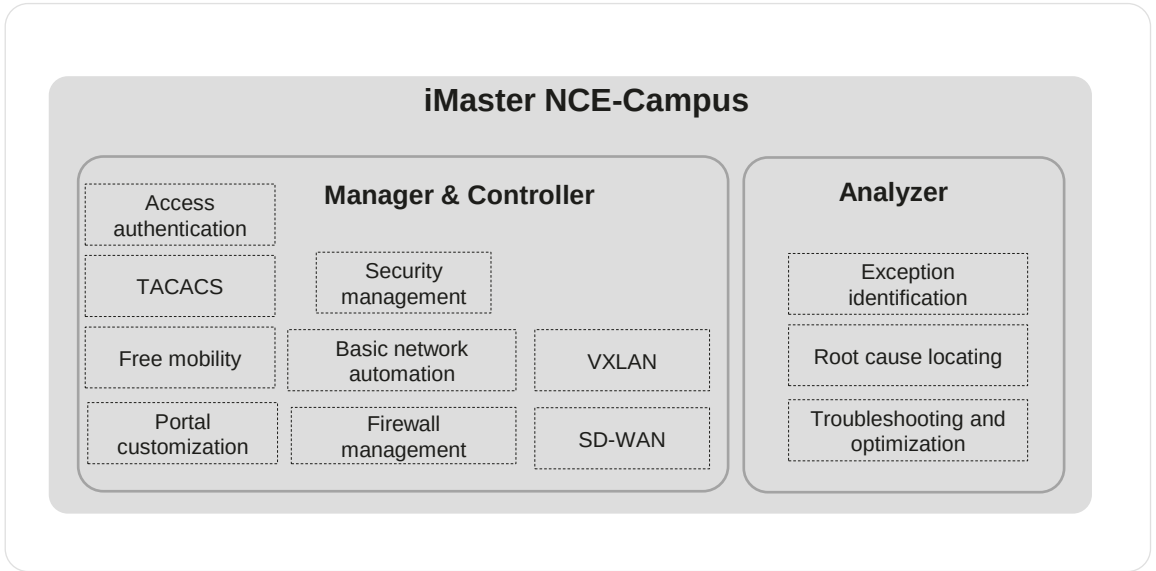
- Multiple protocols, such as NETCONF and SNMP, supporting third-party device monitoring

HUAWEI

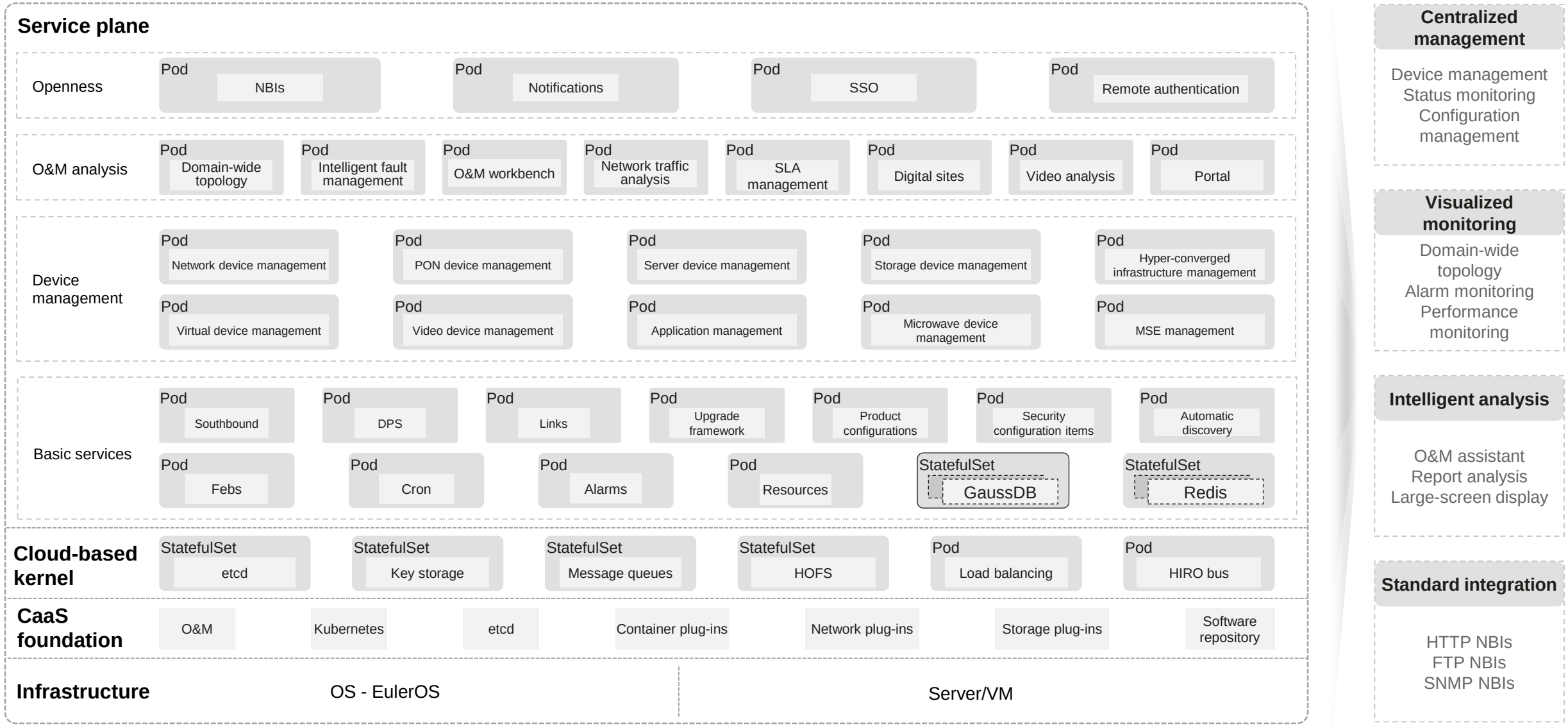
Imaster NCE-Campus - Fully Converged: Manager + Controller + Analyzer







NeoSight's Container-based Architecture Enables Converged, Intelligent, Simplified, Open, and Centralized ICT O&M Products



Centralized management

Device management
Status monitoring
Configuration management

Visualized monitoring

Domain-wide topology
Alarm monitoring
Performance monitoring

Intelligent analysis

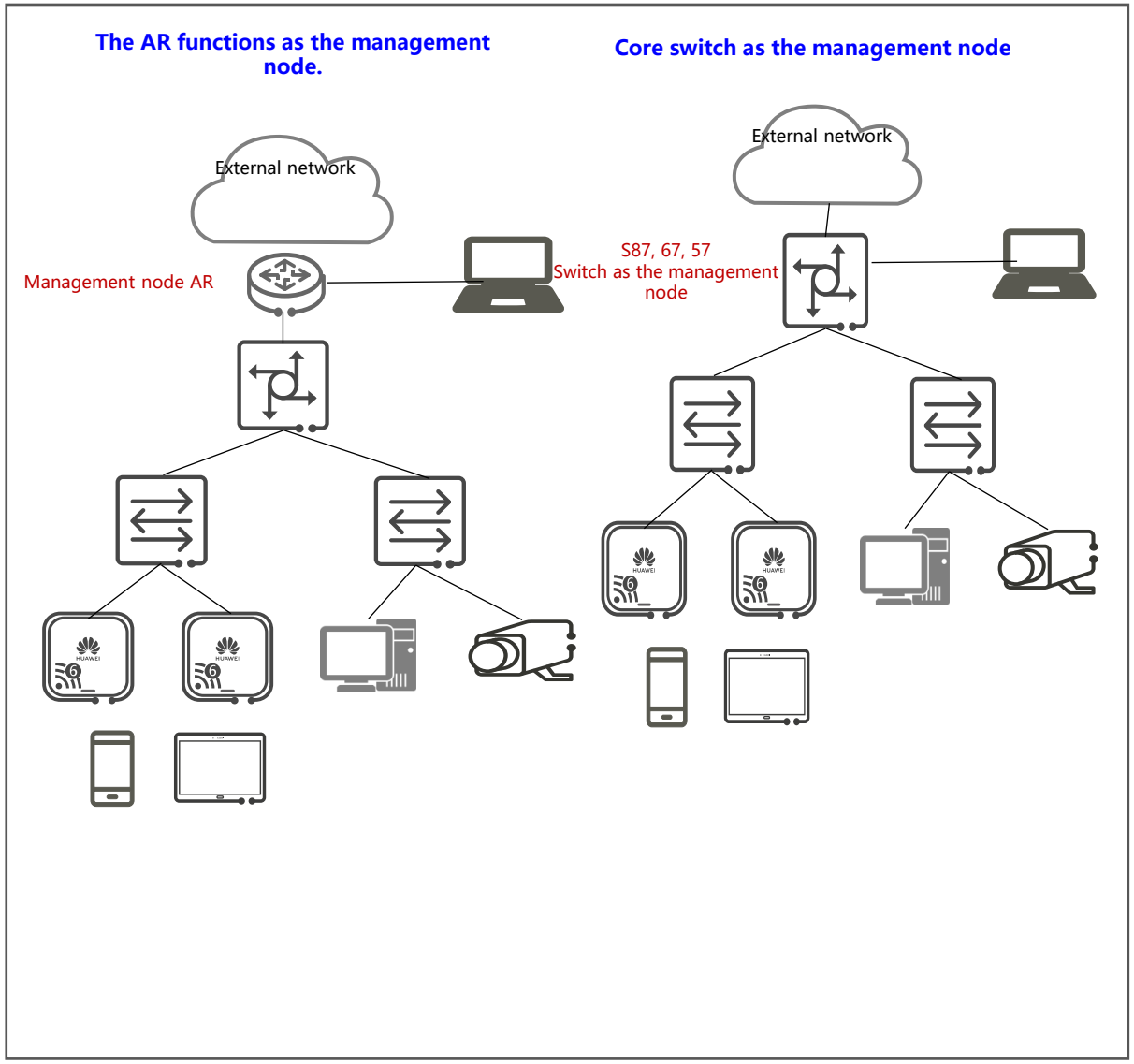
O&M assistant
Report analysis
Large-screen display

Standard integration

HTTP NBIs
FTP NBIs
SNMP NBIs

HUAWEI

One Webmaster device manages the entire network, batch configuration, and visualized O&M of the entire network.



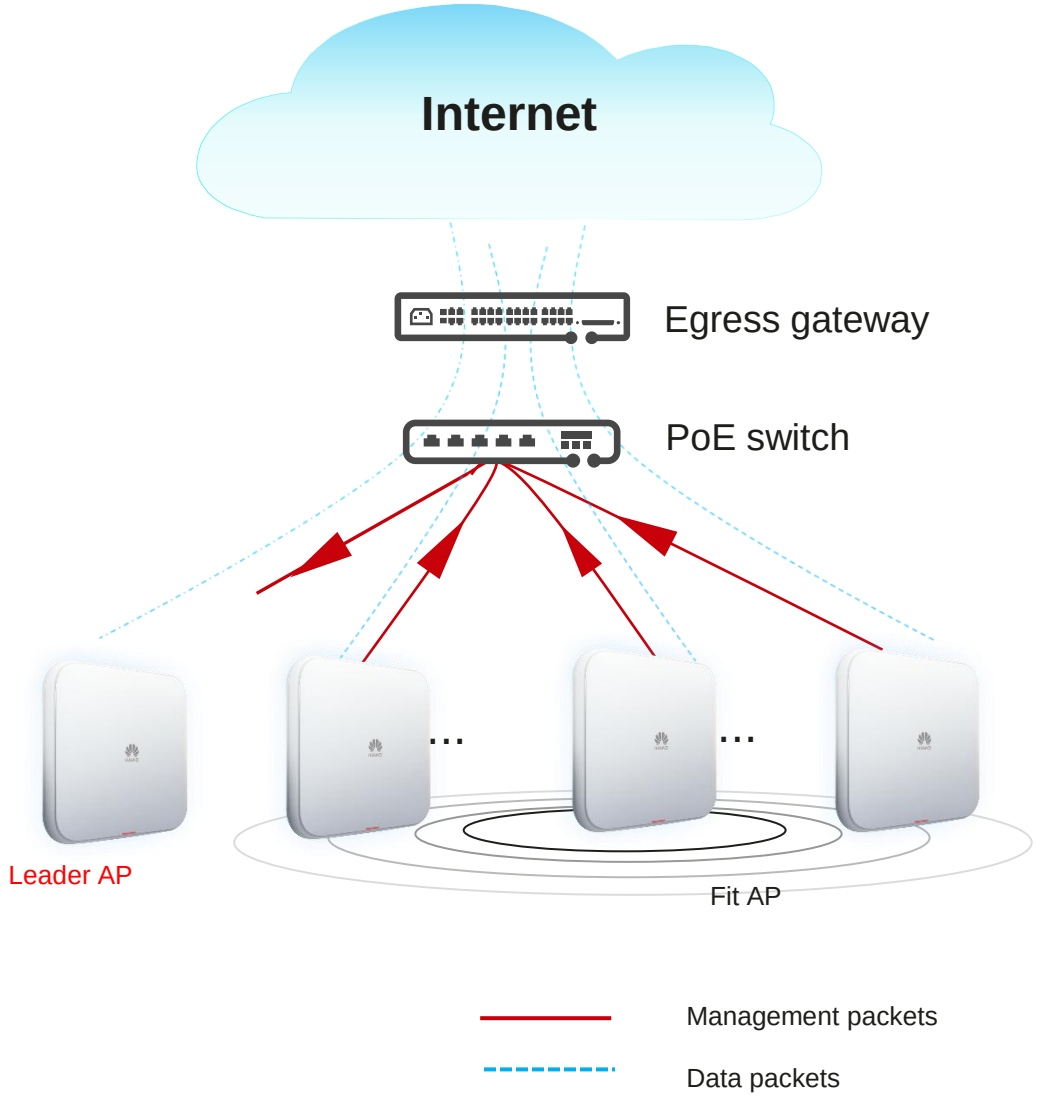
Solution: Manual configuration and O&M on devices one by one→ One device manages the entire network.

- **Customer benefits:**
  - **Zero-cost deployment: server-free and independent software;**
  - **Deployment efficiency improvement: Site visits are not required during deployment. Batch upgrade in minutes;**
  - **Manual maintenance: One-click device replacement;**
  - **One device manages the entire network: SME obtains the LAN-WAN self-management capability, which enables network visualization and improves O&M efficiency by X times.**

- **Huawei benefits:**
  - Enable integrators to deploy sites and improve O&M efficiency by 50%, solving O&M usability weaknesses in the commercial market.

