NO WARRANTY

THE CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE,ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO CASE SHALL HUAWEI TECHNOLOGIES CO., LTD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS MANUAL.

HUAWEI TECHNOLOGIES CO., LTD.
Bantian, Longgang District
Shenzhen518129, P. R. China
Tel:+86-755-28780808

www.huawei.com

Huawei Agile Campus Network Solution

HUAWEI TECHNOLOGIES CO., LTD.

[01]

Challenges to Campus Networks

Since its rollout in 1989, the Ethernet switch has become a key component in IT network development. With network devices such as Ethernet switches and routers increasing in forwarding performance, functional features, and port rate, networks provide advantages of high performance, cost-effectiveness, and ease of use. In recent years, with new concepts such as Bring Your Own Device (BYOD) mobile office, cloud computing, Software-Defined Networking (SDN), Internet of Things (IoT), and Big Data growing in popularity, new technologies andapplications are springing up and deployed on enterprise campuses, posing considerable challenges on campus networks.

Challenges Created by Mobile Applications: Convenient Access Anywhere, Anytime, Higher Speed, and Better Experience

The widespread use of Wireless Local Area Network (WLAN) at enterprise campuses increases employees' demandsfor accessing the corporate network resource anywhere, anytime using any device, as well as enjoying convenient mobile office. However, during mobile office construction, enterprises are often faced with the following challenges:

▪ Ubiquitous access anywhere, anytime

An ever-growing number of mobile applications drives employees to connect tothe enterprise networktowork in an office zone or a conference room, outside a campus, or on a business trip using a corporate PC, a self-owned tablet, or a mobile phone. To overcome this challenge, the top priority is ensuring that users can connect to the enterprise network anywhere, anytime.

▪ Access of a high density of terminals

In scenarios such as conference rooms and stadiumswith a huge number of terminals in use, some terminals may fail to connect to the network even though there is full wireless signal coverage and the signals are strong enough.

▪ Multimedia service experience guarantees

Even though users can effortlessly connect to the campus network, real-timemultimedia services such as video and voice services pose high requirements on packet loss, latency, andjitter. It is challenging to guarantee a good experience of real-time services. In addition, if the service experience is degraded, how to enable the network to precisely identify applicationsand quickly adjust policies such as Quality of Service (QoS) policies is also a huge challenge.

- **Free mobility and consistent experiences**

Toensure that users obtain consistent service experiences when they connect to the campus network at different locations, access control andQoS policies must dynamically vary withthe user location. Nonetheless, on traditional enterprise campus networks, these policies must be manually configured, which overloadsthe network Operations and Maintenance (O&M) personnel. User rights are also difficult to manage. Consequently, enterprises can neither quickly respond to user demandsnor ensure consistent service experiences.

Challenges Confronting Network O&M Personnel: Split Networkand Complicated Network O&M

Enterprise network size (the number of network nodes) andbandwidth have been growing exponentially. Accordingtostatisticsby a well-known consulting firm, the number of terminals connected to networks has reached 10 billion by the end of 2010 which, will grow to 50 billion by the end of 2020. In addition, the widespread use of WLAN andthe rapidly growing mobile Internet-based applications have brought about the following challenges to network O&M:

- **Automatic network deployment**

Currently, most network planning and deployments still rely on manual configuration. Accordingtostatisticsby Huawei, the workload of initial installationand configuration of network devices accountsfor 18 percent of the total routine workload of network O&M personnel. With an exponentially growing number of network nodes, how to implement automatic network deployment andlower the workload of network O&M personnel has become an urgent problem.

- **Unified network O&M**

Service mobility has resulted in large-scale wireless network deployments. Nevertheless, wired and wireless networks usetwo independent management and authentication systems. As a result, management of wired and wireless networks is considerably complicated. To achieve unified management of wired and wireless networks is another big challenge.

- **Network security enhancement**

The mobile office leads to surging terminal and network security problems, and blurs the security protection border. To make matters worse,with diversifying network attack methods, the number of network attacks through unknown attacks keeps increasing. To quickly detect potential network security threats and effectively defend against the threats is another challenge tocampus networks.

- **Simplified network O&M**

Also according tostatisticsby Huawei, the workload of network monitoring and troubleshooting accountsfor 28 percent of the total workload of network O&M personnel. A growing number of real-time services that are sensitive to network quality have created a new challenge to network O&M personnel.

Challenges Created by Burgeoning New Services: Open Services vs. Closed-Off Networks

Today's new services such as the mobile, cloud computing, IoT, and Industry 4.0 place ever higher requirements on the network functionality. Take the number of IETF RFCs as an example. One thousand-some RFCs were released over 20 years while, in the last 10 years, over 3,000 RFCs were released. In order to achieve business success, enterprises hope to shorten the time needed to provision new services. Accordingly, networks are faced with the following challenges:

First, the campus network must be open. User information, location information, and policy management must be open toupper-layer services. When new services are deployed or services are adjusted, network policies can be quickly deployed, and services can be quickly provisioned. In addition, the upper-layer service platform canobtain information from the network, provisioning more Value-Added Services (VAS)and creating more business value. For example, when an enterprise adjusts a specificservice, the network rights, QoS, and security policies must be quickly deliveredto network devices to lower the manual configuration and maintenance workload. If a shopping mall is deployed with a Wi-Fi network, the shopping mall operator hopes tooffervariousVAS such as wireless location, navigation, and precision marketing.

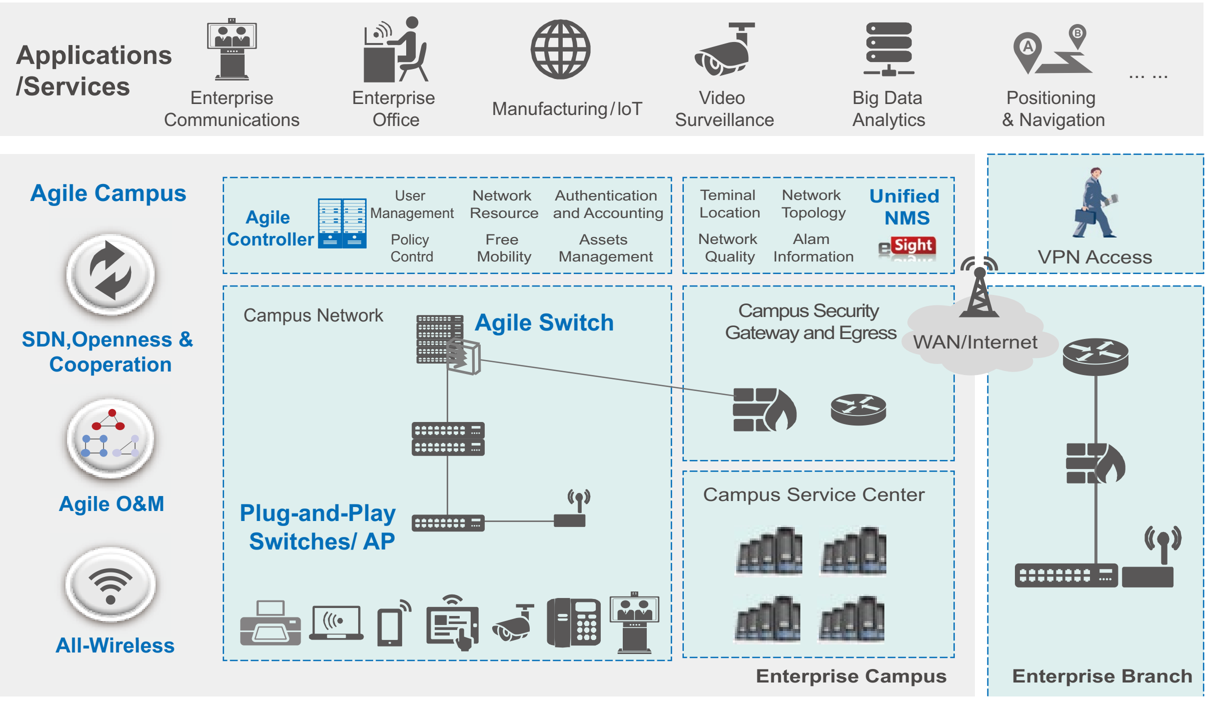
Second, the functional layer of campus network devices must be flexible and programmable. Currently, almost all enterprise networks are composed of switches. However, the packet forwarding plane of traditional switches uses Application-Specific Integrated Circuit (ASIC) chips in which the packet forwarding function is fixed. Consequently, the enterprise networks cannot adapt to new services, applications, or standards. If enterprise customers require that the network devices should support new protocols and standards, the ASIC chip must be redesigned andproduced. The average chip production period is 24 months, which affects new service provision.

