One Net

Huawei Technology Campus Network Solution

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

1. Introduction

A technology campus consists of the administrative committee, enterprises, universities, and scientific research institutions. For example, high-tech industrial parks, science and technology parks, science parks, and software parks are technology campuses. Enterprises in the technology campus are mainly intelligence-intensive enterprises and technology campus information affects its development. The administrative committee in the technology campus hopes to attract more enterprises and organizations by providing better Internet services. With rich experiences and practices in campus network construction, Huawei provides a complete array of network solutions.

2. Challenges and Development Trends on the Technology Campus Network

2.1 Challenges

As the enterprise service develops, the enterprise network transforms from a traditional wired Local Area Network (LAN) into a ubiquitous service network. This allows branches, residential users, and traveling staffs to access the enterprise network anytime and anywhere.

In the era of the Internet of Things, the technology campus networks transform from IT dedicated networks to enterprise-oriented Internet of Things to connect numerous diversified terminals. Enterprise services, including services on monitors, door control platforms, and meters, develop extensively.

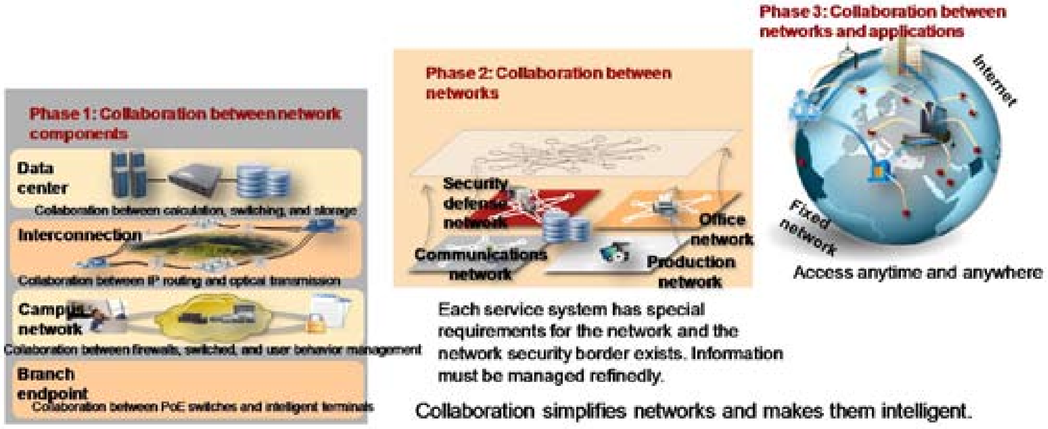
Service diversity imposes new requirements on network quality and security. Networks are no longer "pipes", but provide various services.

Information realtimeness, disaster recovery, and multi-channel sharing require information centralization.

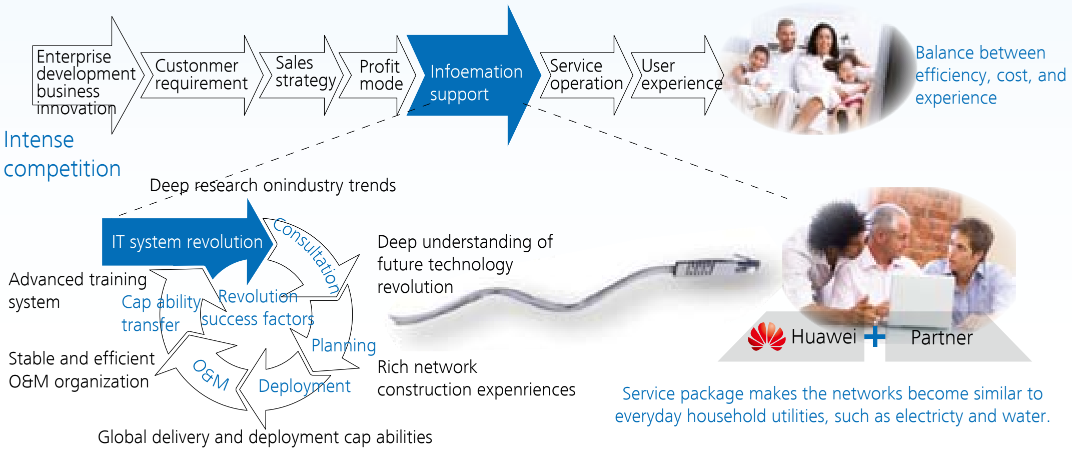
How to maintain the complex ICT systems with limited manpower and maintenance capability is a major concern of enterprises and the administrative committee. Campus networks must be easy to maintain.

2.2 Development Trends

Collaboration: Collaboration between networks, network components, and networks and applications simplifies networks and makes them intelligent.


Phase 1: Collaboration between network components
Data center
Collaboration between calculation, switching, and storage
Interconnection
Collaboration between IP routing and optical transmission
Campus network
Collaboration between firewalls, switched, and user behavior management
Branch endpoint
Collaboration between PoE switches and intelligent terminals
Phase 2: Collaboration between networks
Security defense network
Office network
Communications network
Production network
Each service system has special requirements for the network and the network security border exists. Information must be managed refinedly.
Phase 3: Collaboration between networks and applications
Internet
Fixed network
Access anytime and anywhere
Collaboration simplifies networks and makes them intelligent.