-R24C00	R24C10	
① Single-node web system	① Self-discovery: Device self-discovery ② Visualization: automatic topology collection and web page display ③ Simplified deployment: batch configuration delivery, wired and wireless service provisioning, and zero-configuration replacement of faulty devices ④ Intelligent O&M: one-click network-wide upgrade and alarm reporting for loops caused by incorrect connections	

Leader AP – wbudowany w AP prosty kontroler typu instant



- The leader AP integrates some functions of a WAC and manages Fit APs in small and midsize branches and stores, implementing access services without WACs or licenses and thereby saving investment
- Supports PSK, local Portal, 802.1X, and MAC address authentication modes.
- Supports smart radio calibration and Layer 2 roaming.
- Supports the web system.
- *The leader AP does not support cloud management and therefore cannot interconnect with iMaster NCE or CampusInsight.*
- Leader AP specifications:

Model	Maximum Number of Managed Fit APs	Maximum Number of Managed Users
AirEngine 8760 series	48	1024
AirEngine 6760/6761/5760 and 5761 series	32	512
AirEngine 5762 series	16	256

Content

Campusowe Systemy NMS

iMaster NCE Campus

iMaster eSight

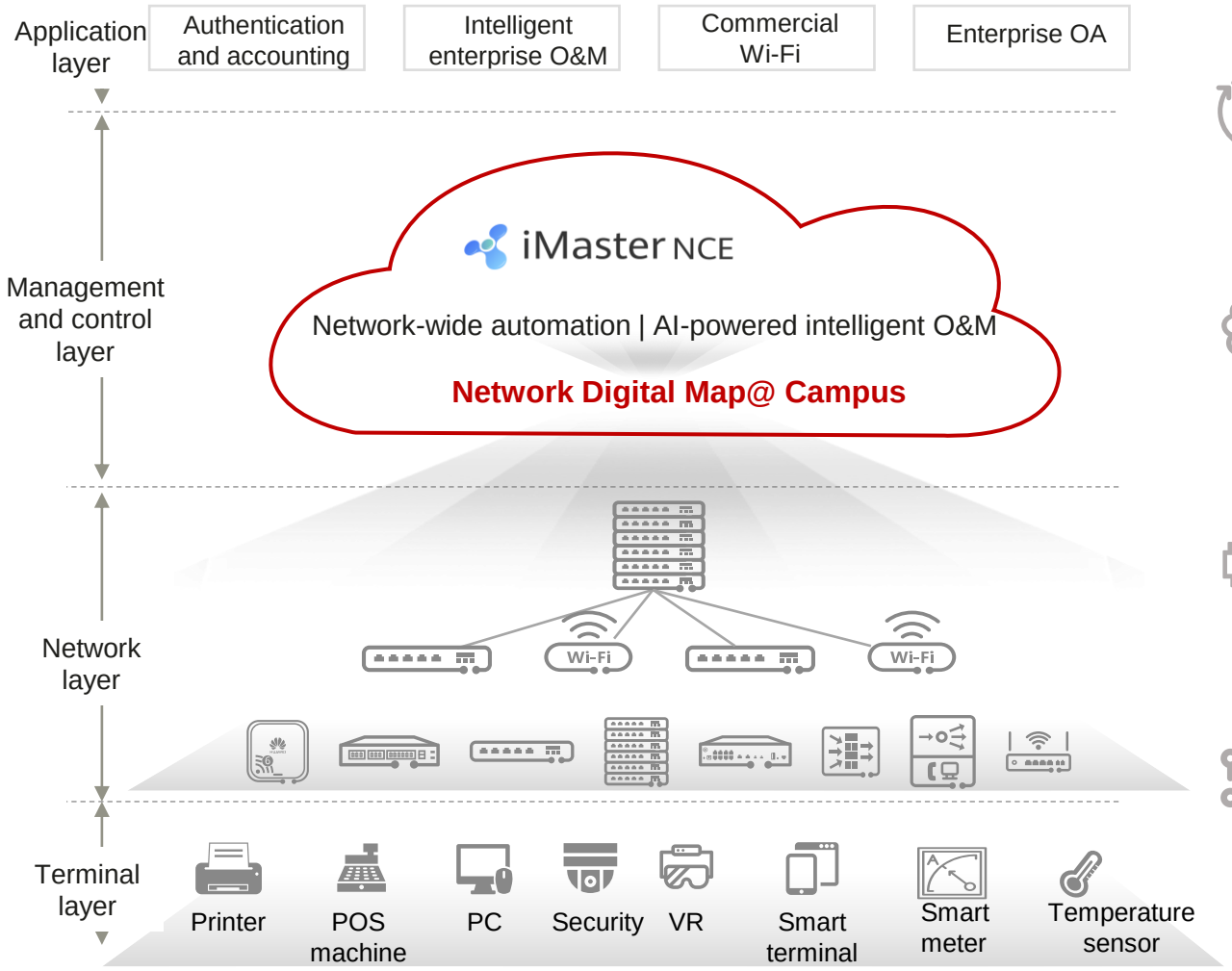
iMaster NeoSight

Podsumowanie + Q&A

EXCLUSIVE NETWORKS

HUAWEI

iMaster NCE-Campus Enables Industry's 1st L3.5 Autonomous Driving Network for Campuses



Zero-wait network: high skill-reliant → automatic management

Full-lifecycle intelligent management (covering network planning, construction, maintenance, and optimization)

Zero-risk terminals: manual management → automatic control

Seamless terminal access, consistent policies

Zero-interruption applications: passive response → proactive assurance

Application visibility, assurance, and fault demarcation

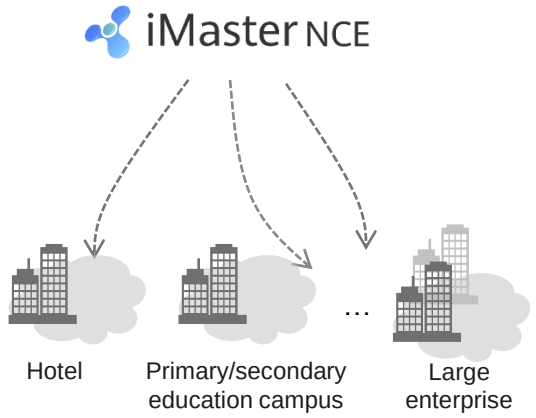
Converged base: a unified converged management platform

- Converged system: Management + authentication + analysis + security
- Converged authentication: 5G terminal + Wi-Fi
- Converged management: LAN + WAN
- Converged deployment: On-premises + MSP-owned cloud + Huawei public cloud

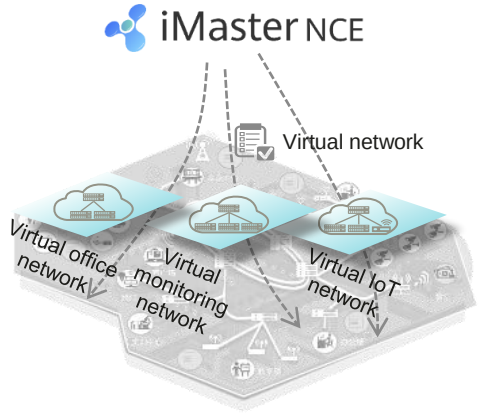
HUAWEI

All-Scenario: Full Coverage from Single Campuses to WAN Interconnection Campuses

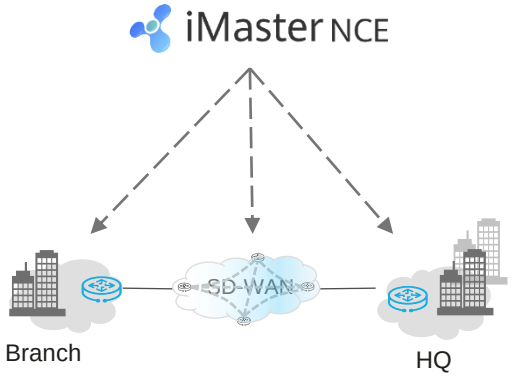
Simple-service campus



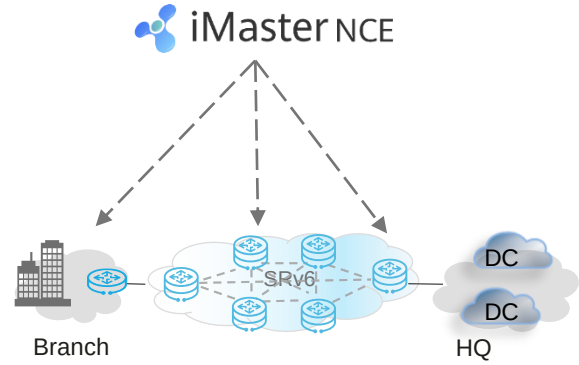
Multi-service campus



Multi-branch interconnection campus

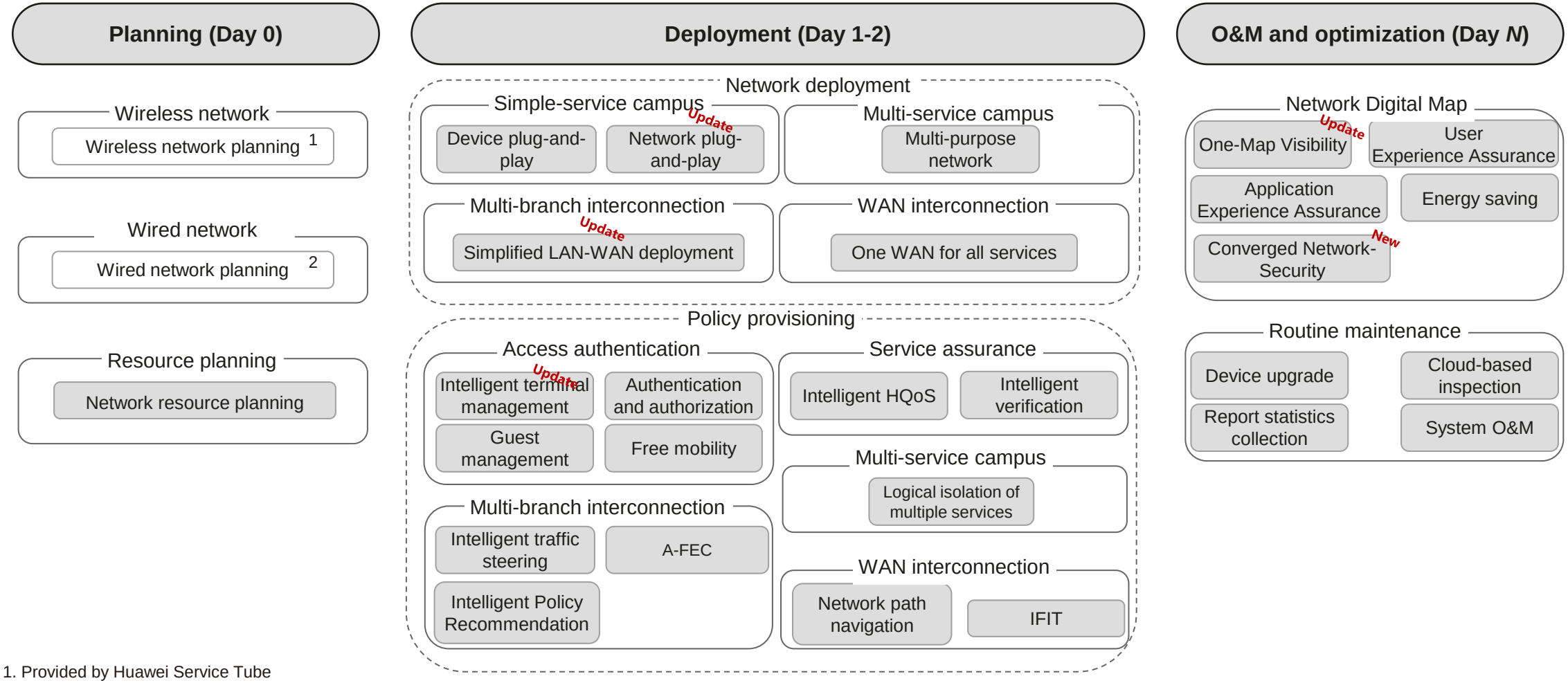


WAN interconnection campus



	Simple-Service Campus	Multi-Service Campus	Multi-Branch Interconnection Campus	WAN Interconnection Campus
Network structure	Mainly single campuses, providing network access and connectivity	Complex network structures, covering multiple areas including multiple buildings and providing multiple services	Wired and wireless networks for Internet access at headquarters and branches Available VPNs between headquarters and branches	Wired and wireless networks for Internet access at headquarters and branches Headquarters and branches are connected through a backbone network.
General requirement	Management and authentication of multiple network devices, such as APs, ONTs, OLTs, switches, and firewalls	Management and authentication of multiple network devices, such as APs, switches, and firewalls as well as multi-service isolation	Management and authentication of multiple network devices, such as APs, switches, firewalls, and ARs, as well as multi-branch interconnection network management	Management and authentication of multiple network devices, such as APs, switches, AR routers, and NE routers as well as backbone network management
Typical scenario	Multi-branch and small-sized enterprise campuses, such as hotels and primary/secondary education campuses	Campuses for higher education institutions, governments, and large enterprises	Large enterprises and financial service outlets	Finance

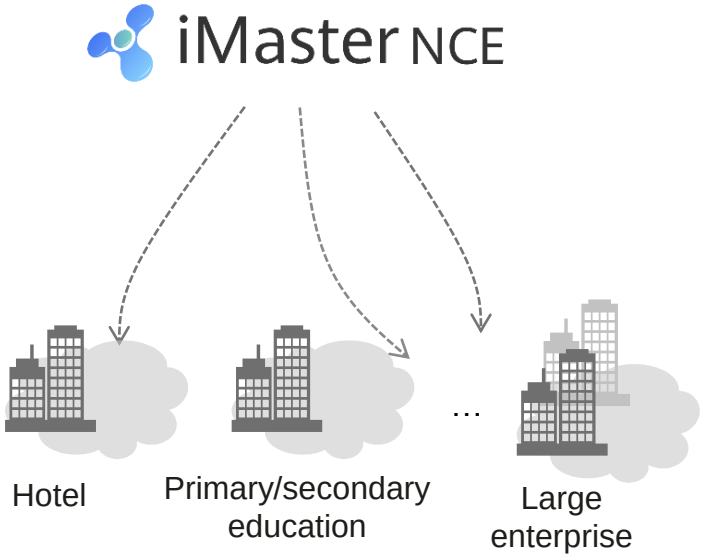
Full-Lifecycle Network Management: Campus Network Management Panorama



1. Provided by Huawei Service Tube
2. Provided manually or by eDesigner
3. Provided by iMaster NCE-CampusInsight (SSO)

Contents

iMaster NCE-Campus: Simple-Service Campus Network Automation Solution



- **Automatic physical network deployment**

iMaster NCE-Campus is used for quick network deployment, implementing device PnP.

- **Automatic service policy provisioning**

Implement instant policy deployment and global policy validation via configuration delivery through the iMaster NCE-Campus GUI (configurations to be delivered: user access authentication policy, guest management, free mobility, HQoS, and terminal identification)

>>

20 minutes

- Device onboarding in 20 minutes
- 0.5 days required for provisioning a branch and completing service commissioning

4 steps

- Simplified small campus deployment
- Large campus network configured and deployed in just 4 steps

6 dimensions

6 dimensional refined permission control according to "5W1H"

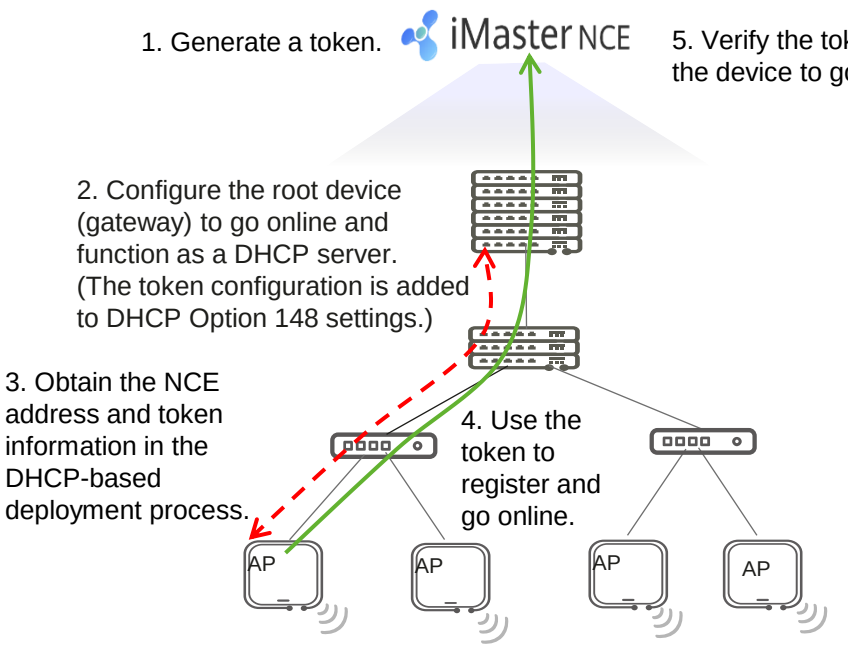
HUAWEI

ESN-Free Deployment : Configuration Planning in Advance and Network Plug-and-Play

Updated in R24C00

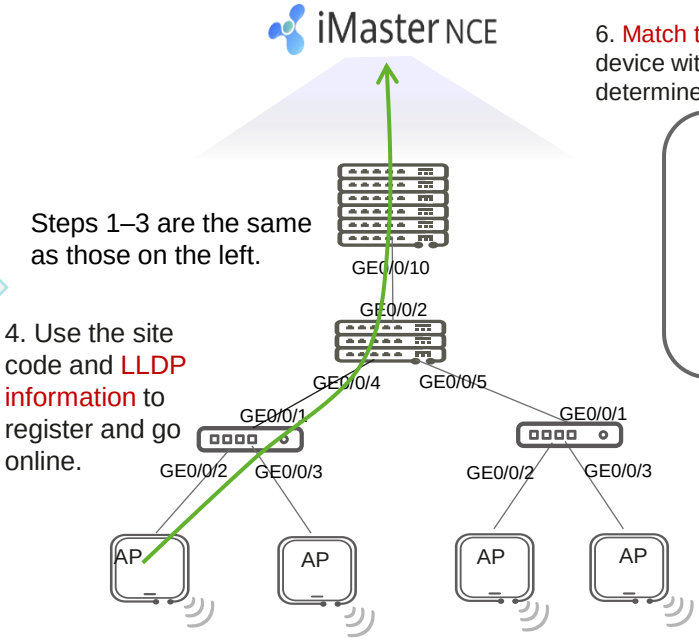
Scenario | A large number of devices at branch sites need to be connected to the network. When devices go online, they automatically match planned devices, without requiring the administrator to enter ESNs. Besides, device configurations can be delivered offline, improving deployment efficiency.

ESN-free deployment (based on DHCP)



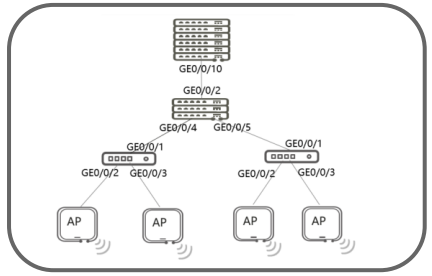
New deployment mode

ESN-free deployment (based on DHCP & LLDP)



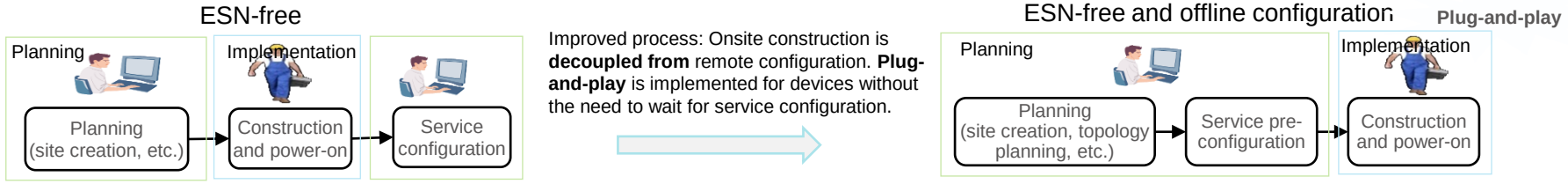
5. Verify the token.