[02]

Huawei Agile Campus Network Solution

2.1 Solution Overview

Huawei Agile Campus Network Solution is the implementation of Huawei's Agile Network Solution in campus networks. The Agile Network Solution is the next-generation network solution designed by Huawei for the enterprise market. This solution leverages the SDN concept andthe latest research achievements in the industry. Based on Huawei's more than 20 years of network deployment experience, this solution enables networks to be more agile for services.



Huawei's Agile Campus Network Solution is intended to resolve users' actual problems in campus networks. Compared to traditional campus networks, an agile campus network achieves the following architectural innovations:

▪ Smart and Open "Brain"

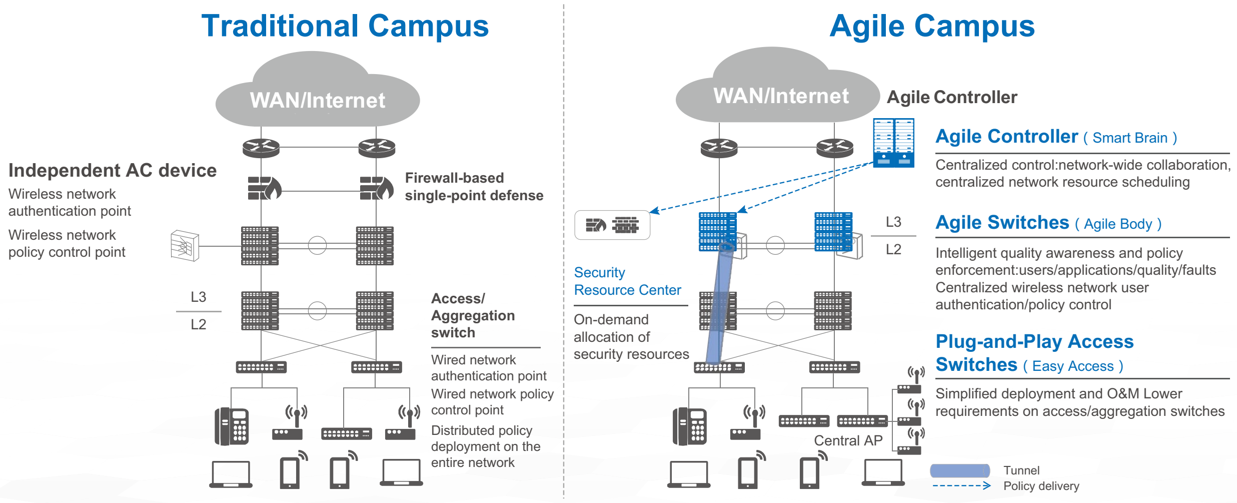
Huawei's Agile Controller is the industry's first controller tointroduce SDN's centralized control concept into campus networks. The Agile Controller implements collaborative control of network-wide devices including switches, WLAN devices, firewalls, and SVN devices. Capable of dynamically allocating network and security resources, the Agile Controller allows network resources to move with user locations and enables on-demand allocation of security resources. Moreover, through standardandopen interfaces, the Agile Controller makes campus network information open to third-party service systems, and provides a secondary development platform, enabling rapid service innovations.

▪ Agile Body and Zero Touch Provisioning (ZTP) of Access Switches

Huawei's Agile Campus Network Solution builds a campus network using programmable agile switches instead of traditional switches that use ASIC chips. The solution achieves intelligent quality awareness and policy enforcement, such as awareness of user information, service types, service quality, and network faults. This solution also achieves unified authentication of wired and wireless users and policy enforcement. Additionally, using Huawei-developed fully programmable Ethernet Network Processor (ENP) chips, the agile switches implement full programmability in the forwarding plane, enabling rapid new service provision. The solution also implements automatic deployment of devices at the access layer, such as access switches and WLAN Access Points (APs), which are plug-and-play. This substantially lowers the network management workload and network O&M costs.

▪ Security Resource Pooling

Huawei's solution integrates independent security devices on the traditional campus network. All services on the entire network can share the security resource. The security resource pool turns individual security resources such as firewalls into a resource pool that isshared network-wide.


Traditional Campus
WAN/Internet
Independent AC device
Wireless network authentication point
Wireless network policy control point
Firewall-based single-point defense
L3
L2
Access/ Aggregation switch
Wired network authentication point
Wired network policy control point
Distributed policy deployment on the entire network
Agile Campus
WAN/Internet
Agile Controller
Security Resource Center
On-demand allocation of security resources
L3
L2
Central AP
Tunnel
Policy delivery

Agile Controller (Smart Brain)

Centralized control:network-wide collaboration, centralized network resource scheduling

Agile Switches (Agile Body)

Intelligent quality awareness and policy enforcement:users/applications/quality/faults Centralized wireless network user authentication/policy control

Plug-and-Play Access Switches (Easy Access)

Simplified deployment and O&M Lower requirements on access/aggregation switches

Through the three unique innovations, Huawei's Agile Campus Network Solution helps enterprises build an all-wireless campus network that supports agile O&M, SDN, and openness andcooperation. By leveraging this solution, users can connect to the campus network anywhere, anytime, andobtain an excellent service experience. In addition, IT O&M personnel can carry out full lifecycle management of the campus network. Moreover, the solution supports rapid functional expansion and connection to third-party systems, enabling campus networks to be more agile for services.

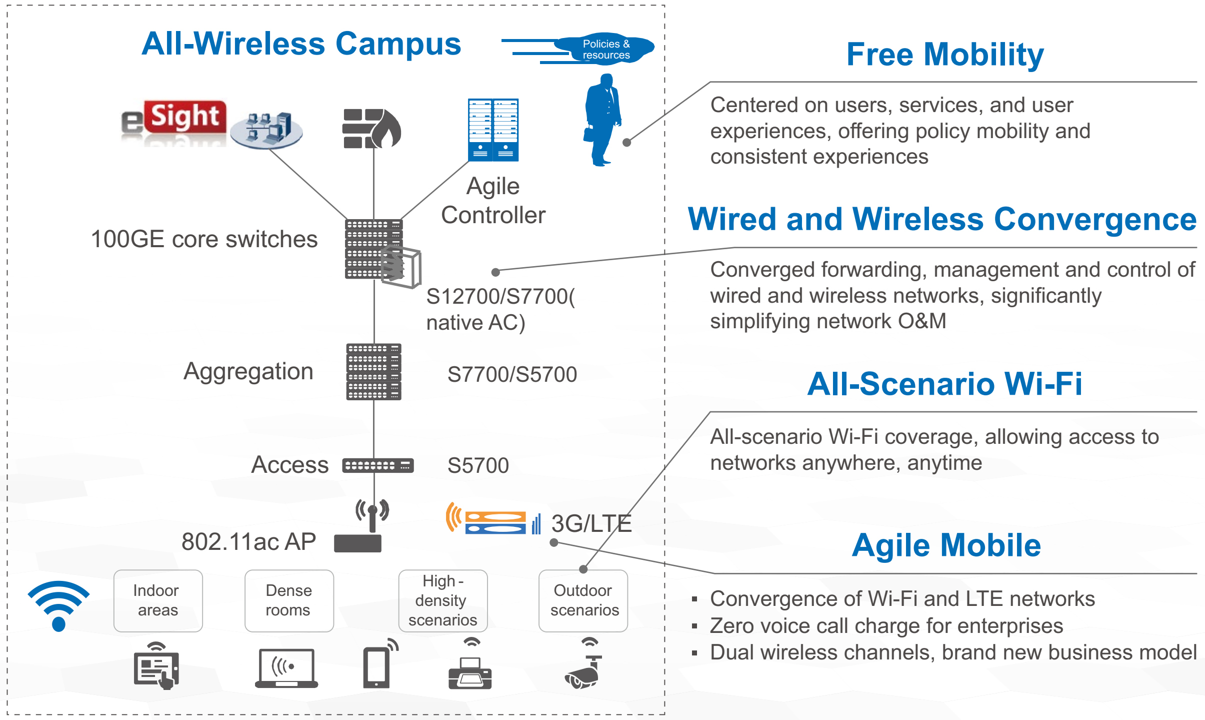
2.2 Solution Details

2.2.1 All-Wireless Campus Network Provides Access Anywhere, Anytime, Guaranteeing Excellent User Experiences

The rapid development of new network technologies and the widespread use of BYOD drive mobile office and wireless access to grow in popularity. Users want to work anywhere, anytime in a mobile fashion.

However, due to blind spots, restrictions on the number of access users, insufficient wireless throughput bandwidth, and access rights control on traditional wireless campus networks, users connecting to the network through a WLAN cannotobtain a smooth experience as wired network users. In addition, it is difficult to guarantee experience consistency for mobile office users. The wired and wireless networkseparationresults in high network O&M costs.