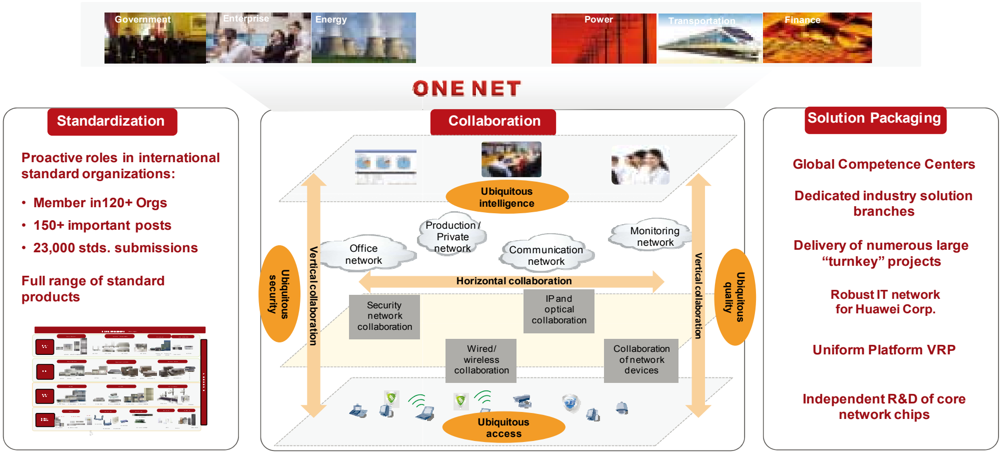
Service package: Enterprise development and business mode innovation depend on information platforms. Integrated services balance network construction costs, efficiency, and experience for users. The networks become similar to everyday household utilities, such as electricity and water.


Enterprise development business innovation
Custonmer requirement
Sales strategy
Profit mode
Infoemation support
Service operation
User experience
Balance between efficiency, cost, and experience
Intense competition
Deep research onindustry trends
IT system revolution
Consultation
Revolution success factors
Cap ability transfer
Planning
Deployment
O&M
Advanced training system
Stable and efficient O&M organization
Deep understanding of future technology revolution
Rich network construction expenriences
Global delivery and deployment cap abilities
Huawei + Partner
Service package makes the networks become similar to everyday household utilities, such as electricty and water.

2.3 Huawei One Net Solution

Huawei ONE NET solution is an enterprise network solution that features standardization, collaboration, and integrated services. It provides the following benefits:

- Integrates products, schemes, and services, and provides a basic network platform for industrial applications.
- Provides all-round collaboration solutions for enterprise users across networks, network components, and applications in various application scenarios, based on open protocols. To meet diversified requirements, Huawei works with partners to provide end-to-end integrated network construction services for customers.
- Simplifies networks and provides the optimal experience for users, based on standardized products, all-round collaboration solutions, and integrated services.


Government
Enterprise
Energy
Power
Transportation
Finance
ONE NET
Standardization
Proactive roles in international standard organizations:
• Member in120+ Orgs
• 150+ important posts
• 23,000 stds. submissions
Full range of standard products
Collaboration
Ubiquitous intelligence
Office network
Production / Private network
Communication network
Monitoring network
Horizontal collaboration
Security network collaboration
IP and optical collaboration
Wired/ wireless collaboration
Collaboration of network devices
Ubiquitous access
Ubiquitous security
Vertical collaboration
Vertical collaboration
Ubiquitous quality
Solution Packaging
Global Competence Centers
Dedicated industry solution branches
Delivery of numerous large "turnkey" projects
Robust IT network for Huawei Corp.
Uniform Platform VRP
Independent R&D of core network chips

This document describes the following technology campus solutions:

Basic network solution

Virtual solution

- Horizontal virtualization
- Vertical virtualization
- Network isolation between enterprises
- Data access solution between enterprises