6. Match the LLDP link information reported by the device with the planned link information to determine the device location in the topology.

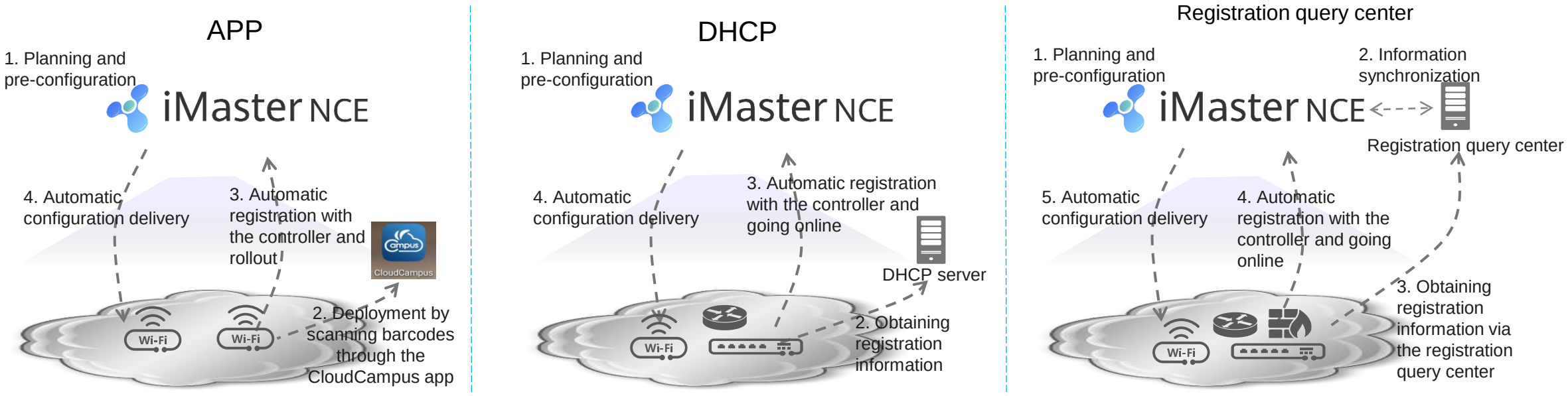


* If no match is found, an alarm is generated and the device cannot go online.

Improvement: After being powered on, a device can automatically match the planned topology location and supports offline configuration.



IP Device Plug-and-Play: ZTP-based Simplified Deployment

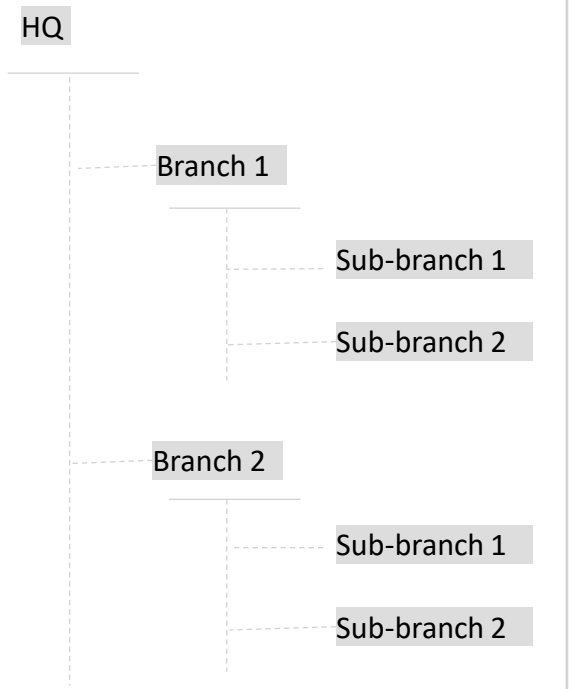


Deployment Mode	Applicable Device	Whether iMaster NCE-Campus Connects to the Internet	Application Scenario
App	AP	Required	Simple network (APs mainly)
DHCP	AP, switch, and AR	Not required	Network planning and management. Network management personnel have the capability of managing and configuring a DHCP server.
Registration query center	AP, firewall, switch, and AR	Required	MSP-owned clouds and HUAWEI CLOUD

Hierarchical Template: Inheriting and Delivering Configurations to Massive Branches in Batches

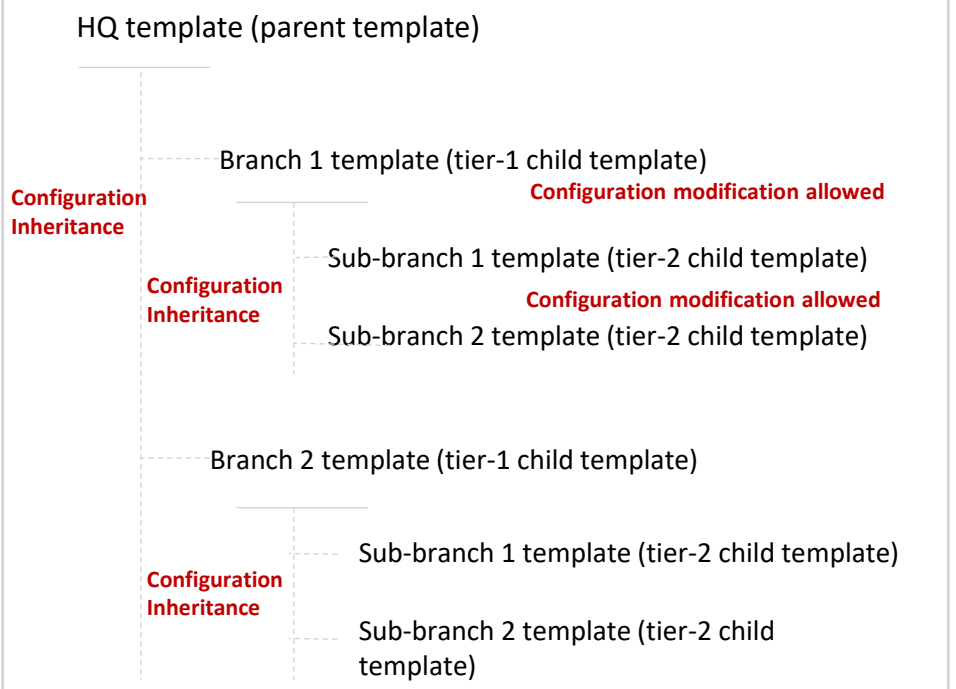
Scenario | In multi-branch scenarios, branch configurations are similar and even the same. If a configuration is changed, multiple repetitive operations need to be performed. This is inefficient and error-prone, often causing rework.

As Is: typical organizational structure



>>

Hierarchical template-based configuration



Time required for configuring a single branch

One week saved for 100 branches

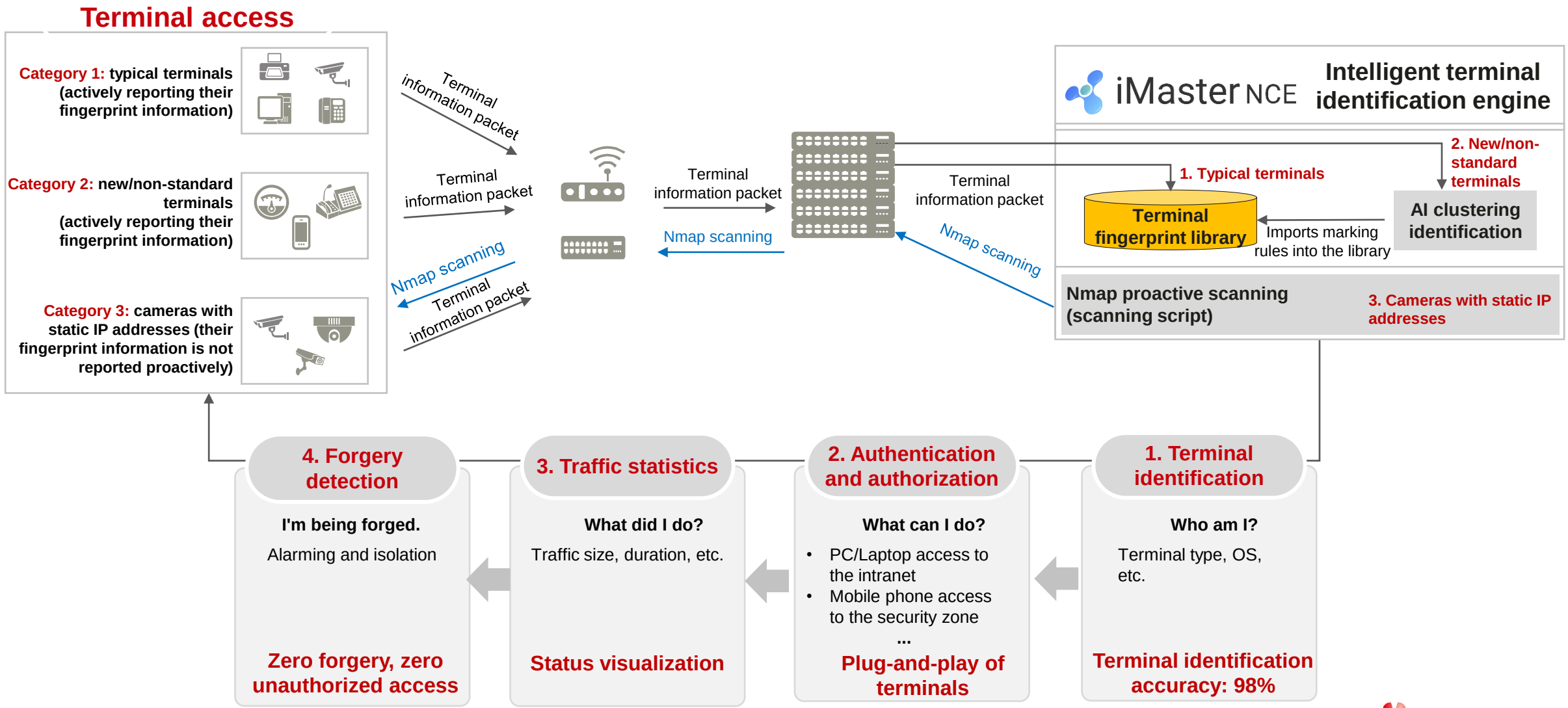
Lower rework rate
(after configuration change and batch configuration delivery)

15%

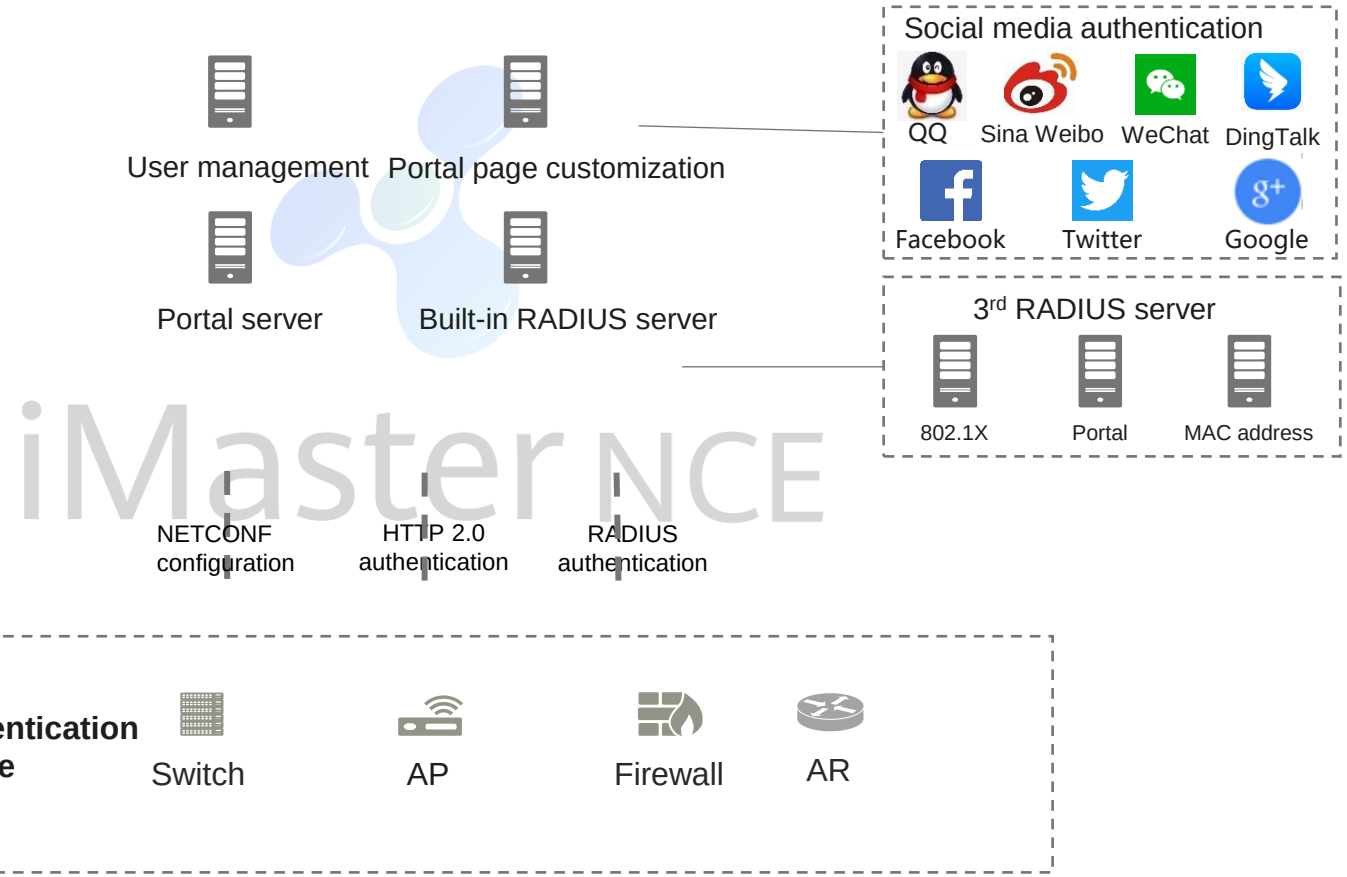
***Constraints**: The LSW of V200 and other V600 devices are supported.*

HUAWEI

Huawei Intelligent Terminal Management Solution:
Plug-and-Play of Terminals, Zero Forgery, and Zero Unauthorized Access



User Access Authentication



Authentication Method

- Portal authentication: user name and password, anonymous, SMS, QQ, Sina Weibo, WeChat, Ding Talk, Facebook, Twitter, Google and passcode authentication
- PPSK authentication
- MAC address authentication
- 802.1X authentication (built-in RADIUS server)
- 802.1X authentication (interconnection with an external RADIUS server)

Transmission Protocol

- Authentication data transmitted through HTTP2.0 and RADIUS
- Configuration data transmitted through NETCONF

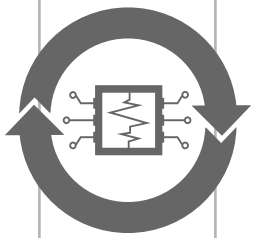
Open-System Authentication

- Interconnection with a third-party Portal server
- Interconnection with social media such as QQ, Sina Weibo, WeChat, Ding Talk, Facebook, Twitter, Google

Intelligent Policy Engine, Achieving Refined Permission Control

Condition: 5W1H

User/user group/role	**User identity** **Who**
Site, region, device group, device type, device, SSID, and IP address	**Access location** **Where**
By week/time point	**Access time** **When**
PC/iOS/Android	**Terminal type** **What**
Company-provided/BYOD terminal	**Device attribute** **Whose**
Wired/Wireless Portal, MAC address, and 802.1X authentication	**Access mode** **How**