Huawei's Agile Campus Network Solution consists of Agile Controller, agile switches, Agile Distributed Wi-Fi Solution, and high-density WLAN APs. The solution implements free mobility using the Agile Controller and agile switches, and builds a campus network that is centered on user and service experiences, guaranteeing consistent experiences for mobile office users. The agile switches with a built-in native Access Controller (AC) work with the WLAN APs to converge wired and wireless networks. Apart from delivering a high-performance forwarding capability, Huawei's solution also implements unified management of wired and wireless networks. Through the all-scenario Wi-Fi network deployment, Huawei's solution provides full signal coverage and high-density user access in various scenarios.



Free Mobility

Centered on users, services, and user experiences, offering policy mobility and consistent experiences

Wired and Wireless Convergence

Converged forwarding, management and control of wired and wireless networks, significantly simplifying network O&M

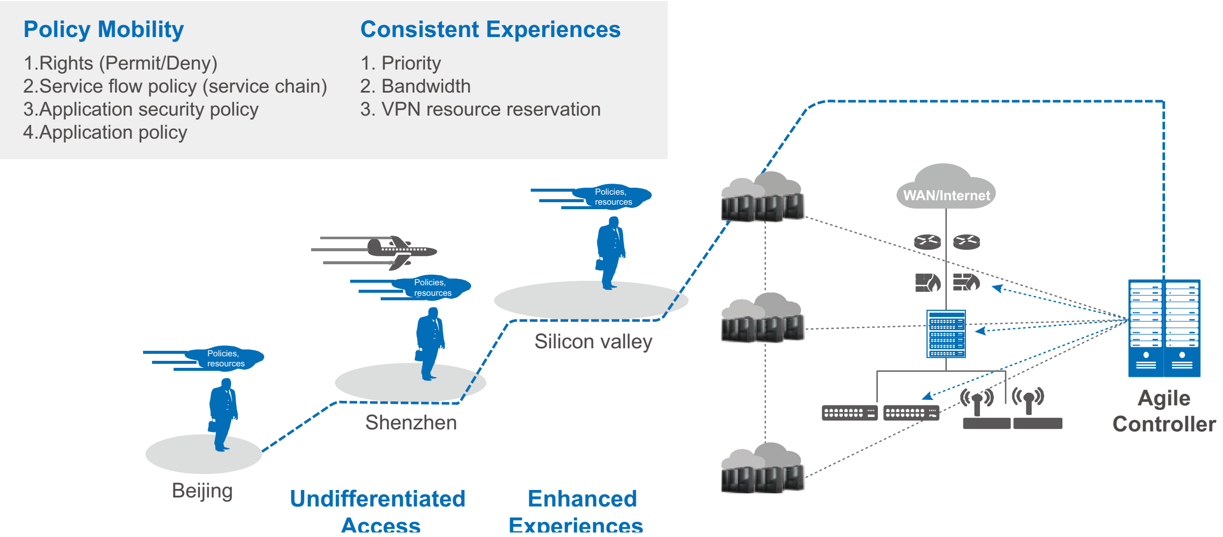
All-Scenario Wi-Fi

All-scenario Wi-Fi coverage, allowing access to networks anywhere, anytime

Agile Mobile

- Convergence of Wi-Fi and LTE networks
- Zero voice call charge for enterprises
- Dual wireless channels, brand new business model

2.2.1.1 Free Mobility: Centered on Users, Services and Experiences



Huawei's Agile Campus Network Solution uses the Agile Controller and agile switches, andintroduces the centralized control concept of SDN into campus networks. The Agile Controller centrally manages and controls network-wide policies. Specifically, the solution defines user-, service- and experience-centric policies on the Agile Controller, and then delivers them to policy enforcement devices such as switches, Next-Generation Firewalls (NGFWs), and SVN devices. When a user connects to the campus network from different locations using different terminals through a wired intranet, a wireless intranet, and a remote extranet, the Agile Controller automatically identifies the user and the user groupto which he or she belongs, and sends user policies to network-wide policy enforcement devices. Thisensures that users' network access is completely decoupled from their IP address, and they could obtain consistent service experiences.

▪ Service- and User Experience-Centric Policy Management

Huawei's Agile Campus Network Solution defines user rights, access control, andservice flow policies, experience-related user and service priorities, bandwidth, and VPN resources based on user groupsandapplication identification on the Agile Controller. The solution implements not only inter-user-group rights control but also rights control between a user groupand a resource group, thus achieving flexible, fine-grained user rights control and reducing the consumption of device resources (for example, the number of ACLs). Additionally, device-based application identification guarantees bandwidthand priority for particular users and services, resolving the problem that mobile office experiences cannot be guaranteed due to frequently changing IP addresses.

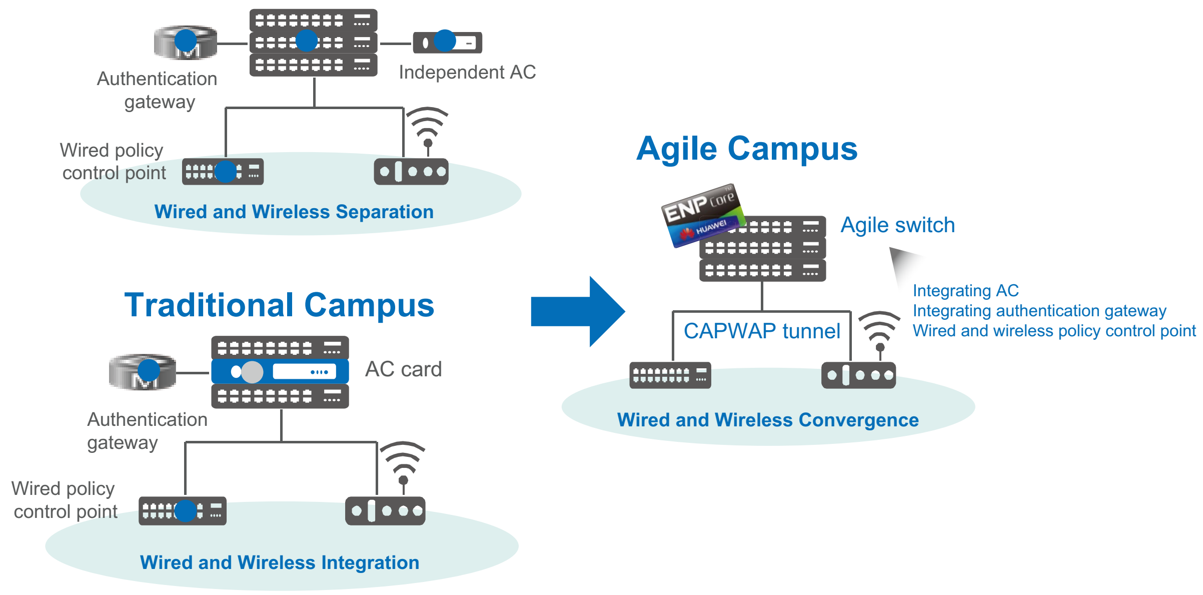
▪ Unified User Experience Guarantees

No matter whether users access an enterprise's intranet resource or the Internet resource from a branch or the campus headquarters or in a remote manner, corresponding bandwidthandQoS policies are deployed on key policy enforcement points that influence the service experience, such as VPN access gateways, Internet egress firewalls, and branch egress devices. In this way, users can attain consistent service experiences. Additionally, a VIP user's traffic can be preferentially scheduled, and sufficient bandwidthis guaranteed. For example, the solution allows automatic selection of VPN gateways and preferential access for VIP users. That is,whena user remotely connects tothe network through a VPN gateway, the VPN client will automatically select an access gateway with the lowest latency. Additionally, whena gateway's available resource has been exhaustedbya large number of online users, the gateway automatically forces some users to go offline to release system resources for VIP users, ensuring preferential access and higher-priority service experiences forthem.

2.2.1.2 Wired and Wireless Convergence: Outstanding Performance and Simplified O&M

On traditional campus networks, common wireless deployment methods includethe methods using independent AC devices andAC cards. Wired and wireless networks are separated in forwarding and control planes. With the arrival of the 802.11ac protocol and widespread use of the BYOD mobile office, AC devices have become performance bottlenecks due to their limited forwarding capacity and port rate. Wired and wireless user authentication and policy management are independently performed on switches and ACs, which overloads the network O&M personnel.