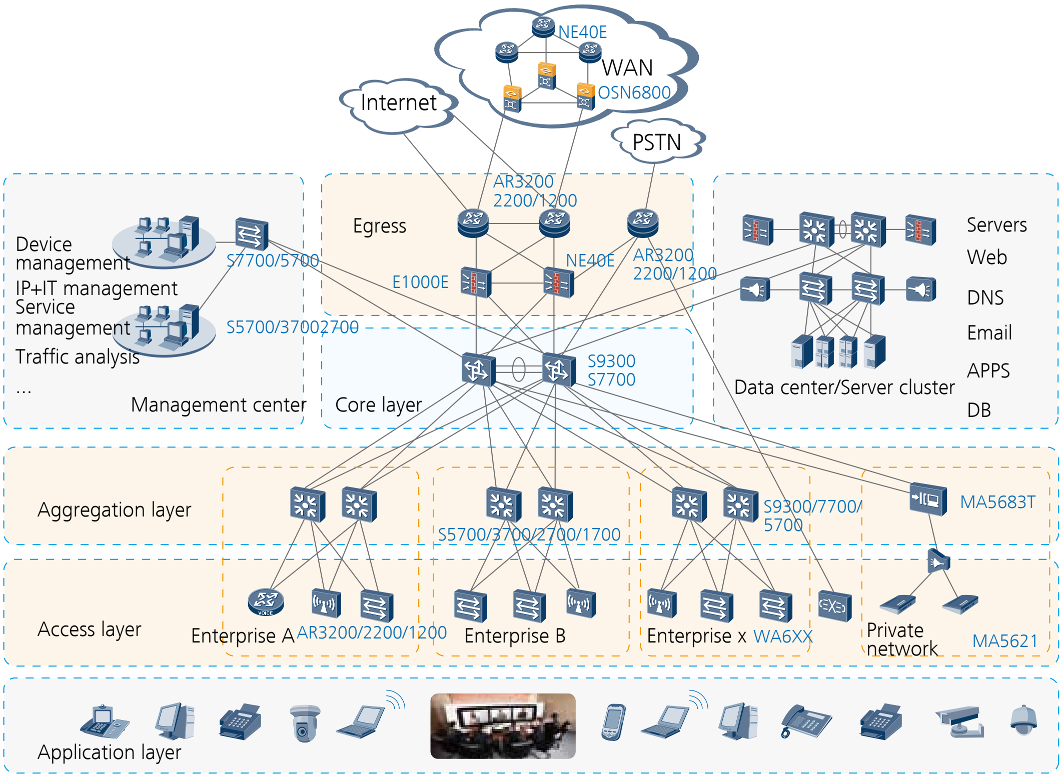
Security solution

Wireless solution

Voice and UC communication solution

3. Basic Network Solution of the Technology Campus Network

Generally, technology campus networks are high-density non-operation networks crowded with numerous terminals and users. Reliability, deployment, and maintenance of campus networks are of utmost importance. Technology campus networks often use star topologies. Based on the open network architecture, hierarchical networking, and modular design, enterprises can select Layer 2 or Layer 3 architecture and use appropriate application modules based on the enterprise scale. The technology campus network connects to external networks through the Internet, PSTN, or WAN.



Application layer

This layer contains terminals, including computers, laptops, printers, fax machines, Plain Old Telephone Service (POTS) phones, Session Initiation Protocol (SIP) phones, mobile phones, and cameras.

Access layer

This layer contains the devices that connect terminals to campus networks, for example, Ethernet switches. Some terminals, such as Access Points (APs) and IADs, need dedicated access devices.

Aggregation layer

This layer contains access devices and users and connect them to the core layer. This layer allows a large number of users to access the core layer. On some campus networks, the Layer 3 gateway is deployed at the aggregation layer to function as a L2/L3 edge device. The Layer 3 gateway at this layer is responsible for user management, QoS scheduling.

Core layer

This layer is only responsible for high-speed connections on a campus network, but does not process user services. The core layer improves bandwidth use efficiency and speeds up route convergence.

Campus egress

The egress connects the campus network to the public network. Internal users and external users (such as customers, partners, branch network users, and remote access users) of the campus network communicate with each other through the egress.

Data center/Server cluster

The data center zone or server cluster contains servers and application systems that provide data and applications for users.

Network management zone

This zone manages networks, servers, and application systems. It mainly provides functions of fault management, configuration management, performance management, and security management.

Solution characteristics:

- The star topology uses the core node as the root to ensure a stable architecture, which facilitates expansion and maintenance.
- Each module corresponds to a department or functional system and has its responsibilities. Network topology changes in a department do not affect other departments. This facilitates fault location.
- The dual-node redundancy design and trunk links improve network reliability.
- All types of terminals can access the campus network, and the IP network transmits all services.
- Branches, remote employees, partners, and external users can access the technology campus network.

4. Virtual Solution of the Technology Campus Network

To implement horizontal and vertical virtualization, the technology campus network uses CSS, stack, Eth-Trunk, and MPLS VPN at the core layer, aggregation layer, and access layer. This prevents Layer 2 loops on the traditional enterprise network, ensures reliability, and isolates services of different departments of an enterprise.

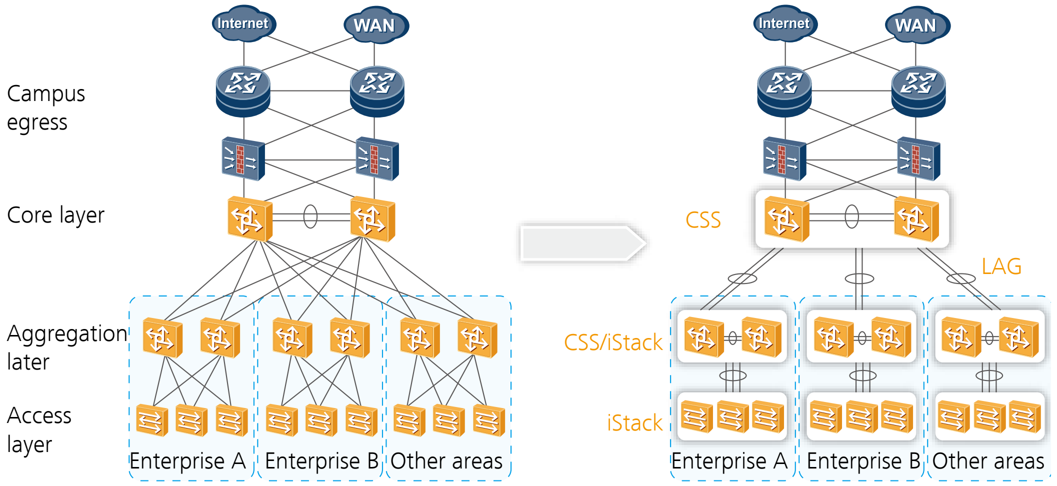
4.1 Horizontal Virtualization

1) Network Requirements

The core layer of a technology campus network or an enterprise requires high reliability, scalability, and forwarding capability.