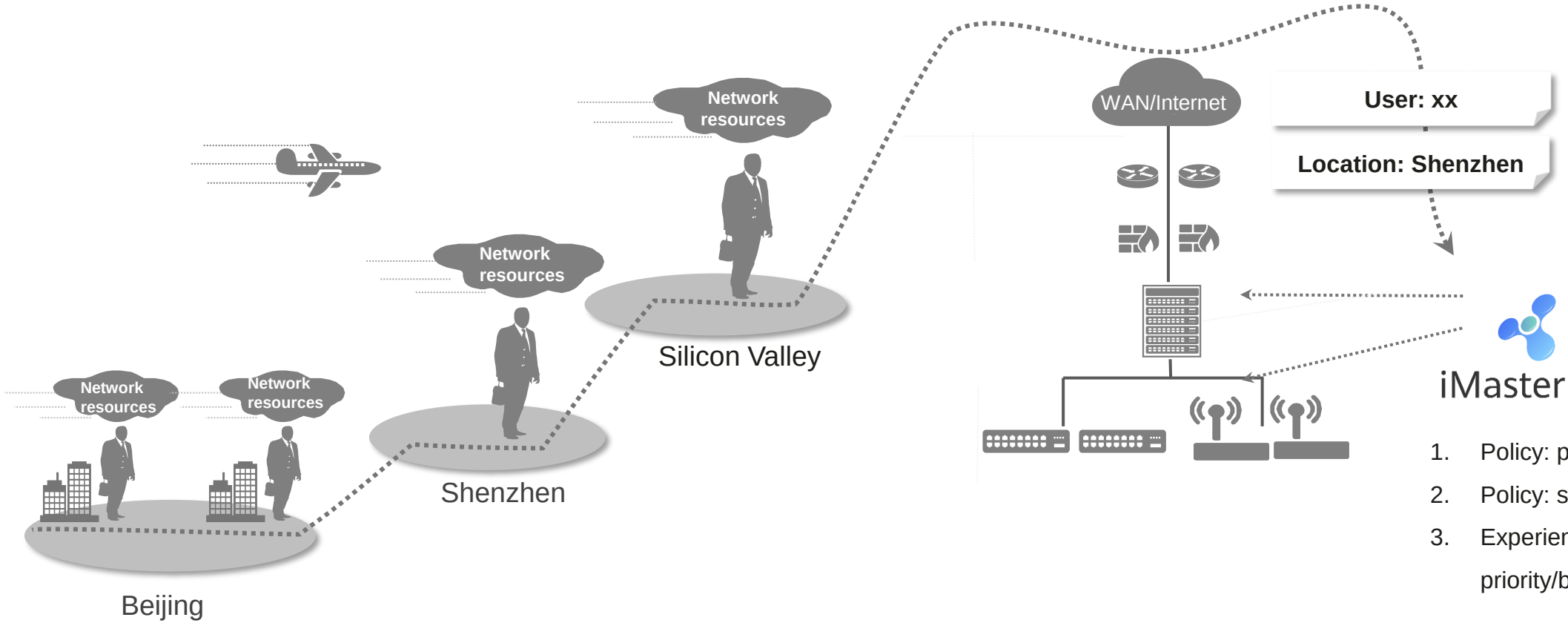


Intelligent policy engine

Result: Fine-grained permission control

Permission	VLAN/ACL/security group, VIP user...
Bandwidth	Uplink/Downlink bandwidth, DSCP
QoS	High/Medium/Low Traffic and online duration control (supported only in Portal authentication mode)
Application	Application group/application
Security	URL filtering

Free Mobility: Policies Following Users, Ensuring Consistent Experience



1. Policy: permission
2. Policy: security
3. Experience: priority/bandwidth

Users can access the network anytime, anywhere, ensuring consistent service policies and network experience for users.

Intelligent HQoS: User-/Application-Based QoS Policy

Requirements & Challenges

QoS policies are not enough in video service scenarios

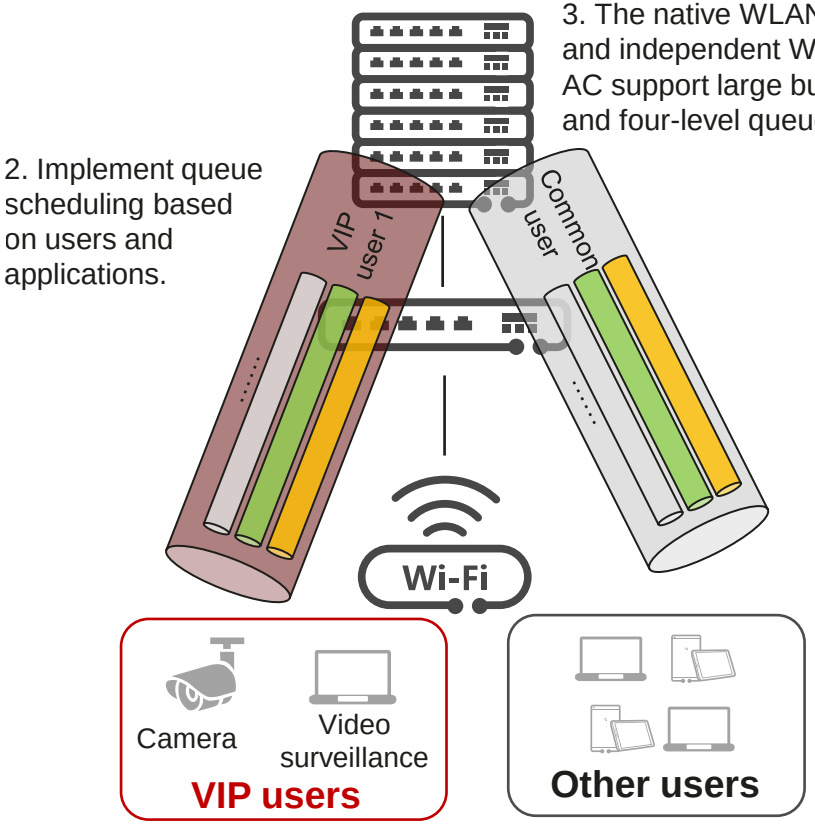
(Example) Building surveillance scenario:
As wireless video services increase, a large number of network resources are occupied, causing downlink congestion in some scenarios.

>>

User-/Application-based QoS policy: ensures experience of key users and applications

iMaster NCE

1. Define VIP users.
   Define the application priority.



S12700E: 40*25GE card, 4 GB buffer
AirEngine 9700-M: 512 MB buffer

Restrictions:
- The wireless network requires the tunnel forwarding mode.
- S12700E: Only the card providing 40 x 25GE ports supports HQoS; S5731/32-H: supporting 25G uplink ports
- It is recommended that the proportion of VIP users be less than or equal to 10%.
- The application scheduling template is configured on the WLAN AC through the web system.

Specifications:
- The S12700E supports 16K VIP users per card. The AirEngine 9700-M supports 1800 users per board.
- iMaster NCE-Campus supports up to 31 application scheduling templates.

Huawei Intelligent Verification Solution: Service Rollout and Changes with Zero Errors

① *Minute-level* test verification

Hours → **Minutes**

② *Comprehensive* connectivity verification

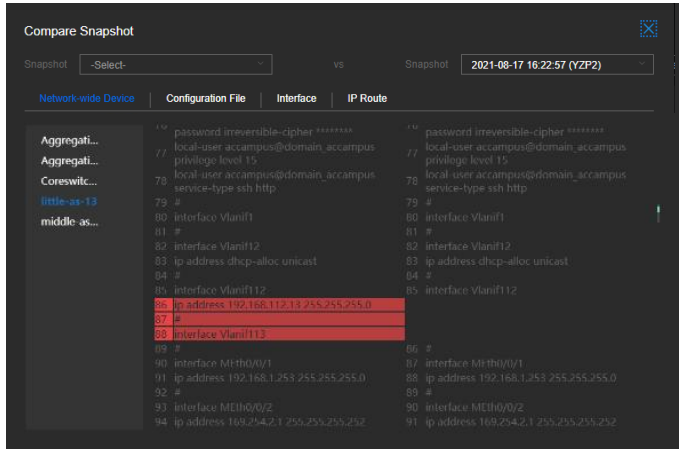
Inadequate testing → **All-inclusive testing**

③ *Accurate* test results

Inaccurate results → **Accurate and trustworthy results**

Snapshot comparison

Compares snapshots to quickly identify inconsistency in devices, configuration files, interface link status, and IP routes.

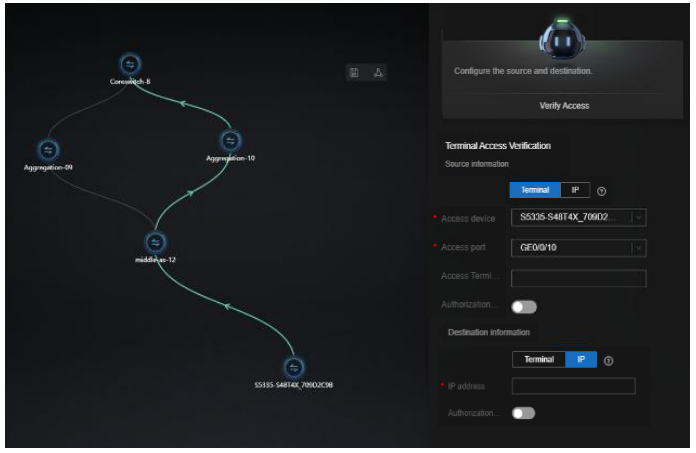


Subnet reachability verification

Clearly displays the connectivity between all service subnets on the entire network

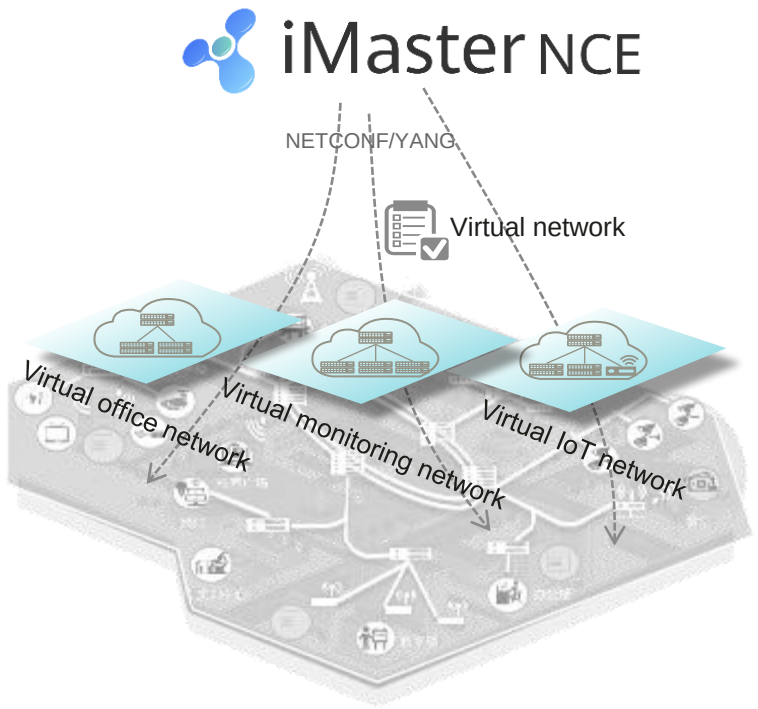
Terminal access verification

100% digital modeling of the network environment and real-time, precise simulation to verify terminal access permissions, ensuring a secure, reliable network



Contents

iMaster NCE-Campus: Multi-Service Campus Automation Solution



- **Automatic physical network deployment**

Physical networks are automatically deployed through simplified site deployment and PnP LANs.

- **Automatic virtual network provisioning**

Virtual networks are software-defined and are automatically provisioned through iMaster-NCE-Campus and web page-based centralized deployment.

- **Automatic service policy provisioning**

Service policies are software-defined and are automatically provisioned through iMaster NCE-Campus and free mobility.

>>

1 network

One network for multi-purpose: Multiple services are transmitted on one physical network and are logically isolated, saving costs.

3 steps

Network configured and deployed in just 3 steps

5 minutes

Fast network adjustment within just 5 minutes, achieving higher efficiency

HUAWEI

Contents

Application Scenarios of iMaster NCE-Campus

-- Automated Network Planning

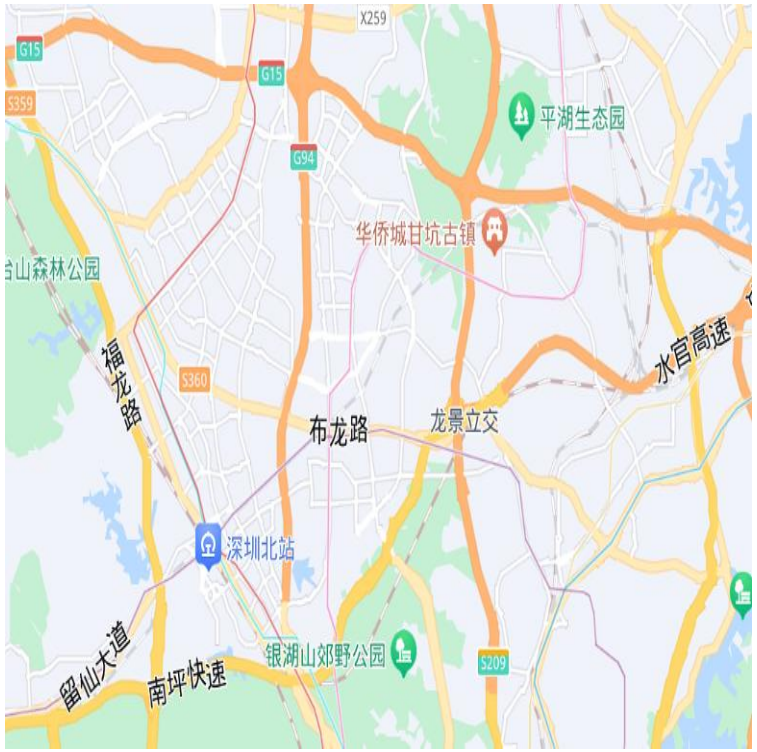
-- Automated Network Deployment

-- Intelligent Network O&M and Optimization

Campus Network Digital Map: Digital Foundation for Campus Networks, Ensuring Ultimate Campus Service Experience

Similar to the traffic map, the network digital map is a digital twin of the physical network world. It offers high visibility and interaction, and is ideal for building a digital intelligent management platform.

Traffic map



Holographic visibility

Road traffic map Personnel heat map Real-time satellite map	⟷	Application view User view Network view

Fault locating

Traffic congestion relief	⟷	Conference lag locating

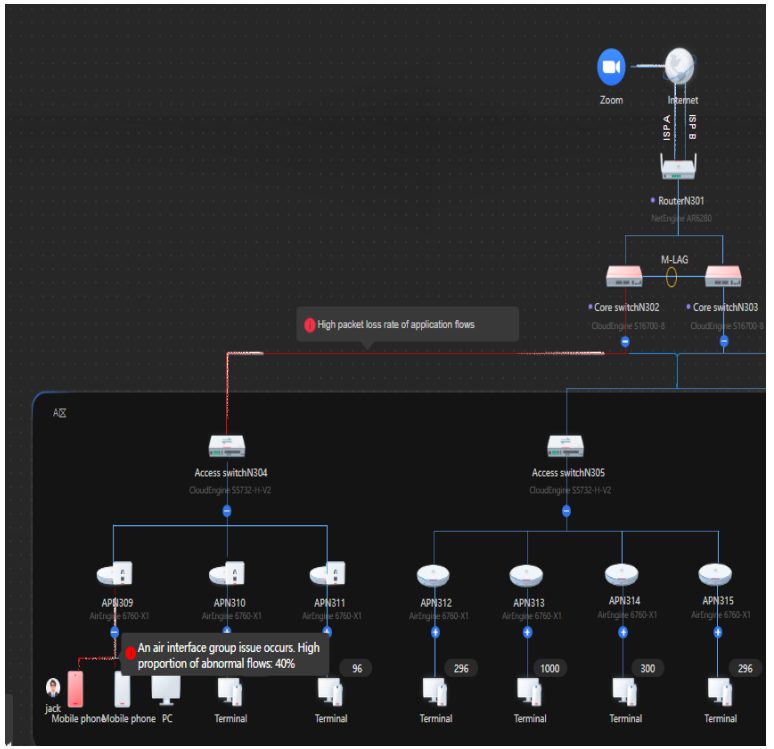
Key assurance

Bus lane Preferential pass of special vehicles	⟷	Key conference assurance VIP user assurance

Service expansion

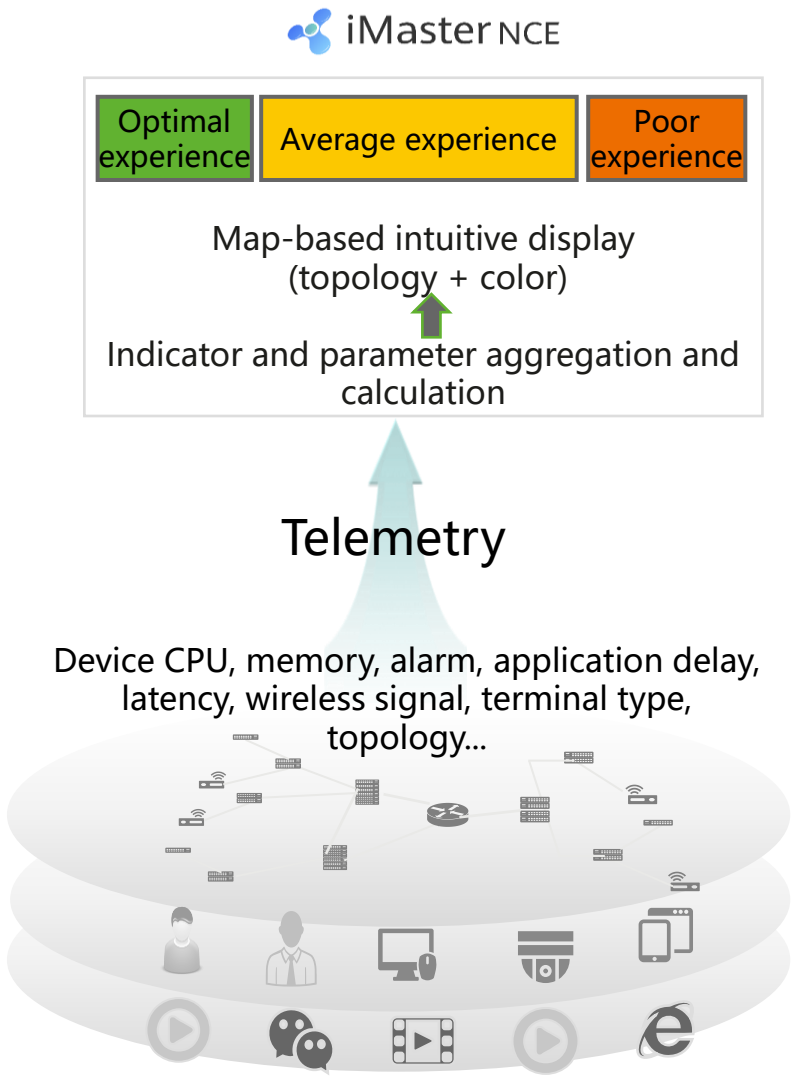
Ride-hailing and takeout	⟷	Asset locating Energy saving

Network digital map



The network digital map is experience-centric, improving O&M efficiency and ensuring ultimate campus network experience.