Huawei has put forth its innovative idea of wired and wireless convergence, which takes full advantage of both wired and wireless networks. Huawei's Agile Campus Network Solution converges and optimizes wired and wireless networks in terms of both user access and network management experiences, helping enterprise users obtain consistent utilizationand management experiences.


Authentication gateway
Independent AC
Wired policy control point
Wired and Wireless Separation
Traditional Campus
Authentication gateway
AC card
Wired policy control point
Wired and Wireless Integration
Agile Campus
ENP Core
HUAWEI
Agile switch
Integrating AC
Integrating authentication gateway
Wired and wireless policy control point
CAPWAP tunnel
Wired and Wireless Convergence

- **Converged Forwarding: Improving Performance with Unified Wired and Wireless Traffic Forwarding**

Wireless functions are integrated into a line card as a built-in feature. In this way, forwarding, control, and management planes of wired and wireless networks are converged at the network element level. Agile switches' forwarding capacity (up to the terabit level) and scalability completely eliminate the traffic bottlenecks caused by the traditional forwarding function of AC devices andACcards. In addition, users do not need to purchase additional AC devices or AC cards, significantly reducing customers' Total Cost of Ownership (TCO).

- **Converged Management: One Device Manages One Campus, Simplifying Management**

There are large numbers of access switches and WLAN APs on a traditional wireless campus network, which makes it difficult to manage the entire network. Huawei's Super Virtual Fabric (SVF) technology can not only virtualize fixed switches into remote virtual cards on a core or aggregation switch, but also virtualize APs as ports on a switch. Through this virtualization technology, the network architecture of "core/aggregation switches + access switches + APs" can be virtualized into one device, which implements centralized, simplified management of devices, services, andusers.

- **Converged Policy: Unified Management of Wired and Wireless Users for Consistent Experiences**

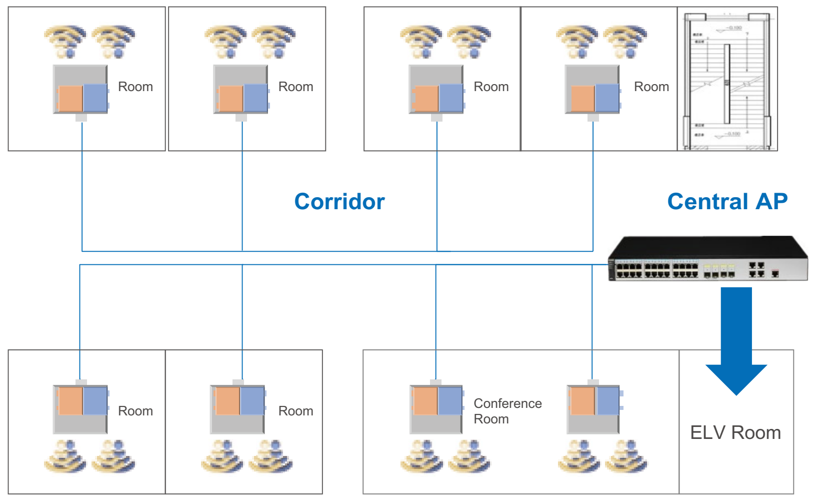
Separate wired and wireless authentication points on the traditional wireless campus network make it hard to centrally authenticate and manage users. With the native AC function of agile switches, Huawei's Agile Campus Network Solution centrally deploys wired and wireless access authentication points on agile cards of the agile switches, implementing unified user authentication and service management. Policy association between a user authentication point and a policy enforcement point is achieved through Control and Provisioning of Wireless Access Points (CAPWAP) tunnels between the agile switches and access switches. This simplifies configuration and maintenance of vast quantities of access switches. Unauthorized users cannot connect to the Layer 2 network, which guarantees network security. In addition, authentication point switches can be precisely aware of access devices, link status, user access locations, and ports, achieving fast fault troubleshooting and improving O&M efficiency.

Throughthe converged forwarding, management, and policy, the wired and wireless convergence solution implements centralized management of wired and wireless networks, optimizes user experiences, and simplifies network O&M.

2.2.1.3 All-Scenario Wi-Fi: Full Wireless Signal Coverage & Ubiquitous Access

Huawei provides an all-scenario Wi-Fi coverage solution for complex campus scenarios, such as indoor areas, high-density stadiums, outdoor scenarios, and dense rooms, ensuring high-density, ubiquitous WLAN coverage and guaranteeing high-quality user access experiences. For high-density coverage scenarios, taking stadiums as an example, by leveraging the industry's first 3D network planning tool, various high-density deployment methods, top-notch smart antenna technology, andmulti-user collision control technology, Huawei's solution completely eliminates Wi-Fi access experience degradation. Additionally, Huawei's all-scenario Wi-Fi solution has been commercially deployed at many stadiums across the globe.

For scenarios with a complex indoor structure, for example, student dormitories, hospital wards, hotel rooms, and conference rooms, Huawei has put forth a brand new Agile Distributed Wi-Fi Solution. An active Radio Frequency (RF) module is installed in each room, and is connected to a WLAN AP through cables. Comparedto traditional ways in which WLAN antennas are deployed in different rooms with feeders, Huawei's Agile Distributed Wi-Fi Solution features the followingadvantages:

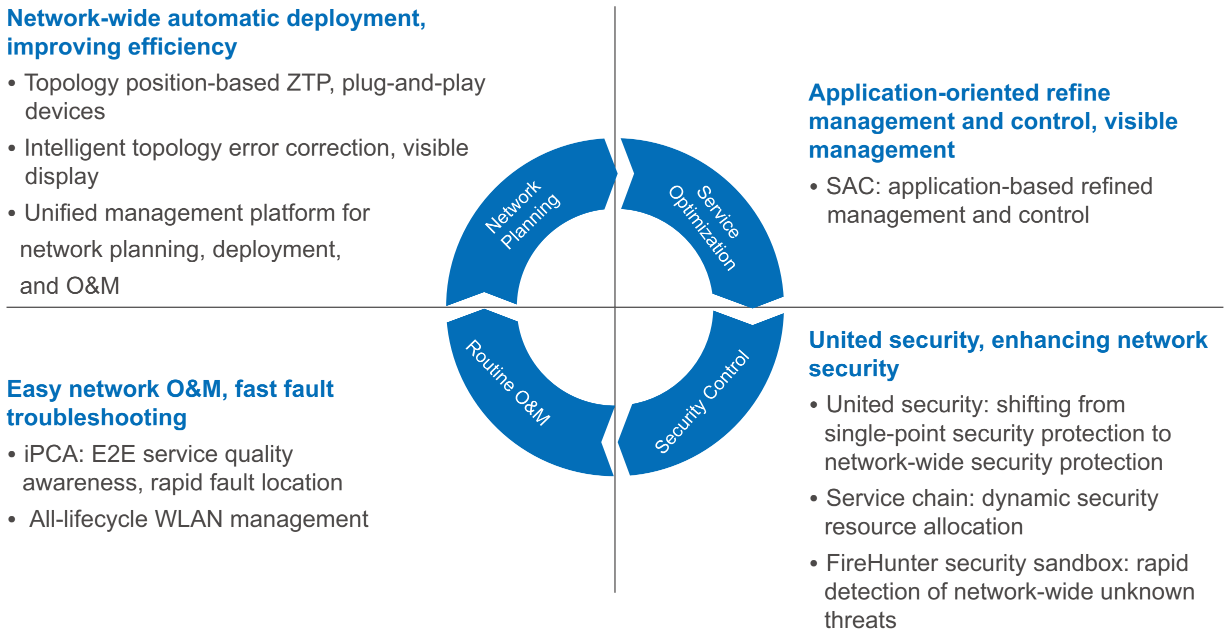


- Full coverage: Connects remote RF modules to the central AP through cables, providing better signal coverage without wall penetration or feeder loss.
- High service reliability: The central AP supports the link failure survival function, so that wireless user services remain uninterrupted when the link between the AP andACfails.
- Easy deployment and management: The central AP automatically manages remote RF modules, ensuring rapid deployment and convenient management.
- High Return on Investment (ROI): RF modules need no Agile Controller license, reducing the number of APs andensuring users a high ROI.

2.2.2 Agile O&M: Full-Lifecycle Campus Network Management, Lower TCO

With the rapid development of campus networks, the network size keeps scaling up. Particularly, the widespread use of new services such as the IoT, mobile office, and High Definition (HD) video conferences forces the network bandwidthandsize togo through explosive growth. However, network O&M labor force is rather limited, which brings about a huge challenge to customers.

Tohelp customers resolve this problem, Huawei introduces the concept of agile O&M. Huawei's agile O&M solution helps address challenges to O&M and management in different phases, from network planning and construction to service optimization, security control,and routine O&M, implementing full-lifecycle management of the entire campus network and substantially increasing O&M efficiency and lowering customer TCO.