2) Solution

Horizontal virtualization uses the CSS or stack technology at the core layer, aggregation layer, and access layer of the campus network to virtualize multiple physical devices into a single logical device. It simplifies the network structure and protocol deployment and improves network reliability and manageability.



3) Solution Characteristics

- Simplified deployment: Horizontal virtualization changes the mesh topology into a tree topology, where network layers are connected by a link aggregation group (LAG). Using this solution, you can prevent loops without deploying cumbersome protocols like MSTP and VRRP.
- Routing optimization: CSS and stack technologies change the campus network topology into a loop-free and tree topology, which reduces the operation and maintenance workload. You can clearly view the transmission path where service traffic passes. Expansion of each stack or cluster node does not change the network architecture or communication between upper- and lower-layer networks.
- Simplified management: Horizontal virtualization virtualizes multiple physical devices into a logical device, which simplifies device management.

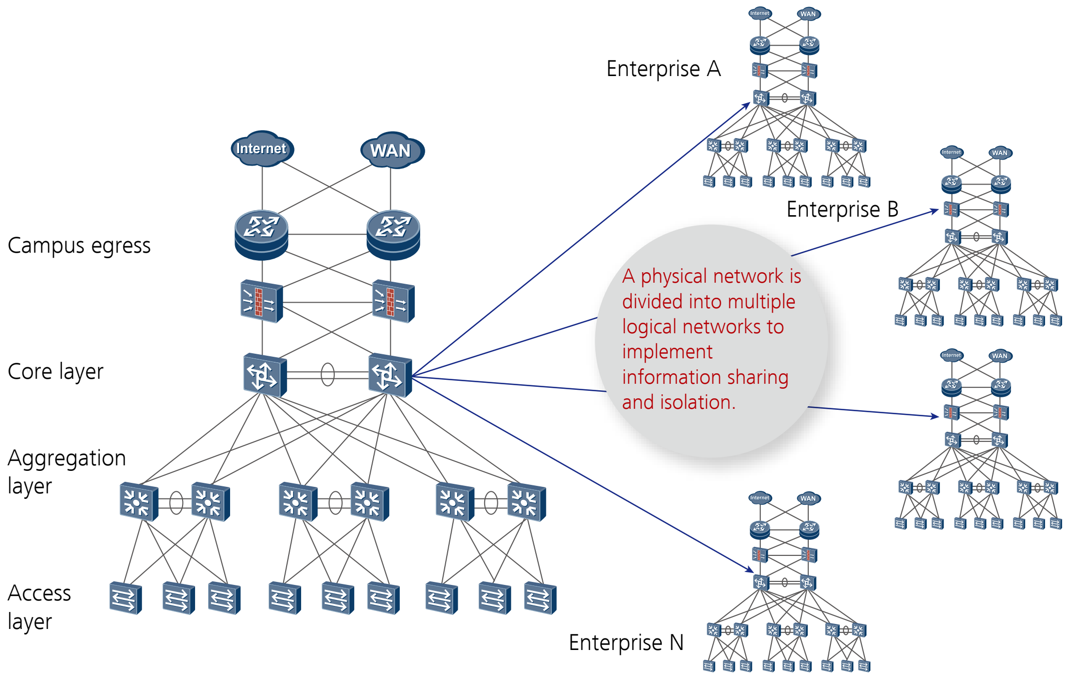
4.2 Vertical Virtualization

1) Network Requirements

Enterprise services need to share physical resources and be isolated securely.

2) Solution

Users or services may use different resources, security policies, and management policies. Vertical virtualization virtualizes the shared resources, including hardware devices and application services, into multiple sets of logical resources for different groups or services.


Enterprise A
Internet
WAN
Campus egress
Core layer
Aggregation layer
Access layer
Enterprise B
A physical network is divided into multiple logical networks to implement information sharing and isolation.
Enterprise N

3) Solution Characteristics

- Access control: ensures that access users are reliable and secure.
- Logical service isolation: isolates services of users with different privileges and allows certain users to communicate with each other.
- Resource isolation: controls users' access permission to network resources.

4.3 Network Isolation Between Enterprises

1) Network Requirements

A technology campus network transmits enterprise office services, production services, and sales services. An enterprise has high requirements for reliability, security, scalability, and performance on the technology campus network. They also require that access between different departments and resource access rights of departments are limited. This solution uses VLAN, ACL, and VPN technologies to isolate network resources. It simplifies network complexity and maintenance.