Telemetry, Meeting Real-Time Analysis Requirements



Map-based display, color-based display, and intuitive experience awareness

The comprehensive experience score is calculated based on the weighted calculation of related parameters of users and applications.

Collect network data in seconds based on Telemetry.

More indicators are reported, including multiple performance indicators of users, terminals, and applications.

Experience modeling

Network indicators: latency, speed, and signal strength
Application indicators: packet loss and latency of data flows
Terminal parameters: dual-band or not

→ User experience score

Device alarm information → Device status

Packet loss and latency of application flows → Application status

→ Site status

Link latency and packet loss → WAN link

* The flows whose packet loss rate is greater than 20% are marked as abnormal flows. The flows whose percentage of abnormal flows exceeds 20% are marked as abnormal applications.

One-Click Optimization: One-Click Experience Assurance for Key Services

Key conferences and VIP users raise requirements for experience assurance. However, the assurance efficiency of network O&M personnel is low. With the sharp increase of audio and video traffic, rapid experience assurance gradually becomes a must.

As-Is: Difficult experience assurance

Service department

Key service assurance requirements

Time-consuming and labor-consuming, unable to perform experience assurance in a timely manner

Network department

Develop strategies (depending on experts).

Output configurations (complex configurations).

...

Deliver configurations (to a large number of devices).

Complex configuration

The conventional configuration procedure is complex and involves a large number of parameters. Devices are configured one by one, making it difficult to respond to service requirements in a timely manner.

Expert-dependent

Network configuration depends on expert experience, resulting in high labor costs.

To-Be: One-click experience assurance

Easy to interact

One-click service assurance settings via the large-screen entry on the digital map, easy to interact

Configuration automation

iMaster NCE automatically generates and delivers configurations in batches based on service intents.

Service assurance → One-click assurance → Take effect in time.

Automatically generated

Network settings
...
Network configuration *n*

Deliver

Network device A
...
Network device Z

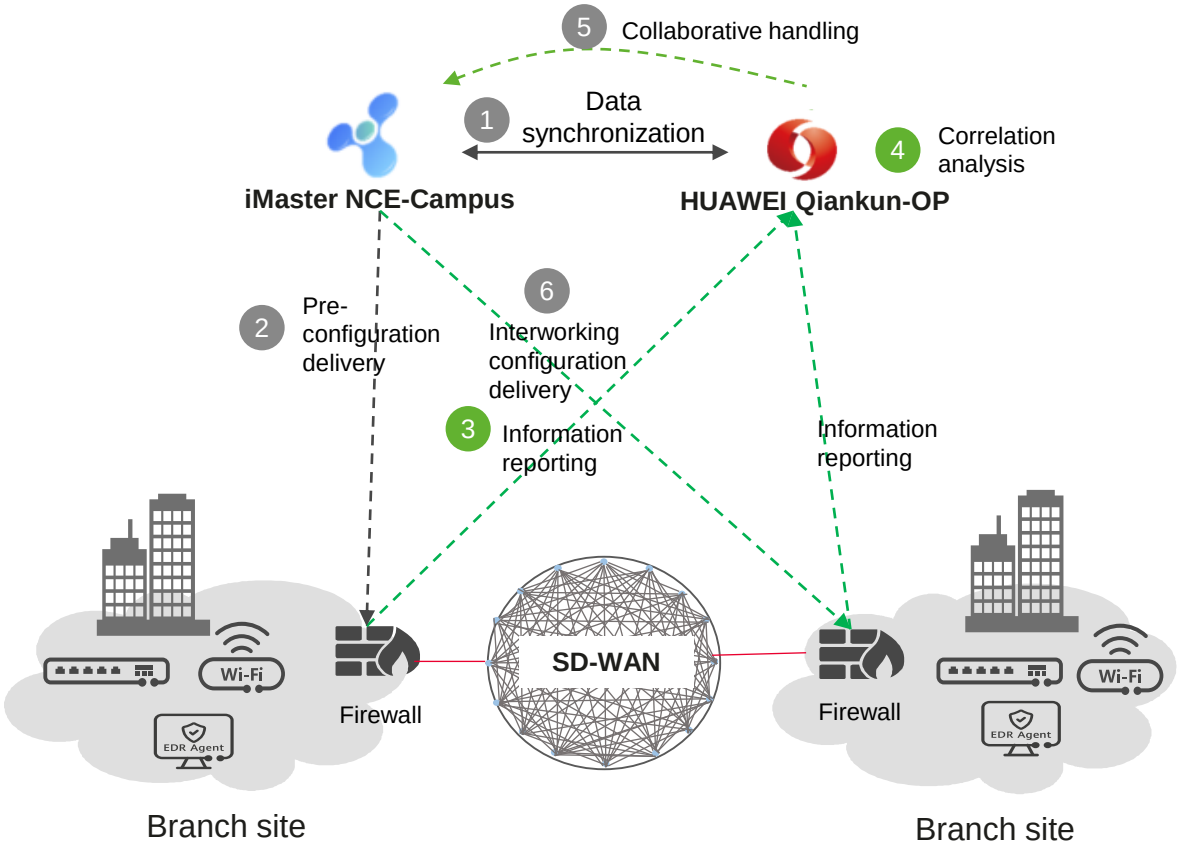
VIP user assurance

Application assurance

Network-Security Converged Management: Unified Network and Security Platform, Delivering a Unified O&M Experience

New in R24C00

Ransomware attacks have become top threats in the industry, and security protection is a rigid demand for customer services. Traditional network management and security analysis require multiple platforms and portals, resulting in high O&M costs and poor user experience.



Fully converged GUI

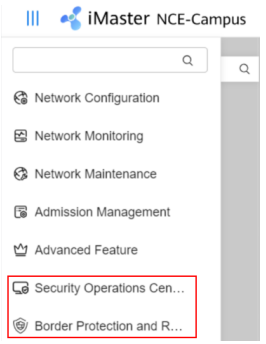
iMaster NCE-Campus provides a unified portal and model to improve unified network and security operations experience. A unified configuration portal is available for collaborative configuration on HUAWEI Qiankun-OP and iMaster NCE-Campus.

Capability focus

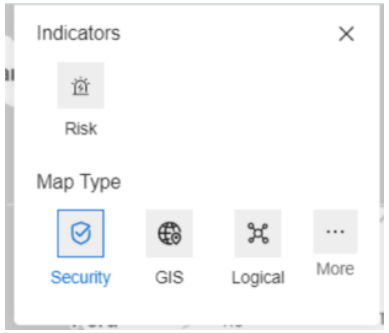
HUAWEI Qiankun-OP: security event correlation analysis, similar to a **security analyzer**

iMaster NCE-Campus: configuration and policy delivery, similar to a **security policy controller**

Constraints: HUAWEI Qiankun-OP and iMaster NCE-Campus need to be deployed and interconnected with each other.



Security menu



Security view

HUAWEI

Routine Maintenance: Full-Process Assurance

Device Upgrade

Remote device upgrade, customized upgrade policies, and visualized, automated upgrade: minimize the adverse impact on upgrades caused by manual operations.

>>

Cloud-based PMI

Cloud-based PMI provides online in-depth health monitoring over network-wide devices, obtaining network status in real time and ensuring healthy network operations.

>>

Report Statistics

Reports can be customized on demand to display site traffic statistics and terminal behavior analysis results.

>>

System O&M

System O&M is implemented through system monitoring, fault diagnosis, and backup and restoration, minimizing the adverse impact on the services caused by the system.

HUAWEI

Content

Campusowe Systemy NMS

iMaster NCE Campus

iMaster eSight

iMaster NeoSight

Podsumowanie + Q&A

HUAWEI

Technical Specifications of eSight Compact Edition

Type	Indicator	KPI in Compact Edition	Standard Specifications	Advanced Specifications	Unit
Management Specifications	Equivalent NEs	300	5000	20000	Number
User specifications	Maximum number of registered users	100	1000	1000	Number
	Maximum number of online users	10	100	100	Number
Alarm specifications	Maximum number of current alarms that can be stored	20000	50,000	100,000	Record
	Maximum number of historical alarms that can be stored	100,000	4 million	15 million	Record
	Continuous alarm processing capability	1	10	10	Record/s
	Alarm storm processing capability	10	100	100	Record/s
	Maximum interval between fault occurrence and fault display in the monitoring system	15	15	15	Second
Performance	Maximum number of collection units	20,000	1 million	2.6 million	Number
Northbound specification	Maximum number of interconnected northbound OSSs	2	10	10	Number

Appendix 2: Differences Between the Compact and Standard Editions

S-Part Number	S-Part Descpition	Service	Compact Edition	Standard Edition
88034GED	eSight Platform	Basic management service	√	√
88034GEE	eSight Network Management License -1 Device	Network device management service	√	√
88034GEW	eSight Network SLA Management License	Network SLA management service	×	√
88034GEH	eSight Network Traffic Analysis License -1 Device	Network traffic analysis service	×	√
88034GEF	eSight WLAN Management License -1 AP	WLAN management service	√	√
88034GEJ	eSight Video Surveillance Management License -1 Camera	Video surveillance management service	√	√
		Video analysis service	×	√
88034GEK	eSight Server Management License -1 Device	Server management service	√	√
88034GES	eSight Storage Management License -1 Device	Storage device management service	√	√
88034LNM	eSight Microwave Management License -1 Device	Microwave device management service	×	√
88034GEL	eSight PON Management License -1 ONU	PON device management service	√	√
88037DFD	eSight PON Management License -1 ORE	PON device management service	√	√
88034GEN	eSight Virtualization Management License -1 CPU	Virtual resource management service	×	√
88034GEM	eSight APP Management License -1 Instance	Application management service	×	√
88037XYT	eSight HCI Management License-1 CPU	Hyper-converged infrastructure management service	√	√

Understanding iMaster NeoSight and eSight

eSight provides device monitoring, report, and routine maintenance capabilities for ICT infrastructure. It has advantages in a wider management scope, including basic O&M of datacom, optical, server, and storage devices. Monitors alarms, performance, and topology. Report analysis and large-screen display; Network quality diagnosis.

The iMaster NeoSight inherits the eSight capabilities and adds features such as all-domain topology, workbench, terminal management, and fault analysis.

	Comparison Item	eSight	NeoSight
Management scope	Network device, WLAN management, PON device, server, storage, camera, virtual resource, container resource management, hyper-converged, microwave, converged perception engine, operating system, database, and application management	√	√
Common Foundation	Terminal management	×	√
	Domain-wide topology	×	√
	Workbench	×	√
	Fault analysis	×	√
	Performance management	√	√
	Portal	√	√
	Report	√	√
	Large screen management	√	√
	IP address management	√	√
	Service life management	√	√
	Alarm management	√	√
	Link management	√	√
	Power-on and Power-off Management	√	√
	Device upgrade	√	√
	Physical topology	√	√
	eIBMS Asset Management	√	√
	Managing Customized Alarms	√	√
	Automatic discovery	√	√
	Digital Site	√	√
Network Value-Added Features	Network Traffic Analysis	√	√
	Network Profile Management	√	√
	SLA management	√	√
Open integration	Northbound interface	√	√
	Remote notification	√	√
	Certificate Management	√	√

HUAWEI

Can the eSight license be changed to NeoSight?

Answer: Yes. Before the annual fee expires, you can directly change the license of eSight to NeoSight on the ESDP.

NeoSight Deployment Specifications and Configuration Requirements

Answer: The eSight server can be reused.

Deployment Scenario	Physical Machine Configuration Requirements	VM Configuration Requirements	Management Specifications
Simplified version	CPU: 10-core 2.2 GHz or higher Memory: 32 GB Hard disk: 512 GB SSD Network port: 1G Ethernet port > = 1	CPU:12 vCPU Memory: 32 GB Hard disk: 512 GB SSD	Equivalent NE: 0 to 300
Standard configuration	CPU: 12 cores and 2 GHz or higher Memory: 64 GB Hard disk space: 1 TB	CPU:24 vCPU Memory: 64 GB Hard disk space: 1 TB	Equivalent NEs: 0 to 5000
High configuration	CPU: 40 cores and 2 GHz or higher Memory: 128 GB Hard disk space: 1.5 TB	/	Equivalent NE: 0-20000

Content

Campusowe Systemy NMS

iMaster NCE Campus

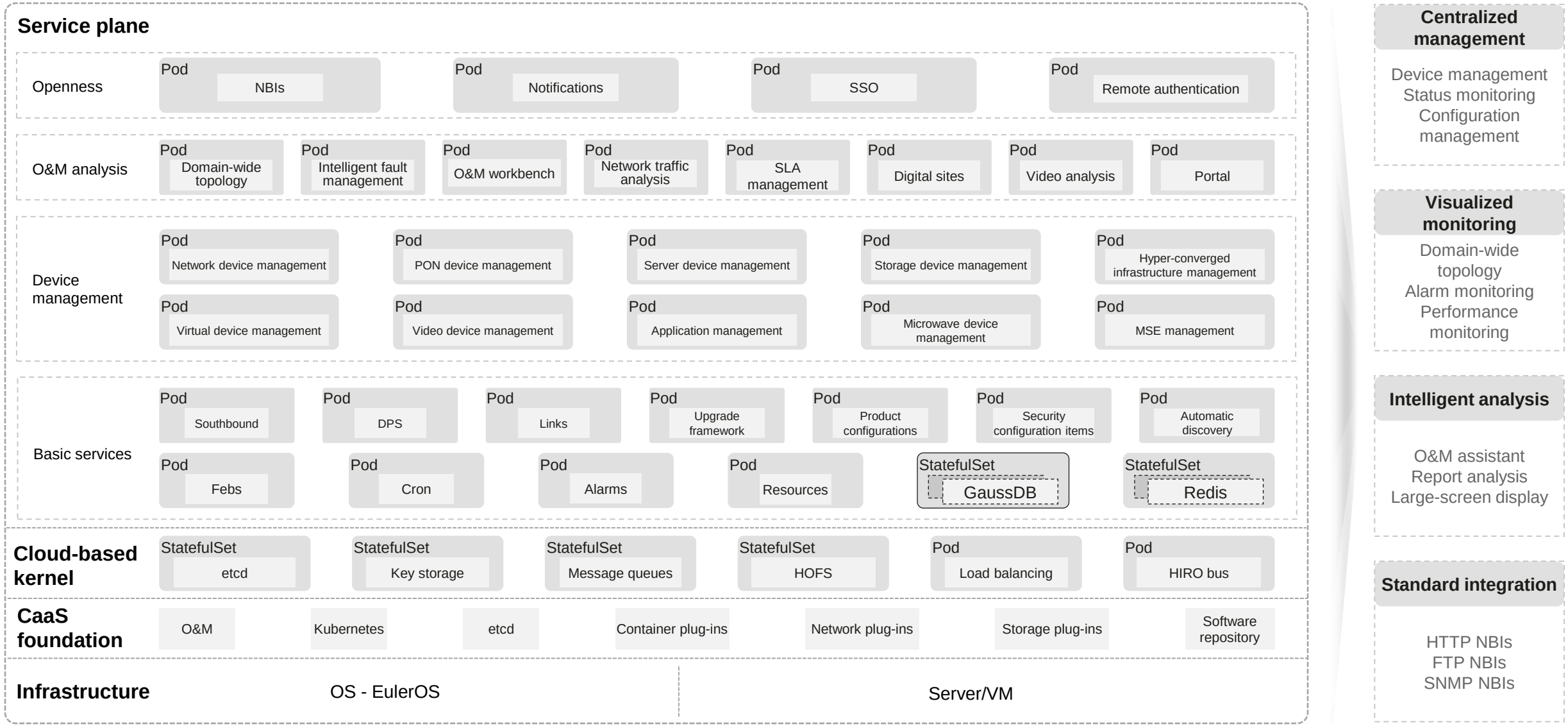
iMaster eSight

iMaster NeoSight

Podsumowanie + Q&A

HUAWEI

NeoSight's Container-based Architecture Enables Converged, Intelligent, Simplified, Open, and Centralized ICT O&M Products