Network-wide automatic deployment, improving efficiency

- Topology position-based ZTP, plug-and-play devices
- Intelligent topology error correction, visible display
- Unified management platform for network planning, deployment, and O&M

Application-oriented refine management and control, visible management

- SAC: application-based refined management and control

Easy network O&M, fast fault troubleshooting

- iPCA: E2E service quality awareness, rapid fault location
- All-lifecycle WLAN management

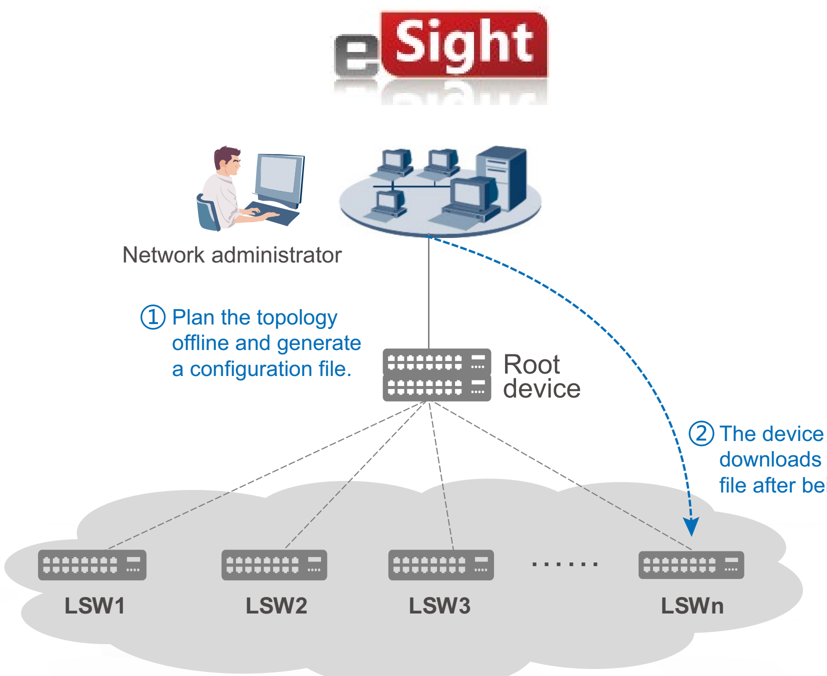
United security, enhancing network security

- United security: shifting from single-point security protection to network-wide security protection
- Service chain: dynamic security resource allocation
- FireHunter security sandbox: rapid detection of network-wide unknown threats

2.2.2.1 ZTP: Significantly Improving Device Deployment Efficiency

Traditional network deployment requires manual command lines or web management, and the devices must be configured onebyone. On large-sized campus networks, the workload of repeated manual configuration is heavy, and the manual configuration is often tedious and complicated. Some automatic configuration solutions are put forward by vendors in the industry in recent years. They can partially reduce the workload of device configuration, but two problems remain unresolved. First, network planning is separated from network deployment. When the network deployment results are inconsistent with the initial planning results, it is hard to detect the inconsistency in time. Second, these solutions must manually collect information such as theMAC address and Equipment Serial Number (ESN), so they cannot achieve fully automatic deployment.

Huawei's ZTP solution provides a unified network management platform — eSight Network Management System (NMS) platform, on which network planning, deployment, and O&M are integrated. After being powered on, devices can automatically obtain configuration files from the eSight based on the planned network topology. The devices are plug-and-play, significantly improving deployment efficiency.



① Plan the topology offline and generate a configuration file.

② The device automatically downloads the configuration file after being powered on.

- **Unified O&M Management Platform, Improving Management Efficiency**

  As a unified O&M management platform, the eSight centrally manages network planning, deployment, and O&M, thus reducing errors in network configuration management and improving O&M management efficiency.

- **Topology Location-Based, Plug-and-Play Devices, Improving Deployment Efficiency**

  After the network topology is planned on the eSight, configuration errors are visibly displayed by the eSightwhen the network deployment results are inconsistent with the network planning results.

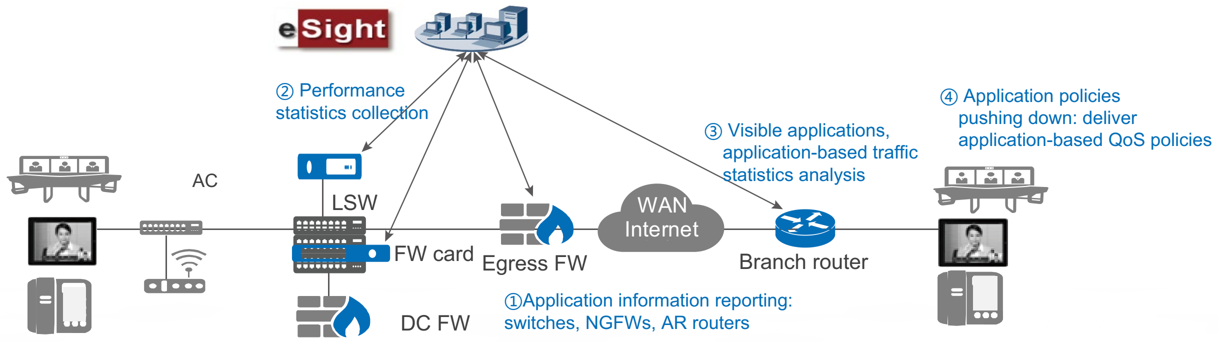
  After being powered on, the devices to be deployed automatically obtain configuration files from the eSight based on the topology location. The devices are plug-and-play, and require no onsite manual configuration. Even 1,000 devices can be deployed simultaneously, which accommodates the requirements on large campus network construction.

- **Unified Network Management and Maintenance, Lowering O&M Costs**

  After the device deployment is complete, the ZTP solution supports automatic backup of configuration files, automatic and zero-configuration replacement of faulty devices, and batch software version upgrades on the devices, thus lowering O&M costs.

2.2.2.2 SAC: Service-Oriented, Fine-Grained Management and Control

The rapid development of network andmultimedia technologies drives network applicationsto become increasingly diverse, which puts a strain on the network bandwidthresource. Network applications such as Point-to-Point (P2P) applications often "maliciously"consume network bandwidth, resulting in network congestion. Traffic of these applications also mixes with the business-critical traffic of enterprises. Traditional technology based on IP addresses or ports cannot accurately identify network applications. In addition, network administratorsareunableto learn about the accurate network usage status to guarantee the optimal experience for particular users andservices.


eSight
② Performance statistics collection
AC
LSW
FW card
DC FW
Egress FW
WAN Internet
③ Visible applications, application-based traffic statistics analysis
Branch router
④ Application policies pushing down: deliver application-based QoS policies
①Application information reporting: switches, NGFWs, AR routers

Tohelp customers overcome this challenge, Huawei provides its Smart Application Control (SAC) technology. Based on the analysis of packet headers, the SAC technology achieves application layer-based traffic inspection and control by identifying and analyzing the applicationlayer. By intelligently classifying variousapplications, identifying service types, and implementing fine-grainedQoS policy control, this technology restricts non-critical service traffic toensure smooth and highly efficient operations of critical business services. You can gain the following advantages from Huawei's SAC solution:

- **Powerful Application Identification Capability**

  Huawei's network devices deliver a powerful application identification capability, and Huawei's Next-Generation Firewall (NGFW) is able to identify more than 6,000 applicationsin a fine-grained fashion, implementing analysis of Layer 3 to Layer 7 protocols andapplications.

- **Visible Analysis Management**

  The network-wide, application-based statistical analysis results are centrally displayed on the eSightvia visible reports. TheeSight displays the application traffic distribution from multipledimensions such as users, devices, and areas, enabling rapid network adjustment andoptimization.

- **Application-Based, Fine-Grained Management and Control**

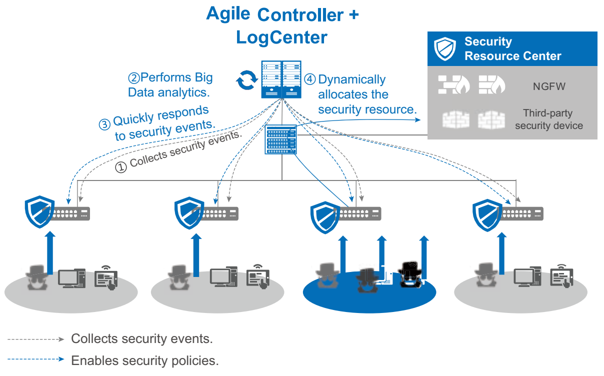
  The SAC solution implements fine-grained QoS management and control policies on service flows based on applications. For example, the solution limits the rate forapplication traffic, and adjusts bandwidthand priority to guarantee the quality of business-critical services.