2) Solution

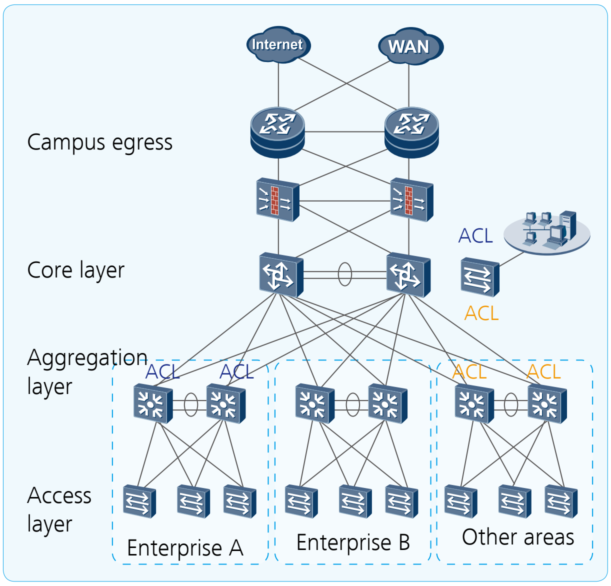
VLAN+ACL

A physical LAN is divided into multiple logical broadcast domains, multiple VLANs. Devices in a VLAN can directly communicate with each other, whereas devices in different VLANs cannot communicate directly. VLAN technology enables users to share resources on the physical LAN and ensures Layer 2 isolation.

The VLAN technology implements Layer 2 isolation. ACLs are deployed at the Layer 3 edge and data area edge to isolate Layer 3 services. Policies are configured based on service requirements to control access between enterprises.

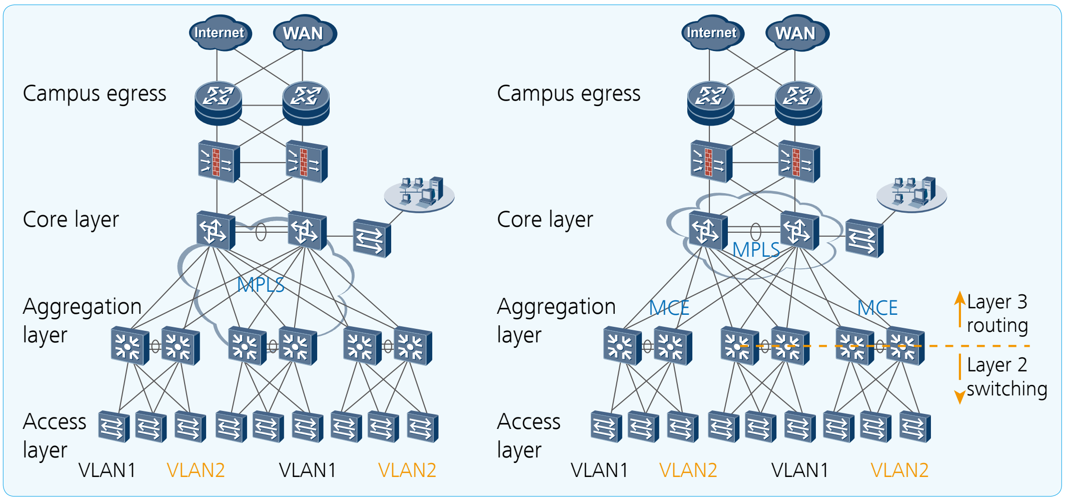
The VLAN and ACL technologies have the following advantages:

- Easy deployment (it is applicable to small-scale campus networks)
- Low requirements for network device functions, which reduces purchase costs



MPLS VPN+VLAN or MPLS VPN+MCE+VLAN

MPLS L3VPN networking is flexible and extensible, and MPLS VPN supports MPLS QoS and MPLS TE. It often works with MCE at the aggregation layer to isolate services.



MPLS VPN+VLAN or MPLS VPN+MCE+VLAN has the following advantages:

- High resource usage efficiency, powerful extensibility, a large number of VPNs, and easy VPN expansion(it is applicable to large- or mid-scale campus networks)
- Service isolation using private routes, simplified architecture, and easy maintenance
- Flexible access control policies and flexible networking, such as extranet networking and hub-and-spoke networking, to meet the requirements for isolation of various services

4.4 Data Access Solution Between Enterprises

1) Network Requirements

Enterprises often access data centers leased by the technology campus. Access rights of enterprises need to be isolated.

2) Solution

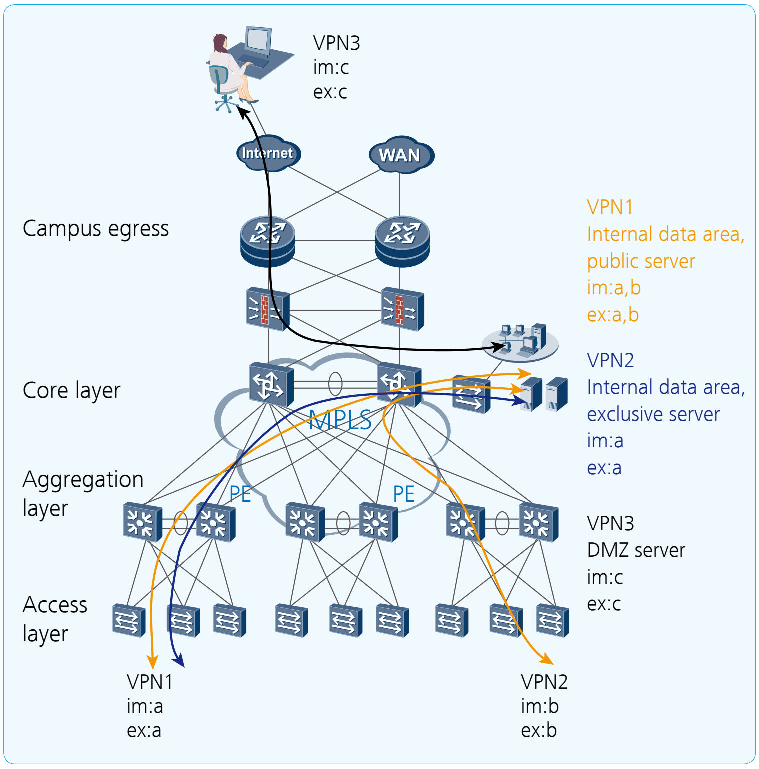
Data center servers are classified into the following types:

Public server: provides public application services for different enterprises or user groups of different security levels.

Exclusive server: provides exclusive application services for an enterprise or user groups of the same security level.

DMZ server: provides value-added services such as web services and email services for Internet users.

MPLS L3VPN uses RT attributes to control route advertisement and selection. This makes networking flexible. VLANs can also be used to isolate services.



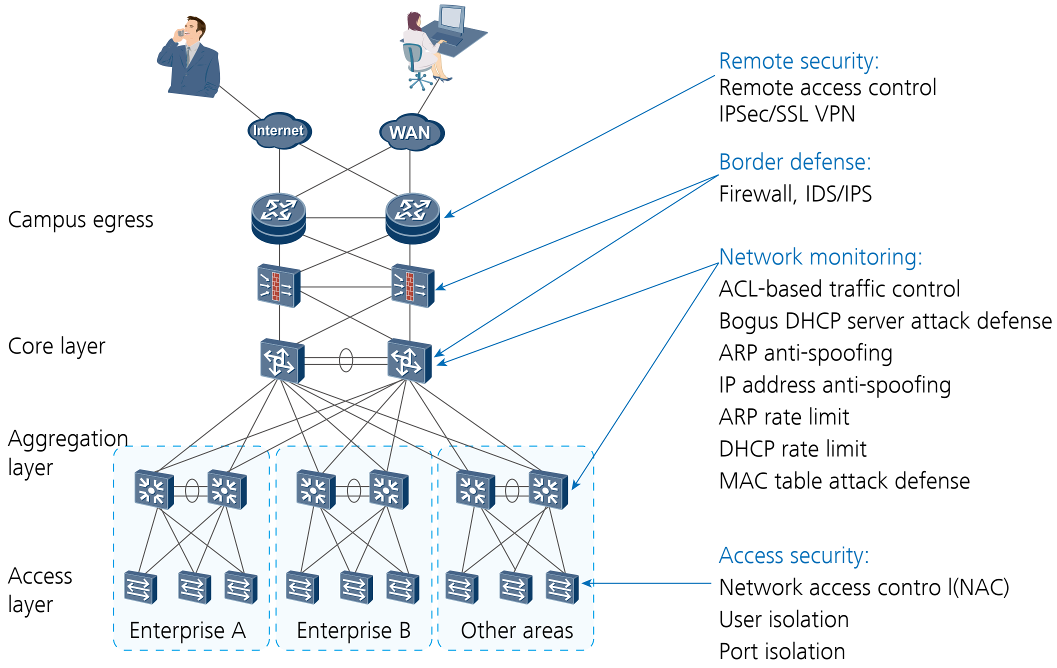
3) Solution Characteristics

Isolation by making full use of data center resources

Flexible deployment by using servers in different scenarios and advertising MPLS VPN routes

5. Security Solution of the Technology Campus Network

The technology campus network has potential security risks from spams, hacker attacks, and worms. The security solution ensures security for the Internet egress, technology campus, and remote access using an integrated network platform.



Remote security:
Remote access control
IPSec/SSL VPN

Border defense:
Firewall, IDS/IPS

Network monitoring:
ACL-based traffic control
Bogus DHCP server attack defense
ARP anti-spoofing
IP address anti-spoofing
ARP rate limit
DHCP rate limit
MAC table attack defense

Access security:
Network access contro l(NAC)
User isolation
Port isolation

Solution characteristics:

Edge security: isolates services or controls user access on the campus egress, physical partition, and service partition.

User behavior management: monitors user behaviors, and optimizes and controls user network.