Centralized management

Device management
Status monitoring
Configuration management

Visualized monitoring

Domain-wide topology
Alarm monitoring
Performance monitoring

Intelligent analysis

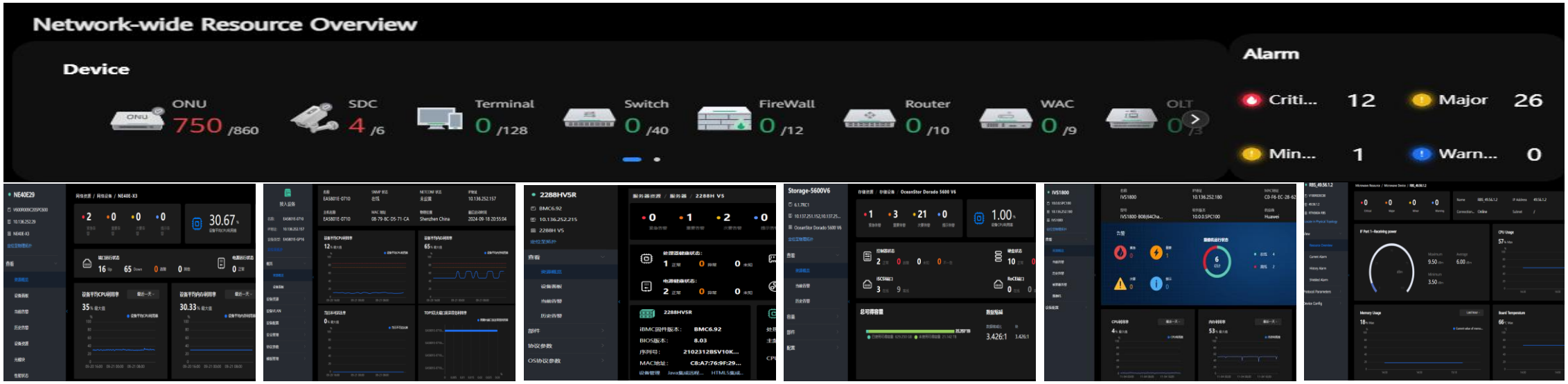
O&M assistant
Report analysis
Large-screen display

Standard integration

HTTP NBIs
FTP NBIs
SNMP NBIs

HUAWEI

Centralized Management of Cross-Industry Devices Reduces O&M costs



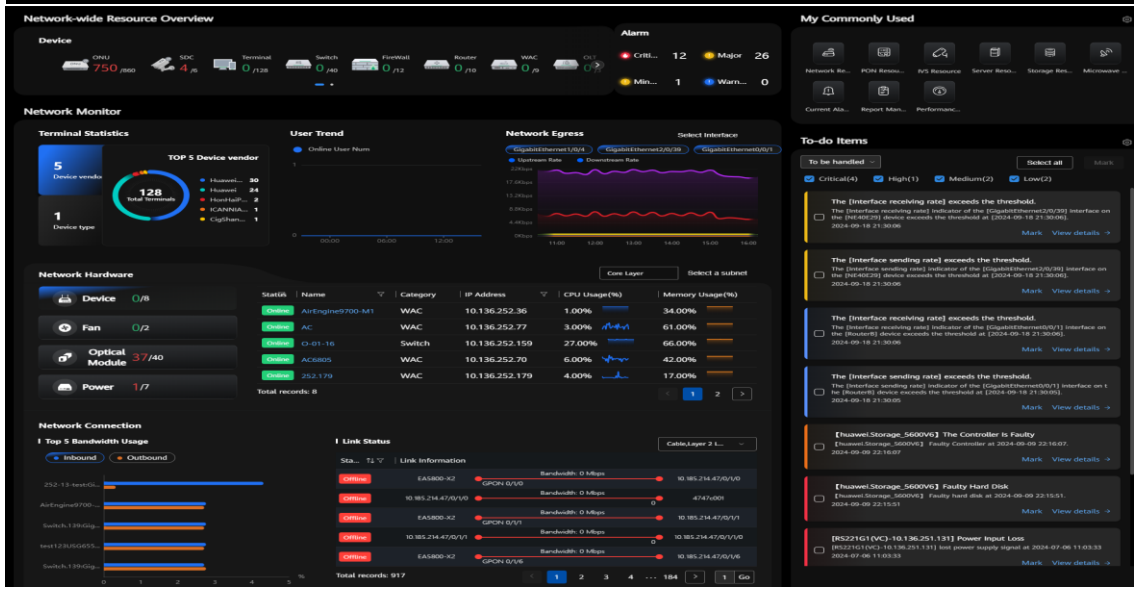
Network Optical Server Storage Video Microwave ....

SNMP ICMP Telnet Redfish SSH HTTPS SFTP

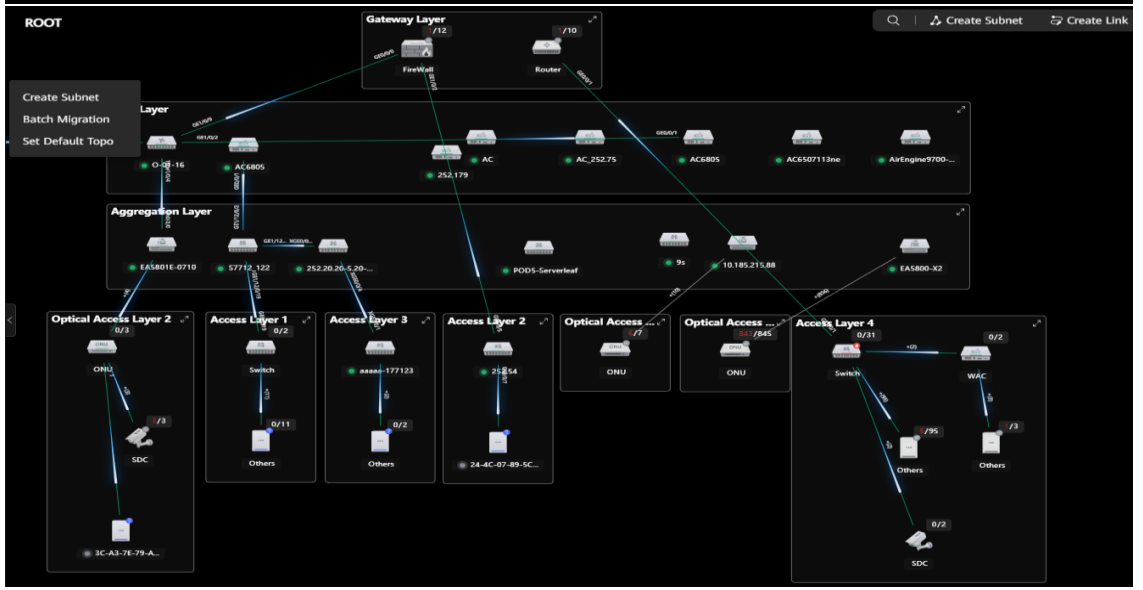
HUAWEI

Multi-dimensional Visualized Monitoring Improves O&M Efficiency

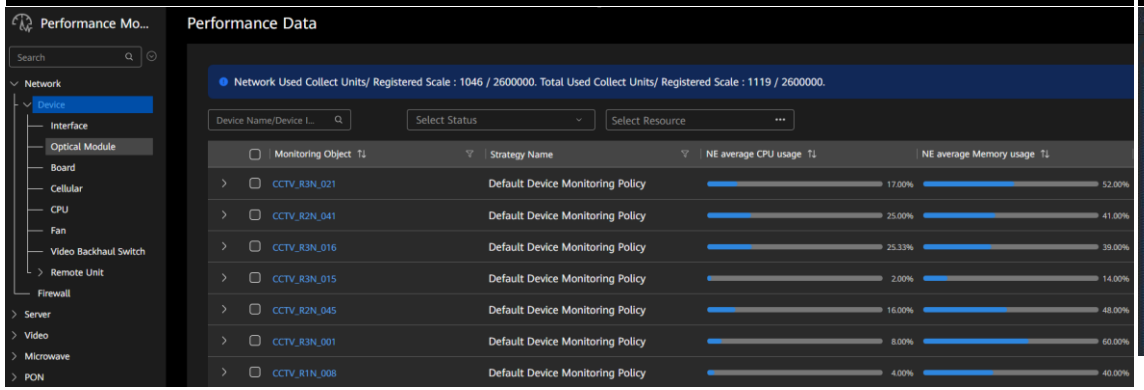
O&M workbench: centralized monitoring of network-wide devices, hardware, and connections



Domain-wide topology: displaying device, link, and terminal status in a visualized topology



Performance monitoring: visualized performance and various OOTB policies

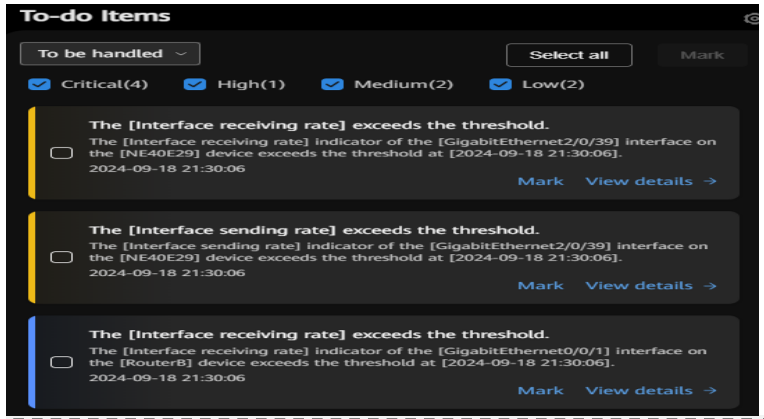


Alarm management: visualized, uninterrupted alarm monitoring and on-demand alarm rule configuration

HUAWEI

Intelligent Fault Detection, Data Analysis, and Data Perspectives

Intelligent fault management



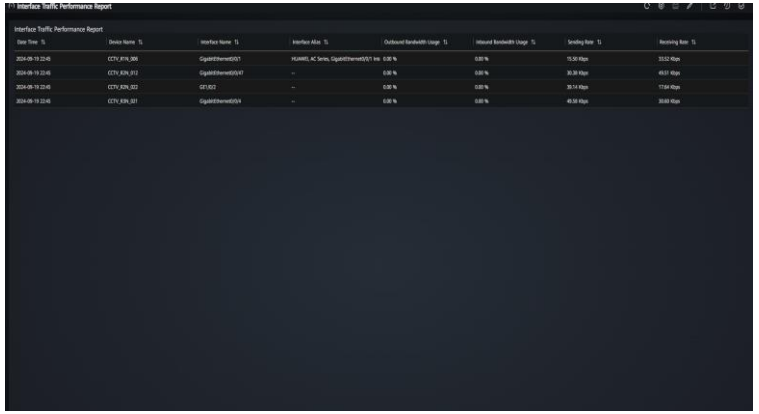
Proactive prevention: Typical faults, such as network loops and terminal exceptions, are automatically detected, enabling zero-wait risk awareness

Fault source tracing: The intelligent fault analysis engine automatically traces fault paths and root causes, improving diagnosis efficiency.

Category	Issue
Hardware	The device board is faulty.
Hardware	The optical module of the device is faulty.
Hardware	The optical module power is abnormal.
Hardware	The CPU usage of the device exceeds threshold.
Hardware	The storage space of the device exceeds threshold.
Hardware	The fan module of the device is abnormal.
Hardware	The power supply of the device is abnormal.
Hardware	The AP is offline.
Hardware	The device port is down.
Hardware	The board temperature is high.
Hardware	The power supply of the AP is insufficient.
Hardware	The power input is lost.
Hardware	The hard disk is lost.

Category	Issue
Hardware	The controller is faulty.
Hardware	The disk is faulty
Connection	Layer 2 loop
Connection	The switch has a PoE failure.
Connection	The device link is disconnected at the core layer.
Connection	The device is faulty.
Connection	The device is offline.
Connection	The device output rate of the interface is abnormal.
Connection	The device input rate of the interface is abnormal.
Performance	The inbound bandwidth usage on the interface exceeds the threshold.
Performance	The outbound bandwidth usage on the interface exceeds the threshold.
Performance	The percentage of receiving packets discarded on interface exceeds the threshold.
Performance	The percentage of sending packets discarded on the interface exceeds the threshold.

Intelligent report



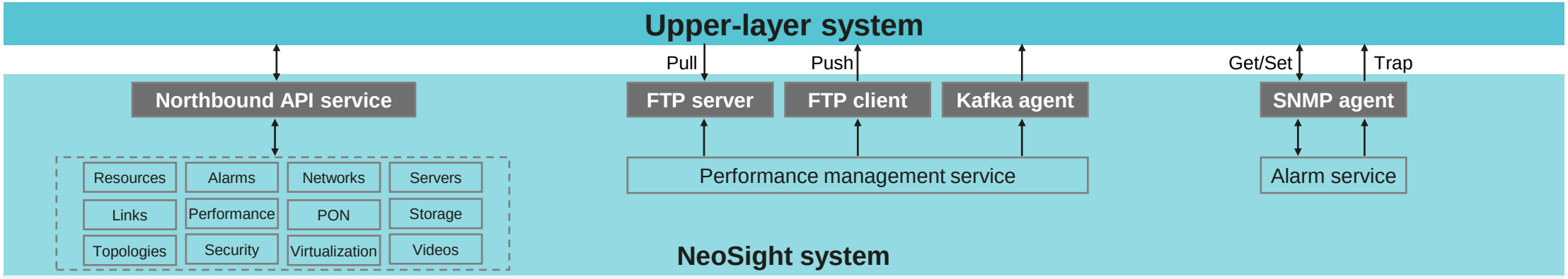
Report framework: Data integration, report display, scenario-based dashboard monitoring, self-service data analysis, periodic reports, and email notification capabilities are provided. This allows users to view and compare data from different dimensions and improve the quality of operations decisions.

- Preset reports: Multiple preset common O&M reports are provided for users to reuse O&M experience.
- On-demand customization: A flexible drag-and-drop layout allows users to easily customize reports.
- Remote push: O&M reports are periodically generated and sent by email. Multiple file types are supported.

Intelligent large screens

- Preset portals are provided for six typical scenarios: network campuses, WLAN campuses, POL campuses, data centers, and video surveillance.
- Data concerned by O&M roles is integrated from the perspective of users and displayed graphically for users to control the overall situation.
- Information can be displayed on one or more large screens in one-click carousel mode.

Various NBIs Facilitate Adaptation and Integration



Common HTTP (RESTful) NBIs

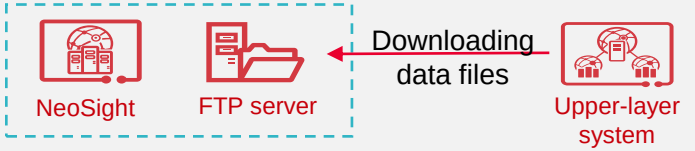
Data interfaces, such as resource, alarm, link, and performance interfaces, are supported. Various protection measures, such as HTTPS bidirectional security verification and access security isolation, are provided to ensure data security.

API access security isolation is described as follows:

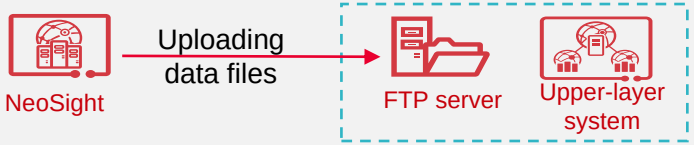
- API authentication: Built-in session, token, and basic authentication mechanisms ensure user authentication in multiple scenarios.
- API authorization: Authorization based on roles (such as administrators and operators) ensures security.
- API log audit and access control

FTP performance data NBIs

- Pull mode: NeoSight functions as the FTP server to provide performance data files, and the upper-layer system obtains the files from NeoSight.



- Push mode: NeoSight functions as the FTP server and pushes northbound performance data files to the FTP server specified by the customer.



Note: SFTP or FTP can be used in both modes. SFTP with higher security is recommended.

SNMP alarm NBIs

- Alarm reporting: Fault alarms, clear alarms, event alarms, acknowledged alarms, unacknowledged alarms, and change alarms can be reported.
- Alarm synchronization: Third-party systems can synchronize alarms periodically to ensure alarm information consistency with NeoSight. During the synchronization, third-party systems can stop the synchronization.
- Alarm clearance: Users can clear alarms on NeoSight based on alarm serial numbers.
- Alarm acknowledgment: Third-party systems can acknowledge alarms on NeoSight based on alarm serial numbers.