  Take the wireless campus network as an example. Large numbers of users on the network utilize services that consume a lot ofbandwidth, such as BT, Emule, andonlinevideos. To control the traffic,network administratorscan accurately identify the traffic of variousapplicationsby deploying the SAC solution. Theycan also display the applications on the eSightthrough visible reports, thus improving network O&M efficiency.

2.2.2.3 United Security: From Single-Point Security Protection to Comprehensive Network Protection

After the mobile office work style and Wi-Fi networks are applied to enterprises, users of any role can access the campus network at any place using any device. In additionto the traditional Internet egress, multiple new network security threat sources including campus Wi-Fi access and remote access come into being. Approaches of hacker attacks and virus transmission become ever more diversified and complex. Security threats are borderless, security devices defend against attacks independently from each other, and deployment of security devices during network reconstruction is complex. As a result, traditional physical location-based single-point defense and border security protection ideas can no longer secure the campus network. Enterprises need to integrate and allocate security resources over the entire network to proactively detect threats and defend against attacks in a highly efficient, flexible, and full-scale manner.

In order to help enterprise users effectively secure their campus network, Huawei offers its Agile Campus Network Solution that leverages the Agile Controller, security resource center, and agile switches, as well as Big Data analytics and SDN concepts to integrate and schedule security capabilities on the entire network and implement united security. In the system architecture of Huawei' Agile Campus Network Solution, security monitoring points are ubiquitous on the network. The Agile Controller collects security events over the entire network, performs Big Data analytics, anddelivers security policies. Security functions are no longer subjectto constraints of physical locations. Security resources on the entire network can be used on demandby diverting suspicious traffic to the virtual security resource center.


Agile Controller + LogCenter
Security Resource Center
NGFW
Third-party security device
②Performs Big Data analytics.
④Dynamically allocates the security resource.
③ Quickly responds to security events.
① Collects security events.
Collects security events.
Enables security policies.

1. Collects security events on the entire network

Security events include network and security device logs, terminal user behavior logs, and abnormal traffic logs.

2. Performs Big Data analytics

The controller analyzes collected mass data and detects potential security risks.

3. Quickly responds to security events

Sends alarms in real time and recommends a response; flexibly delivers security policies and quickly responds to security events.

4. Dynamically allocates security resources

Carries out resource pooling of security devices on the entire network and dynamically allocates the security resource according to area, user group, and security event, significantly improving the security protection capabilities of the entire network.

▪ Big Data Analytics: Proactive Defense Againstand Quick ResponsetoAttacks

Integrating security behavior analysis software, the Agile Controller collects logs of various devices, records various security events on the network and, based on Big Data analytics, detects potential threats or attacks that single-point devices cannotdetect. O&M personnel can then "see" potential threats or attacks through an interaction interface. Administrators can adjust security policies to quickly respond to potential threats and attacks. The system can also generate various reports to display various security trends. By using Big Data analytics, security O&M personnel can detect potential threats in time, quickly respond toandprocess the potential threats, and prevent security incidents.

▪ Dynamic Allocation of Security Resources: On-Demand Invocation of Security Capabilities Without Physical Location Constraints

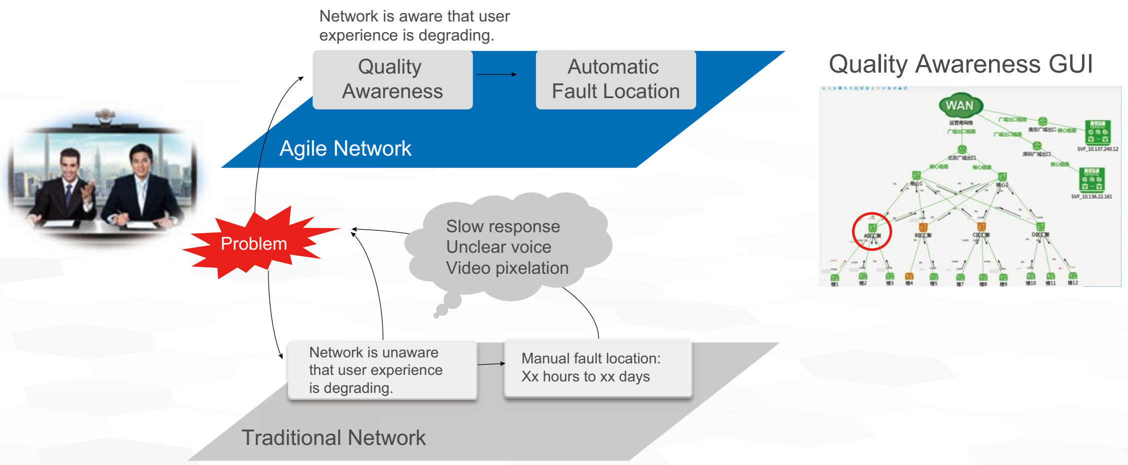
The Agile Controller flexibly invokes security capabilities such as firewall, online behavior management, and antivirus functions in the security resource center in the service orchestration mode. When security devices are virtualized into a security resource center, agile switches can flexibly invoke these security resources using tunneling technologies to protect service traffic as long as the network is reachable. In this manner, deployment anduse of security devices will not be subjectto constraints of physical locations. Security capabilities of the entire network will be quickly released. Security protection for service traffic and effective defense response after security event detection will not be subjectto live network constraints. No additional security device needs to be purchased, which reduces customers' Capital Expenditure (CAPEX).

▪ Prevention of Unknown Threats and APT Attacks: Industry-Leading Unknown Malware Detection Capability

Advanced Persistent Threats (APTs) tend to take advantage of phishing emails or IoT device vulnerabilities. By usinga variety of technologies, APTs are combined into unknown malware. By passing the existing signature detection-based security devices, APTs can achieve the goal of data theft or damage. Huawei provides the next-generation industry-leading high-performance APT detection solution. This solution deploys Huawei's FireHunter sandbox and NGFW at key positions such as the Internet egress, Demilitarized Zone (DMZ) border, intranet core border, and other data center egresses. The NGFW enables traffic filtering and file restoration for interactions between the intranet and extranet. In addition, the NGFW submits suspicious files to the FireHunter sandbox, detects malicious behavior for suspicious files at multiple levels and from multiple dimensions,and then feeds back the detection results. The solution allows larger-scale malware and attack detection through multi-node deployment, and collaborates with LogCenter to achieve APT threat alarming and network-wide security status awareness. Therefore, the solution prevents unknown threats from spreading rapidly, as well as avoiding core information assets losses.

2.2.2.4 Routine O&M: Service Quality Awareness, Controlling All Elements That Affect Service Experiences

On traditional networks, reasons for service quality degradation are often hard to locate due to a lack of effective service quality detection and troubleshooting methods. Huaweiuses its unique, patented service quality awareness technology Packet Conservation Algorithm for Internet (iPCA) to color and count real service packets at nodes where sensitive data service flows are sent, such as the network ingress, IP phones, and IP cameras. TheiPCA technology also performs correctstatistics collection and counting on the colored packets at the network egress, monitors the service quality, locates potential fault points and visibly displays them on the NMS interface. The NMS then notifies network administrators of the potential fault points. In this way, Huawei's iPCA technology completely addresses the problem of difficult IP network experience guarantees.


Network is aware that user experience is degrading.
Quality Awareness
Automatic Fault Location
Agile Network
Quality Awareness GUI
WAN
Problem
Slow response
Unclear voice
Video pixelation
Network is unaware that user experience is degrading.
Manual fault location: Xx hours to xx days
Traditional Network

- **Zero Traffic Cost, Real-Time Quality Detection, and Precise Fault Location**

Huawei's iPCA technology generates no additional performance or traffic cost. This technology enables data flows between users to have network quality awareness capabilities while transmitting services by marking, coloring, and counting real service packets. No additional detection packet needs to be inserted, so services remain uninterrupted. Network quality can be detected in real time, and network faults can be located to a network segment, a link, or even devices such as particular IP cameras, IP phones, and switches.

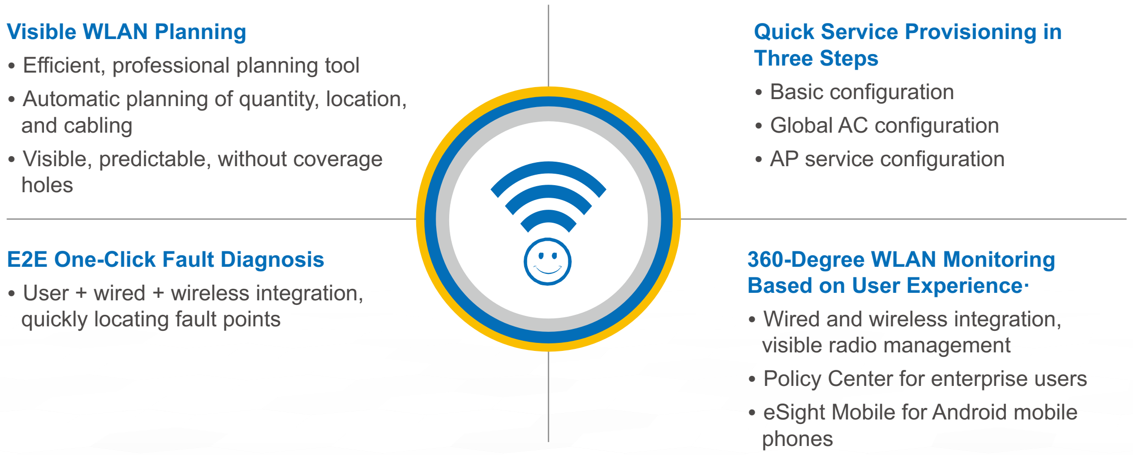
- **MIMO-Based Measurement and Adaptabilityto Networks of Any Scale**

The industry's first Multiple-Input Multiple-Output (MIMO) quality monitoring technology, it canmonitor communications among multiple nodes without resulting in the N2problem. This technology supports Point-to-Multipoint (P2MP) and Multipoint-to-Multipoint (MP2MP) networking, as well as cross-network End-to-End (E2E) detection. This technology solves problems in network measuring in scenarios with multi-path and multi-directional service flows without limiting the network typeandsize. The scenarios includedual-homing, port binding, load balancing, and Layer 2 and Layer 3 E2E network measuring. Network scale is not limited, and no problems exist in connecting third-party devices.

- **Service-Oriented E2E Service Quality Detection**

If the quality of IP phone call or video surveillance is poor in scenarios such as safe cities, rail transport, or emergency command and dispatch, Huawei's iPCA technology performs E2E service quality monitoring, starting withmultimediaterminals. In addition, this technology enables a quick search for the service flow path through the eSight's route selection function. Through the hop-by-hop service quality detection technology, network faults can be precisely located. All these guarantee E2E, service-oriented, precise quality detection and rapid fault location.

2.2.2.5 Routine O&M: Full-Lifecycle Wireless Campus Management



Visible WLAN Planning
- Efficient, professional planning tool
- Automatic planning of quantity, location, and cabling
- Visible, predictable, without coverage holes

Quick Service Provisioning in Three Steps
- Basic configuration
- Global AC configuration
- AP service configuration

E2E One-Click Fault Diagnosis
- User + wired + wireless integration, quickly locating fault points

360-Degree WLAN Monitoring Based on User Experience·
- Wired and wireless integration, visible radio management
- Policy Center for enterprise users
- eSight Mobile for Android mobile phones

Costs of wireless campus network maintenance are much higher than that of wired campus network maintenance. First, large numbers of WLAN APs leadto an increasing number of network nodes. Second, signals are apt to be reflected and attenuated because WLAN signals are transferred in the air, and campus buildings may block the signals. Third, some users may be unableto connect to the WLAN when user distribution is uneven due to innate characteristics of the WLAN.

The full-lifecycle wireless campus management allows smart, automatic WLAN access provisioning, routine network monitoring, and troubleshooting. Network administrators canhelp intranet users easily gain the best service experience.

- **Visible WLAN Planning: Dedicated Tool Ensures Rapid, Accurate, and Simple Network Planning**

Integrating professional network planning software, Huawei's NMS enables simple, highly efficient, and visible network planning, shortening the network construction time by 30 percent and reducing the number of network O&M problems by 20 percent.

- **Agile Configuration: Provisioning Wi-Fi Access in Only Three Steps**

Huawei's highly efficient agile configuration solution allows users to complete the WLAN deployment in only three steps. The solution accelerates Wi-Fi access provision, bringing a 10-fold boost in work efficiency.

- **Daily Monitoring: User Experience-Based, 360-Degree Network Monitoring**

Huawei's NMS canobtainindicators such as the user access rate, access success rate, and disconnection rate. Through Big Data analytics, the NMS figures out the network health degree, and provides root causesand troubleshooting suggestions foranomalies, implementing user experience monitoring.

- **Quick Troubleshooting: Mobile O&M, Fast Network Fault Diagnosis**

If users cannot connect to the network, Huawei's NMS can quickly locate the fault. The NMS then diagnoses the fault from multipledimensions such as terminals, air interfaces, APs, ACs, connectivity, Authentication, Authorization and Accounting (AAA), and Dynamic Host Configuration Protocol (DHCP). In addition, the NMS can provide Key Performance Indicators (KPIs) and troubleshooting suggestions. After installing the eSight Mobile O&M inspection tool on smartphones, network administrators are able to detect the WLAN coverage anywhere, anytime. The eSight Mobile is aware of user

2.2.3 SDN,Openness & Cooperation,Achieving Rapid Service Innovation

Nowadays, criticalissues confronting the development of enterprises are how to enable enterprise ICT systemstobe advantageous when compared tosimilar products from competitors, how to provide networkswith the evolution ability, and how to rapidly introduce new services andfeatures.

In recent years, the network industry has set off a wave of Soft defined Network (SDN) technology to enable the network to be more intelligent and convenient forservices. There have been various techniques and viewpoints about SDN in the industry, such as the forwarding and control plane separation led by Open Networking Foundation (ONF), the centralized management and control architecture, the open programmable architecture represented by the southbound OpenFlow protocol and led by Internet Engineering Task Force (IETF), and the overlay architecture widely used in data centers. When it comes to campus networks, users expectto solve problems such as complex campus policy configuration and management and difficult openness of campus network capabilities using SDN technology. Huawei's Agile Campus Network Solution addresses these problems through centralized policy control, full-layer openness and cooperation, and full programmability. Therefore, the solution assists enterprise customers in saving O&M costsand achieving rapid service innovations.

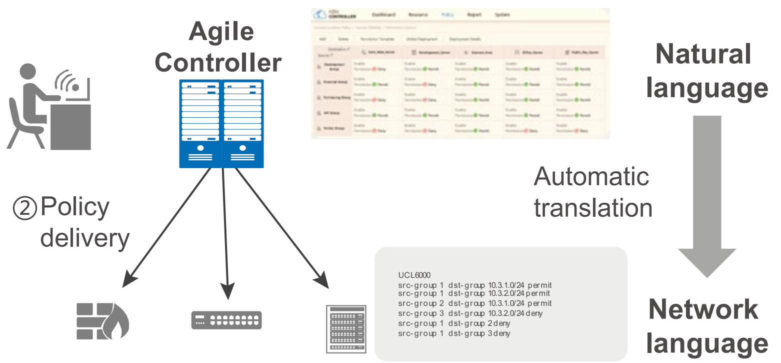
2.2.3.1 Centralized Policy Control: Implementation of SDN in Campus Networks

On a campus network, a large number of policies such as ACL, security, andQoS policies must be deployed. If these policies are configured on network devices onebyone, the workload is rather heavy.To make the matter worse, user locations frequently change in the mobile office era. How can enterprises tackle this challenge by leveraging SDN?

Huawei introduces the Agile Controller into campus networks, implementing the SDN's centralized control concept and achieving network-wide centralized policy control. Network administrators only need to configure policies that arerelated to servicesandrights on the Agile Controller. The Agile Controller automatically translates service policies into command lines on network devices anddelivers them to the corresponding policy enforcementdevices. This implements automatic policy deployment, ensures network-wide policy and service experience consistency, and substantially simplifies campus network O&M and management.