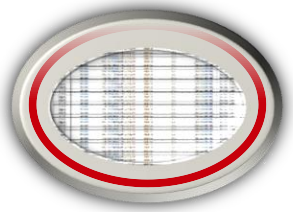
HUAWEI

Domain-Wide Topology for ICT Devices and Terminals, and Real-Time Awareness of Terminal Connections

Challenges

Manual layout is time-consuming and labor-consuming, and the visualization experience is poor

◆ Not visualized



ICT device information is provided in charts and cannot be visualized.

◆ Incomplete

Limited topology drawing capabilities make device layout time- and labor-consuming. It is difficult to display all ICT devices and terminals on one map.

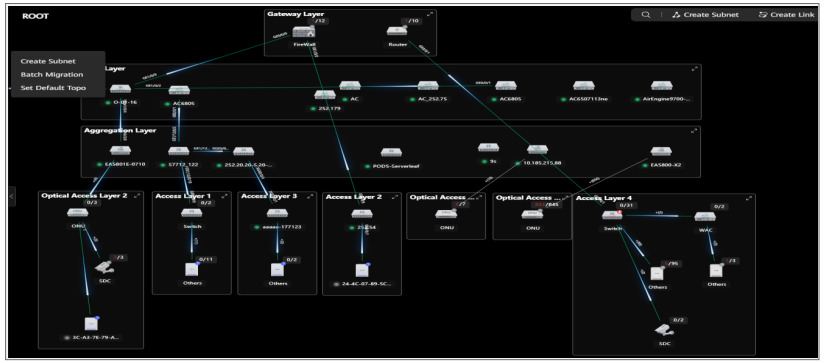
◆ Inaccurate

The device status, connection relationships, and ports depend on manual maintenance.

Solution

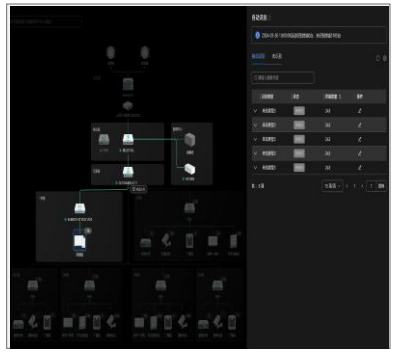
The Huawei-developed automatic layout algorithm enables full awareness of the terminal/link status

Full-stack visualization of ICT devices and terminals, automatic layout, and display of key information such as cross-domain device status, links, and performance KPIs on one map



Layer-by-layer drilldown, enabling real-time awareness of the terminal status and links

Automatic discovery, automatic identification, and cluster labeling of terminals



Benefits

Industry-leading OOTB topology with full-stack visualization

◆ Centralized management

NeoSight manages ICT infrastructures and terminals, including switches, routers, firewalls, PON devices, storage devices, servers, and cameras.

◆ Automatic layout

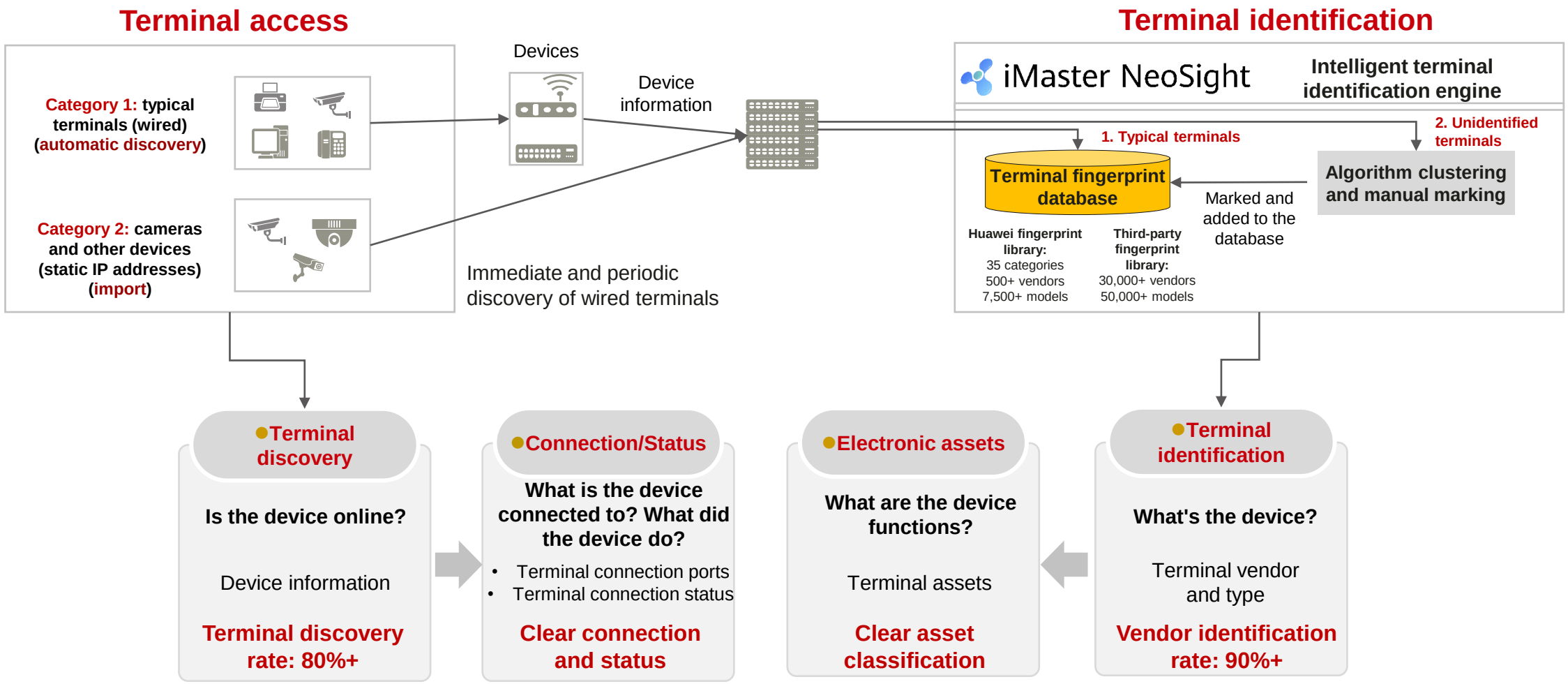
Automatic topology discovery and automatic generation of the logical architecture eliminate the need for manual layout.

◆ Status visualization

The device status and link status are displayed in real time, facilitating real-time awareness of the network-wide device health status.

HUAWEI

Terminal Management: Key Technical Solutions for Terminal Discovery and Identification



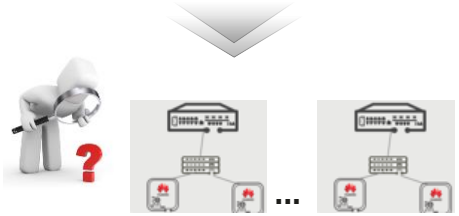
Fault Analysis: Self-diagnosis, Simplified O&M, and Improved O&M Efficiency

Challenges

Difficult fault locating

Camera fault

The computer cannot access the Internet.



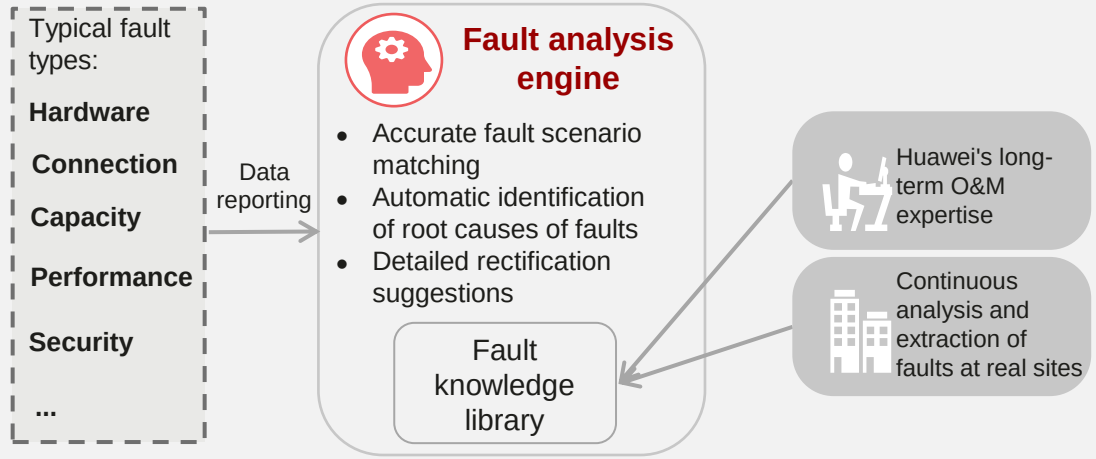
Where does the fault occur?

Slow problem detection	High skill requirements	Inefficient problem solving
Faults are detected after they occur, causing a significant negative impact.	No rectification suggestions are provided. Fault rectification depends on expertise.	The root cause of the fault is unclear, and the fault locating takes a long time.

Solution

Developing an intelligent fault analysis engine to organize typical faults, and trace root causes in one-click mode

Automatic diagnosis



Accurate demarcation

The **dynamic map technology** of the platform is used to restore links related to faulty devices in an E2E manner, **accurately determine fault points**, and provide instance locations and port information, improving fault closure efficiency.

Benefits

Expert-level O&M experience

- **Proactive prevention**

  Typical faults, such as network loops and abnormal terminals (cameras without images), are automatically detected, enabling zero-wait risk awareness.

- **Fault source tracing**

  The intelligent fault analysis engine automatically traces fault paths and root causes, improving diagnosis efficiency.

HUAWEI

Workbench: One-Stop O&M Platform Improves Work Efficiency

Challenges

Isolated information

A large number of menus cause information silos

What information do I need to resolve a problem?

Different O&M personnel need different information

O&M personnel

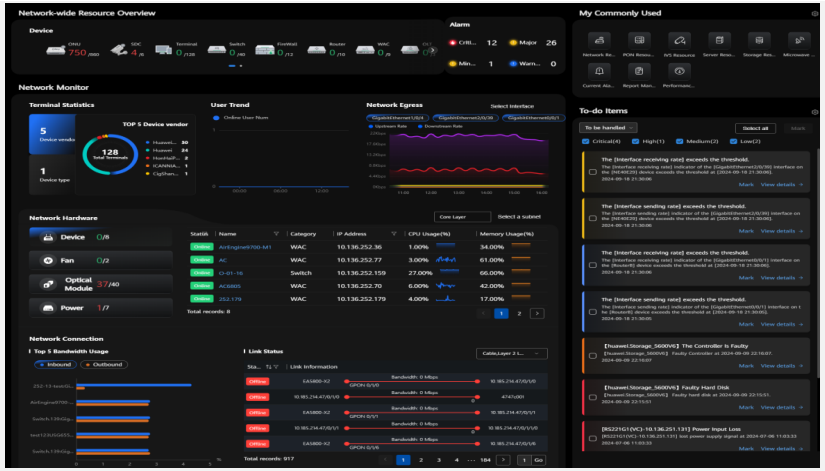
Difficulty in customization the workbench

The workbench cannot be easily customized for different O&M personnel in common scenarios.

Solution

Visualizing key service information and providing quick access to common tools

Information integration



OOTB workbench

A preset simplified O&M workbench is provided, including the device resource overview, KPIs, common links, alarm cards, O&M tools, and to-do items.

Scenario-specific customization

Preset common cards

Multiple preset common cards are provided in the system.

Drag-and-drop customization

The workbench can be customized in drag-and-drop mode.

Benefits

The workbench solves 80% of problems

- **Information integration**

  By default, a one-stop O&M platform is provided for campus scenarios. Key information is visualized, and O&M tools can be quickly obtained, improving O&M efficiency.

- **Scenario-specific customization**

  The workbench can be customized based on different scenarios or users and provide multiple common cards.

HUAWEI

Performance Management

The performance management function supports various resource types and can collect and manage a large number of KPIs. It provides preset common policies, performance monitoring, favorites, and northbound data modules. It allows users to customize collection policies, common favorite items, and alarm generation rules, improving O&M efficiency.

OOTB

- Optimal threshold policies are continuously accumulated and improved to facilitate OOTB usage.

Threshold-crossing alarms

- Performance data is automatically monitored, and alarms can be reported, facilitating network maintenance.

One-click favorites

- Key devices and indicators can be added to my favorites in one-click mode, facilitating important holiday assurance tasks.

Management specifications

- Huge volumes of KPI statistics cn be collected, facilitating network-wide resource management.

HUAWEI

Report Framework

The report framework provides a professional and E2E data analysis and report display platform. It offers the data integration, report display, dashboard-based scenario-specific monitoring, self-service data analysis, periodic reports, and email notification capabilities. Users can view and compare the data from different dimensions to improve the quality of O&M decisions.

Preset common O&M reports

- Multiple preset common O&M reports are provided for users to reuse O&M experience.

Flexible and on-demand report customization

- A flexible drag-and-drop layout allows users to easily customize reports.

Periodic O&M reports

- O&M reports are periodically generated and sent by email. Multiple file types are supported.

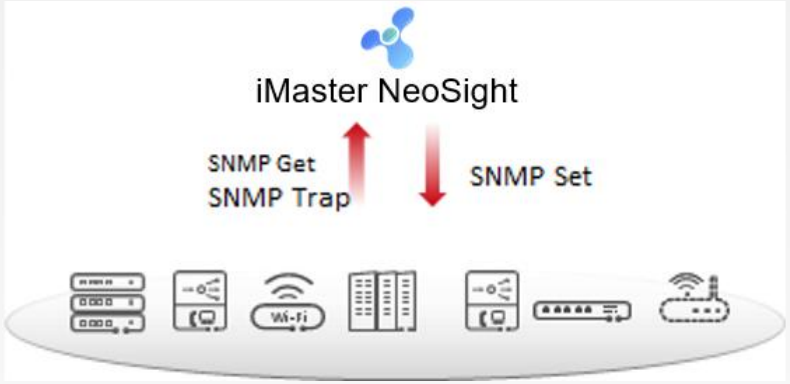
Large-screen display

- Reports can be displayed and managed on multiple large screens.

HUAWEI

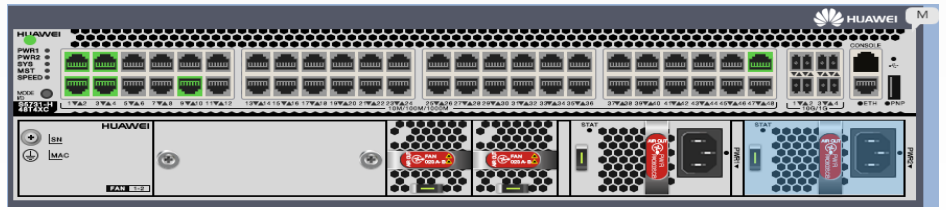
Automatic Discovery and Monitoring of Network Devices

SNMP-based device management



Device management scope	Datacom network devices (such as S, CE, NE, AR, and FW) and third-party network devices managed through SNMP
Principle of automatic discovery	The IP network segments entered by the user are parsed, and SNMP connection requests are sent to valid IP addresses one by one. If an IP address can receive SNMP response packets, the device is successfully discovered.

Automatic monitoring and rich information: basic device information, device interfaces, panels, links, alarms, KPIs, and others



The following device information is automatically monitored:

1. Basic device information
2. Alarm statistics of a single device
3. Key resources: interface, power supply, and fan status statistics
4. Device KPIs: The KPIs that exceed the thresholds are marked in red.
5. Link relationships between a single device and peripheral devices
6. High-fidelity panel
7. Remote unit management

Batch Device Configuration

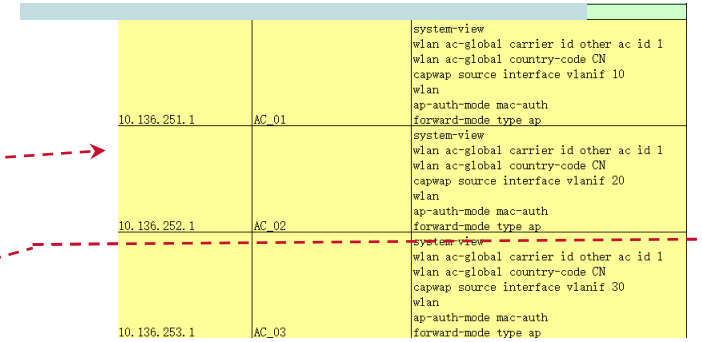
Case: The network administrator of a company needs to reconstruct the network and add three ACs that belong to different networks. The administrator needs to configure different commands on the three ACs to connect the ACs to different networks. Configuring devices one by one after remote login is time-consuming and laborious. The administrator can use the command configuration tool of eSight to quickly solve the problem.

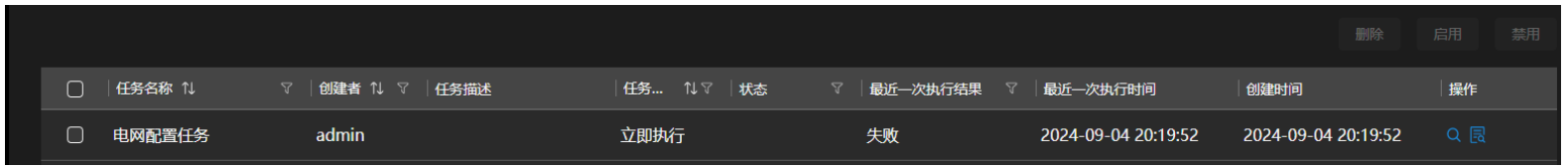
Step1
Fill out the form.