Automatic Network Policy Deployment Based on SDN's Centralized Control Concept

①Natural language-based policy definition and Agile Controller-based automatic translation

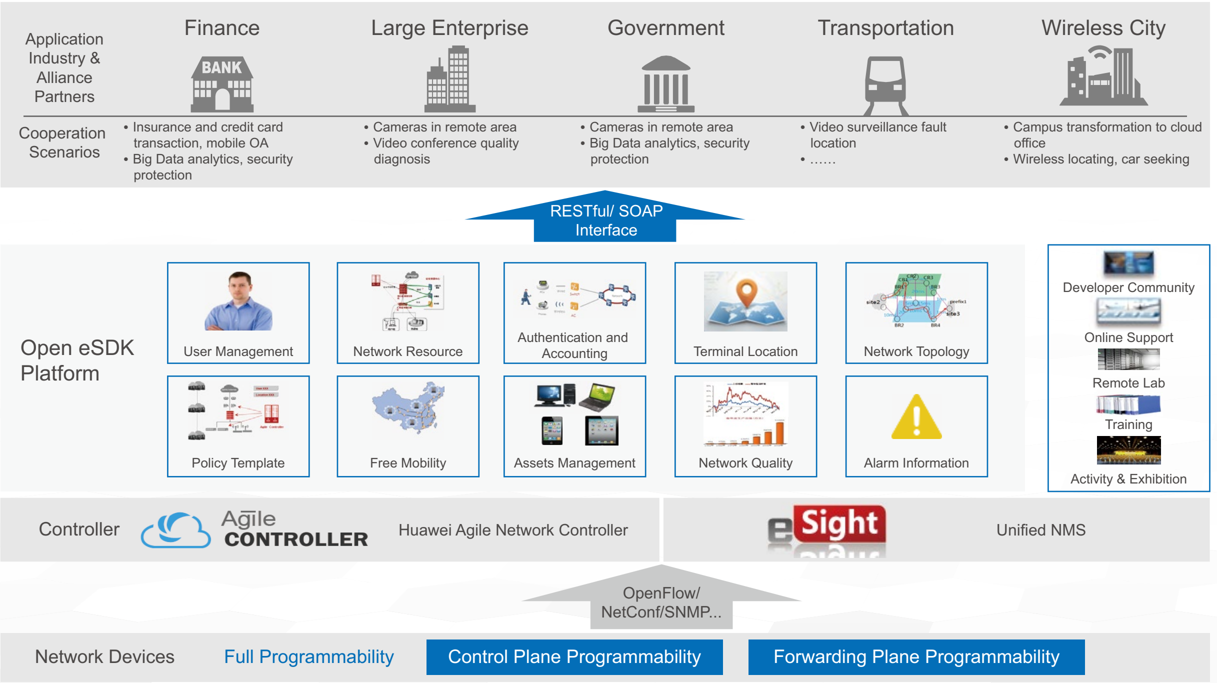


```
UCL6000
src-group 1  dst-group 10.3.1.0/24 permit
src-group 1  dst-group 10.3.2.0/24 permit
src-group 2  dst-group 10.3.1.0/24 permit
src-group 3  dst-group 10.3.2.0/24 deny
src-group 1  dst-group 2 deny
src-group 1  dst-group 3 deny
```

- Natural language-based policy configuration, easy-to-use
- Unified network policy planning and one-click deployment

2.2.3.2 All-Layer Openness & Cooperation: Co-Building a Value-Added Ecosystem

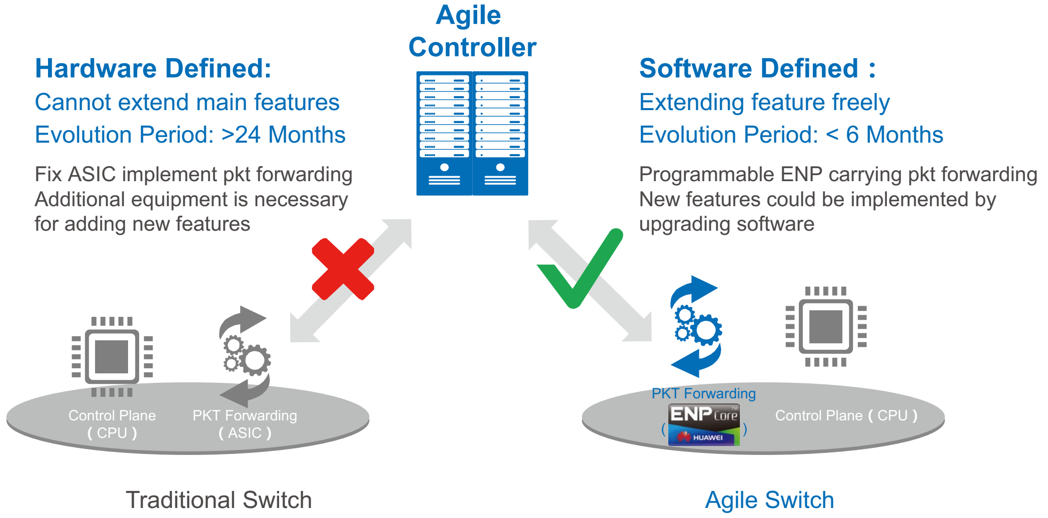
Through open interfaces of Huawei's Ecosystem Software Development Kit (eSDK), Huawei's Agile Campus Network Solution makes various information includingthe user identity, network resource, device location, and network topology open toupper-layerservices. Through these open, standard interfaces, third parties can customize service andapplication systems based on their own service demands in different sectors, such as finance, manufacturing, government, intelligent transportation, and wireless city. Huawei aims at building a value-added ecosystem and establishing a win-win partnership with its partners through openness and cooperation with the Agile Campus Network Solution.



For example, on a startup company office campus, Huawei connects its Agile Campus Network Solution to third-party service systems, allowing entrepreneurs and companies that rent the office zone to apply for ICT resources at any time. Services can be provisioned viaoneclickand automatically delivered. The services of different companies can be isolated from each other, and are thus highly secure. Differing from the traditional infrastructure operation model, this new operation model enables users to migrate their IT and network resources on demand.

2.2.3.3 Fully Programmable: Enabling Networks to Evolve from Being Hardware-Defined to Software-Defined

The fully programmable architecture is a unique enhanced architecture of Huawei's agile network. The core of this architecture is ENP + Protocol Oblivious Forwarding (POF). Based on Huawei's self-developed ENP chips, devices' forwarding function can evolve to the future standards. When a new function must be added to switches using ASIC chips, customers have to replace the old devices because the ASIC chips are non-programmable. Additionally, to implement a new function, customers have to wait for a long time period (standards -> chips -> devices). After deploying agile switches using Huawei's ENP chips, customers can self-define devices' forwarding behavior on the Agile Controller, greatly reducing time for provisioning new functions and services and enabling networks to be SDN-ready.


Agile Controller
Hardware Defined:
Cannot extend main features
Evolution Period: >24 Months
Fix ASIC implement pkt forwarding
Additional equipment is necessary for adding new features
Software Defined :
Extending feature freely
Evolution Period: < 6 Months
Programmable ENP carrying pkt forwarding
New features could be implemented by upgrading software
Control Plane (CPU)
PKT Forwarding (ASIC)
PKT Forwarding
ENP Core
HUAWEI
Control Plane (CPU)
Traditional Switch
Agile Switch

Huawei's agile switch is the first to implement full programmability in both control and forwarding planes, which allowsconvenient provisioning of new services and functions and is software-defined in the real sense. Huawei's Agile Campus Network Solution helps enterprise users easily introduce new functions in software-defined mode, four times faster than the industry average, and stay ahead of competition.

Thanks to the fully programmable architecture, openness, and cooperation, Huawei's Agile Campus Network Solution achieves rapid expansion of network functionalityin a software-defined manner. It is the first solution to directly deploy SDN on campus networks, implementing ubiquitous service innovations.

03

Customer Benefits

Huawei's Agile Campus Network Solution accommodates enterprises' future network requirements: concentration on users, automatic network resource deployment, automatic fault location, and fine-grained network management.

This solution eliminates many tricky problems:

- Lack of experience guarantees
- Low-efficiency deployment
- Single-point security protection
- Slow response to threats and attacks
- Video pixelation, unclear voice, slow network access, and poor remote office and mobile office experiences

The Huawei solution also permits campus enterprise networks to quickly adapt to new services and build a service-friendly network architecture. The solution proactively enables service quality awareness, network optimization, software-defined provisioning of new services, and rapid service evolution.

The ultimate goal of Huawei's Agile Campus Network Solution is tohelp enterprise users enjoy convenient, high-quality communications without any constraints brought about by distance andto enable communication between people and devices and the seamless transfer of information.

04

Why Huawei?

Huawei is proudly backed by over 20 years of experience in the IP field and an outstanding series of network products andsolutions. Recognized as a leading global network solutions provider, Huawei has an excellent long-term strategy for network development and is steadfast in its investment in the network field. Moreover, Huawei's world-class research capabilities and experts offer unparalleled experience in the areas of network standards and chip development.

As a member of over 170 international standardization organizations, for example, IEEE, IETF, ONF, ETSI, and CCSA, Huawei contributes to areas of standards research, product development, and customization capability improvement. Huawei also remains committed to providing smart, programmable, and open networks through its accumulated carrier-grade network experience and innovative products andsolutions.

For more information about Huawei Enterprise ICT Solutions, visit http://e.huawei.com.