Step2
Set the period.
Supports immediate execution and periodic execution (daily, weekly, or monthly).

Step3
View the result.
Supports command re-editing and retry upon failures.

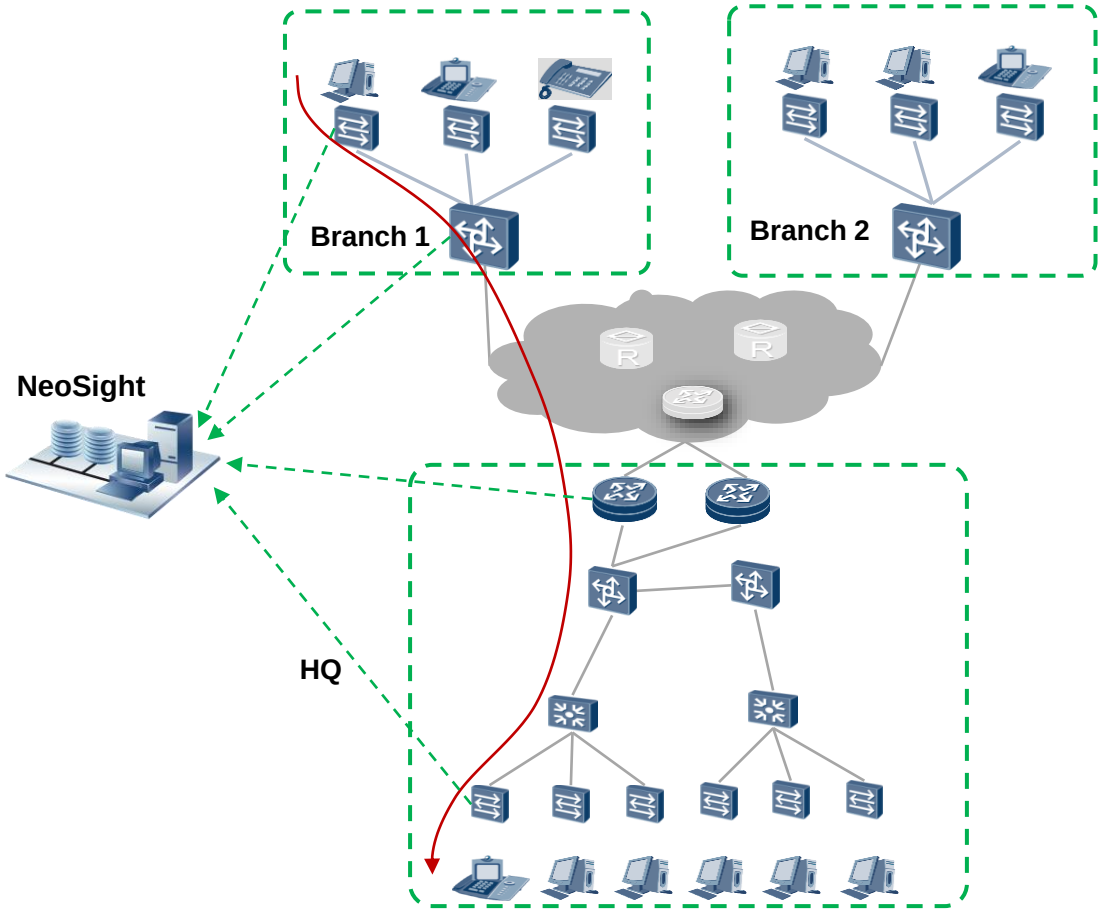
Step4
Audit the task.





HUAWEI

SLA: 24/7 network quality monitoring



Various evaluation models

Supports 6 types of NQA test cases and 16 preset SLA services.

Intelligent network quality monitoring

Supports 2,000 SLA test tasks, periodic detection, and proactive O&M based on quality scores and alarms, helping users to quickly detect problems.

Quick diagnosis and fault demarcation

Segment-based quick diagnosis helps quickly demarcate network faults in real time.

Historical quality analysis and improvement

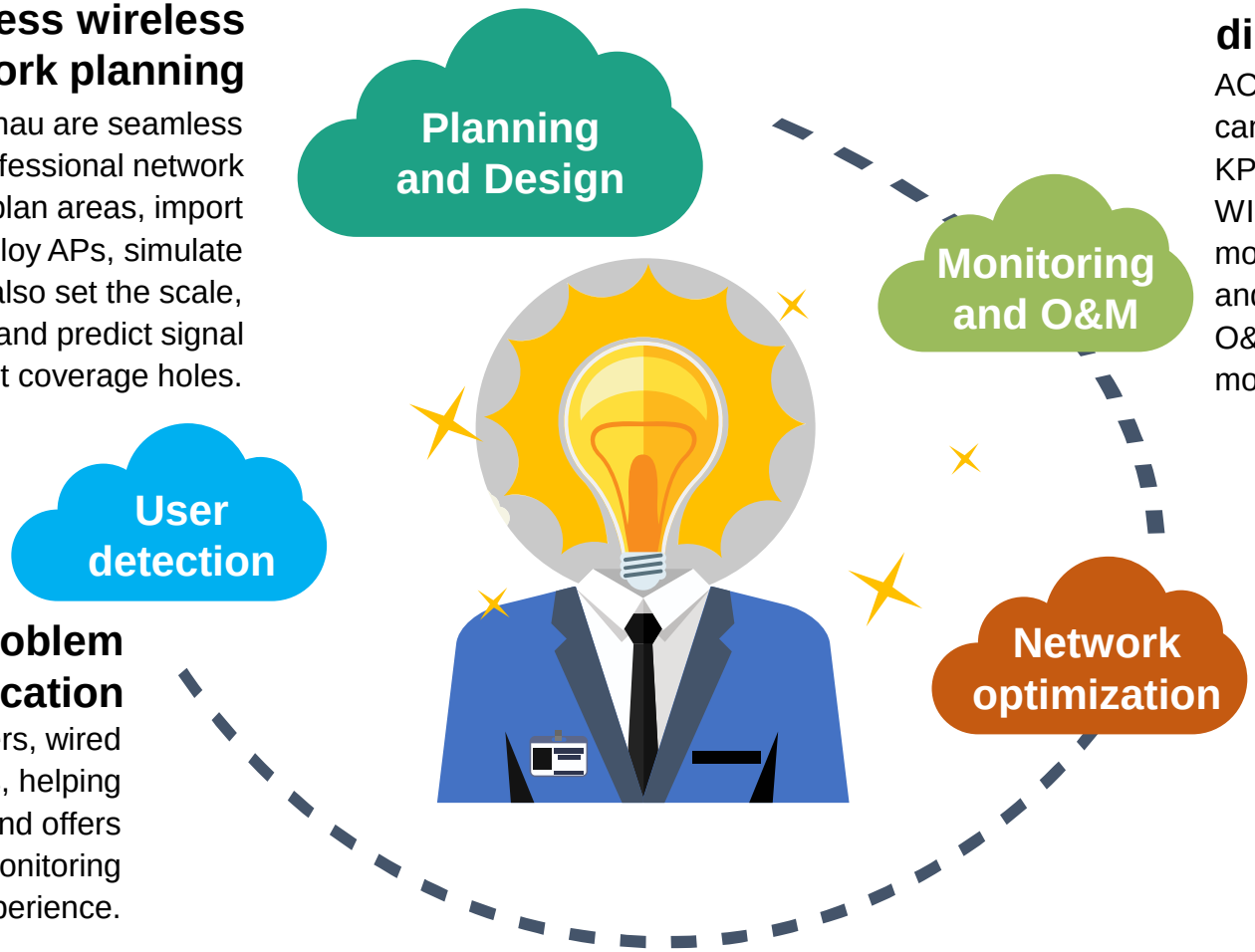
View historical data to learn about fault information and optimize the network.

Note: This function depends on the NQA capability of devices.

WLAN Management, Monitoring, and O&M Solution

Full-process wireless network planning

WLAN Planner and Ekahau are seamless interconnected to import professional network planning data. Users can plan areas, import construction drawings, deploy APs, simulate buildings and floors. They can also set the scale, plan obstacles, and visualize and predict signal coverage without coverage holes.



Regional simulation and multi-dimensional statistics analysis

ACs, APs, users, RF devices, and SSIDs can be managed. Device information, KPIs, and alarms can be monitored. The WIDS security management function monitors unauthorized devices, attacks, and interference sources, and displays O&M information on the portal and region monitoring page.

E2E and quick problem identification

One-click detection integrates users, wired networks, and wireless networks, helping users quickly demarcate faults and offers rectification suggestions. KPI monitoring and user profiling ensure user experience.

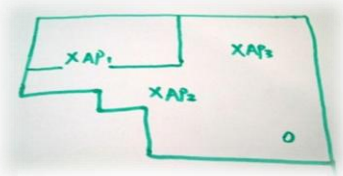
Wireless signal coverage and configuration optimization

The layout is simulated based on the real-time AP power, working channel, scale, and obstacles (shape and attenuation). Signal coverage is also simulated to optimize AP configurations and improve wireless signal coverage.

HUAWEI

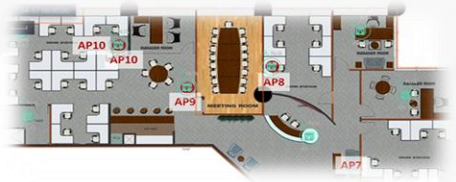
Planning and Design: Precise Network Planning Based on Professional Tools

Manual planning



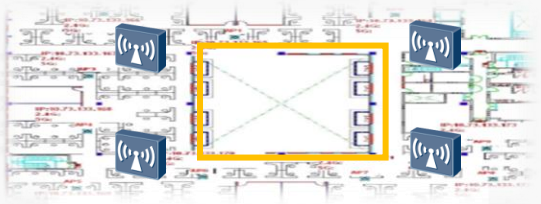
- **Difficulty in quality assurance:** Potential coverage holes and interference may occur. Users' bandwidth requirements are difficult to meet.
- **Inefficient, high risks, and difficult to reuse**

Automatic network planning in two modes



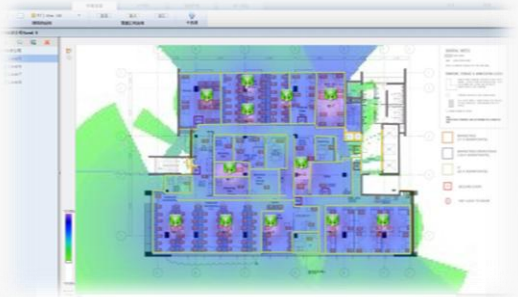
- **Data import:** After completing network planning using the network planning tool, users can import the planning project file on the regional monitoring page to **prevent repeated planning and improve planning efficiency.**
- **Online network planning:** After an AP goes online and runs properly and is synchronized to the NMS, users can **add the AP to the region monitoring management scope** online.

WLAN Planner: professional network planning



- Huawei has developed a standard model library based on years of WLAN **experience** and **excellent project practices**.
- APs are automatically placed based on coverage requirements.
- Floor planning is quickly completed to meet signal coverage, bandwidth, cabling, and power supply requirements.

Detailed planning report, guiding network deployment



- Simulation drawings, planning lists, AP lists, and other planning information are generated.
- **Network planning project files** are generated.

- **Scientific and efficient:** The professional coverage algorithm can **plan a new floor every 30 minutes**, **shortening the network construction period by 30%.**
- **No coverage holes or conflicting areas:** A maximum of **nine levels** of areas are supported. Campuses, buildings, and floors are simulated, **reducing O&M problems by 20%.**
- **Inheritable results:** The results are standardized and can be exported and reused. Huawei's WLAN Planner and Ekahau network planning project files are supported.

HUAWEI

Third-Party Device Management Capabilities

Feature	Capability	Pre-integration (OOTB)	Standardization (SNMP MIB2)	Online Customization without Coding	Constraint
Device management	Device vendor	√	Partially supported	√	SNMP MIB2 standard NeoSight network device management interface specifications
	Device type	√	Partially supported	√	
	Device type	√	Partially supported	√	
	Status monitoring	√	√	/	
	Device name	√	√	/	
	Software version	√	Partially supported	/	
	Link discovery	√	√	/	
Interface management	Interface management	√	√	/	
	Interface performance	√	√	/	
Alarm management	Alarm reporting	√	Partially supported	√	
	Alarm clearance	√	Partially supported	√	
	Multi-lingual alarms	√	Partially supported	√	
Performance management	Average CPU usage	√	X	√	
	Average memory usage	√	X	√	

Content

Campusowe Systemy NMS

iMaster

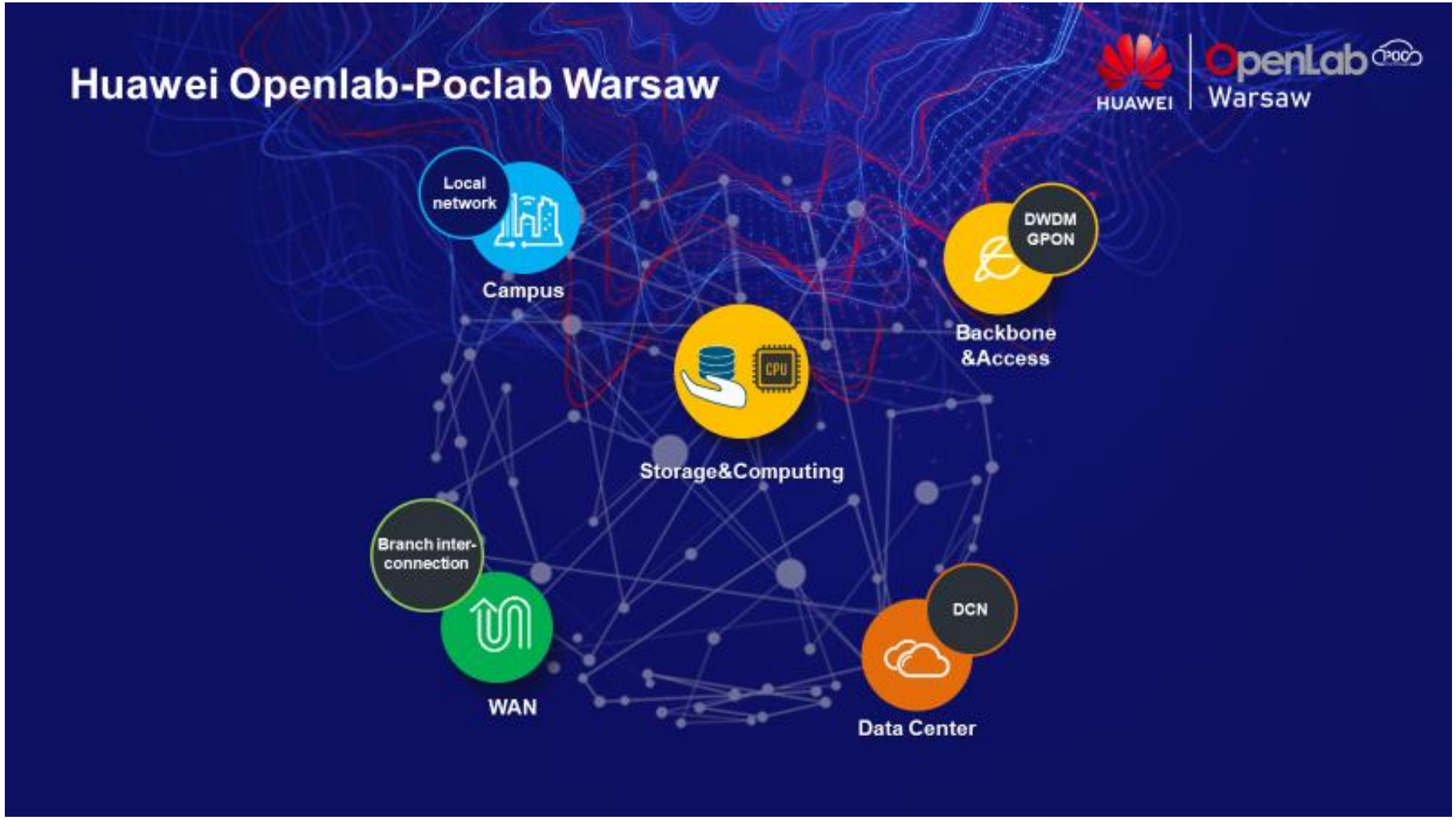
eSight

NeoSight

Podsumowanie + Q&A

HUAWEI

Huawei Warsaw OpenLAB



Local POC Test
For Solution Design

Local Platform for Knowledge and Ideas Sharing

Local Mirror Environment
For Key Customers

HUAWEI

HUAWEI

Building a Fully Connected, Intelligent World

Accelerate Industrial Intelligence with Huawei Intelligent Cloud-Network

Powered by

AirEngine
Wi-Fi 7

NetEngine
Routers

CloudEngine
Switches

HiSecEngine
Security Gateways

iMaster NCE
Network Digital Map

Scan for more information