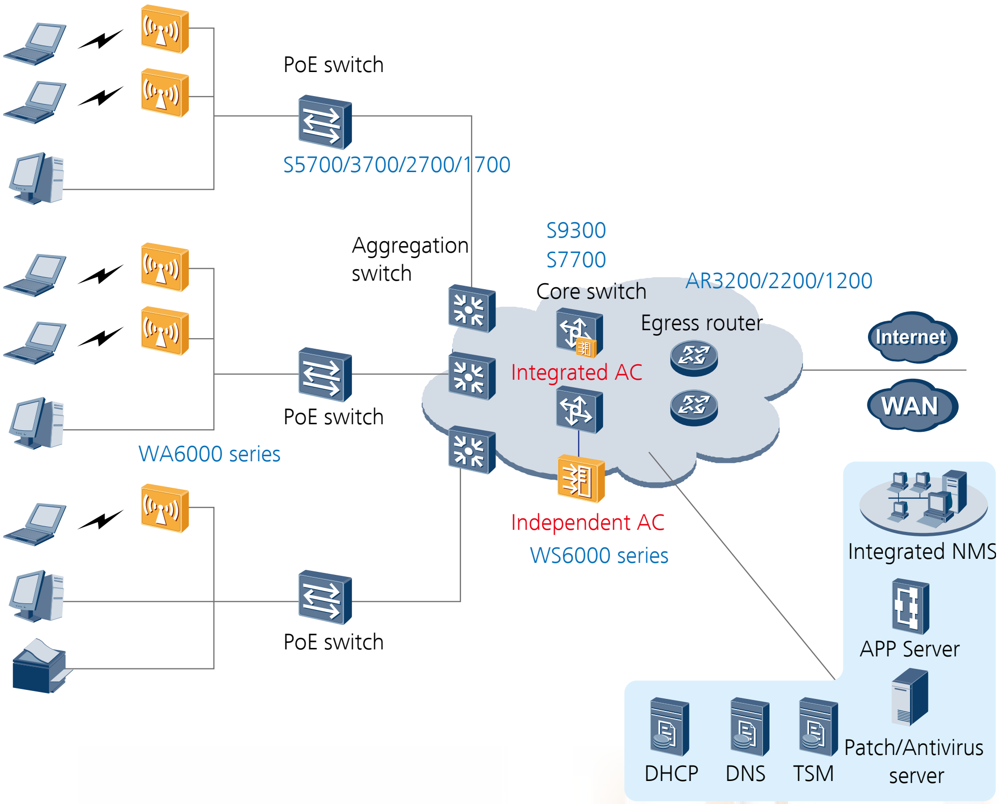
Internet network defense: prevent service interruption caused by ARP spoofing attacks.

User terminal security: provides authentication of terminal users, access policy control, and right management.

Remote access security: ensures information security of remote users using the secure and encrypted tunnel.

6. Wireless Solution of the Technology Campus Network

Enterprise employees want to access network resources anytime and anywhere. Huawei wireless solution integrates wireless and wired services and implements flexible cable layout, meeting requirements of wireless access in different scenarios such as meeting rooms and offices.

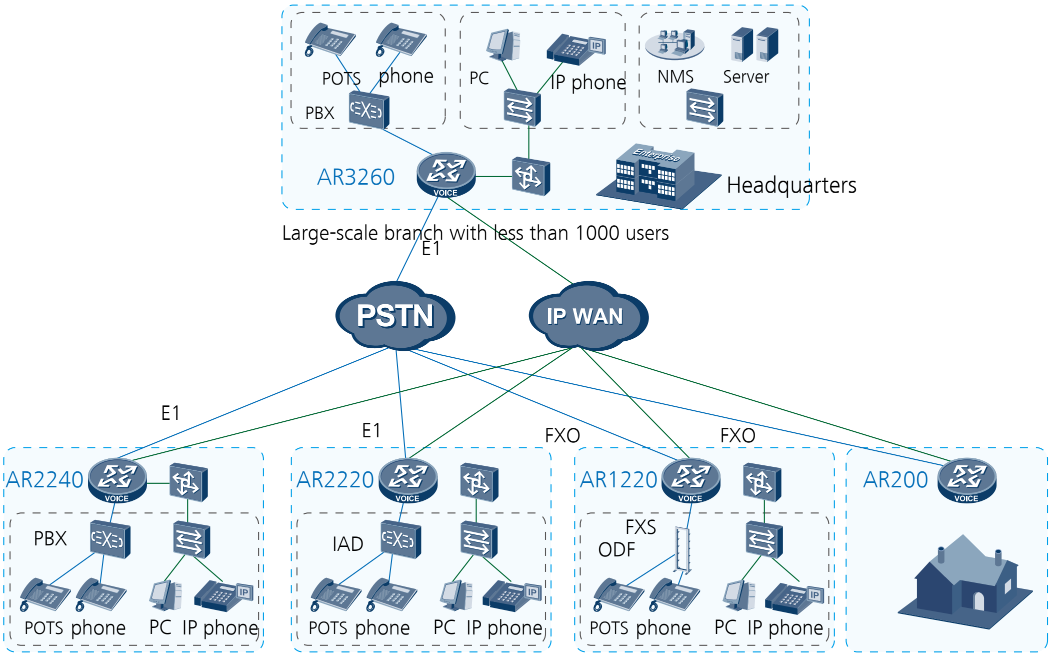


Solution Characteristics:

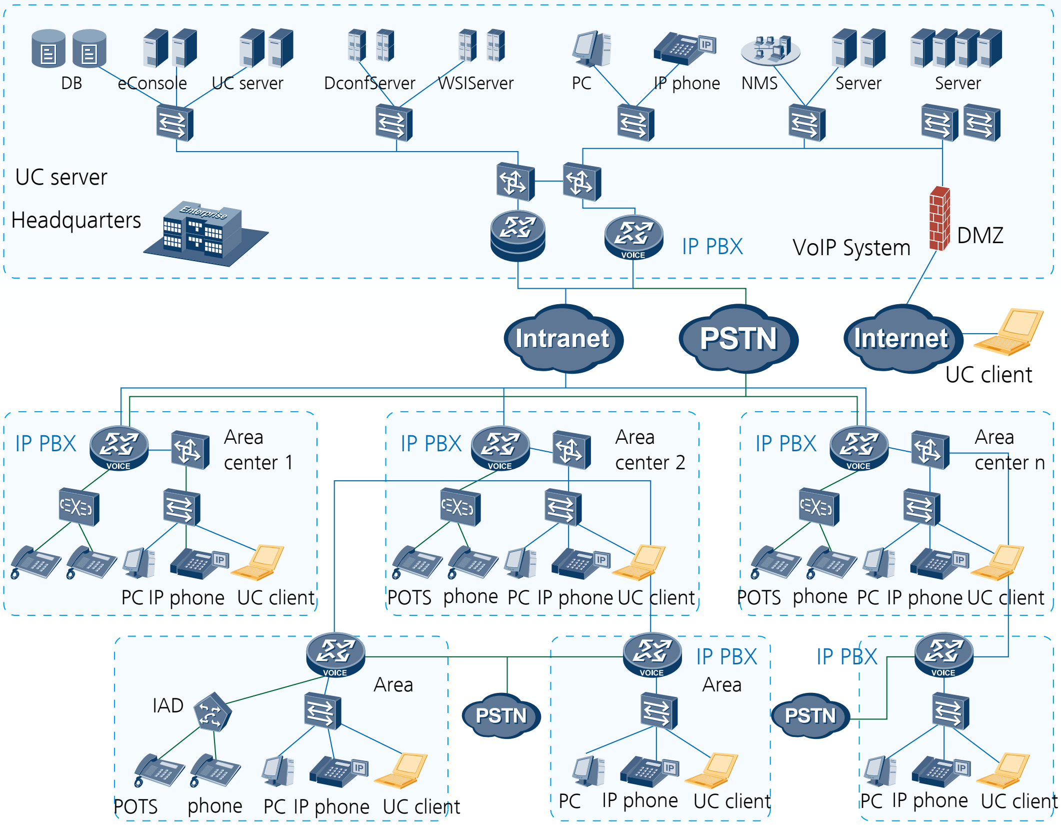
- Wired and wireless authentication and management, and non-blocking
- The integrated or independent AC works with various APs, meeting various requirements.
- This solution provides the 802.11n WLAN network that has high bandwidth and is compatible with 802.11 b/g access.
- The switch provides the PoE function that provides power for APs. This simplifies AP deployment.

7. Voice and UC Communication Solution of the Technology Campus Network

An IP voice communication system faces challenges of how to protect customers' investment, how to coordinate the voice and data services on an IP network, and how to meet requirements for capacity expansion.



Unified communications (UC) is an advanced communication way that integrates computer technologies and traditional communication technologies. UC transmits various application services such as phone, fax, data transmission, audio conference, call center, and instant messaging services on one network platform.



Solution Characteristics:

Improving device use efficiency:

The enterprise IP network carries enterprise voice services. If the enterprise has time division multiplexing private branch exchanges (TDM PBXs) connected to the PSTN network through E1 interfaces, these devices are connected to AR routers through E1 interfaces.

Reducing communication costs:

Voice communication inside an enterprise is implemented by the IP network built by the enterprise. The enterprise does not need to pay toll or local call fees for calls made between enterprise employees.

Enriching communication ways:

This solution supports various value-added services such as the One Number Link to You (ONLY) service. The ONLY service binds a number so that no call is missed.

Improving communication efficiency:

This solution integrates multiple communication methods such as phone, fax, conference calling, instant messaging, and short messaging.

8. Recommended Products

Device	Recommended Product	Description
Access switch	S1700 series switches S2700 series switches S3700 series switches	The access switch supports ACLs, QoS, and rate limiting, which isolates services securely and ensures quality of key services.
Aggregation switch	S5700 series switches	Layer 3 gigabit switch that provides various user isolation and security measures, NAC, and precise ACL control. Two switches can constitute a stack.
Core switch	S7700 series switches S9300 series switches	Layer 3 chassis switch that provides various user isolation and security measures, NAC, precise ACL control, built-in AC, and uniform scheduling and management.
Enterprise egress router	AR3200/2200/1200 series routers NE40E series routers	The enterprise egress router provides LAN/WAN/ADSL2+/G. interfaces and integrating firewall, IPSec, and voice functions
Network management system	eSight	Network management system designed for enterprise campus networks.
Terminal proxy	TSM Agent	Terminal security management software that provides strong terminal security management functions, including user authentication, terminal security check, system repair, behavior management, asset registration, and bulletin receiving.
NAC server	TSM Server	The NAC server provides security access control, terminal security management, patch management, terminal user's behavior management, software distribution, and asset management.
AP	WA603/633/653 series	WLAN device that supports 802.11a/b/g/n. It provides automatic AC discovery and configuration, and real-time management, simplifying network deployment.
AC	S9300 SPU board WS6603 series	Access controller applicable to MANs and enterprise networks for wireless access. It has a large capacity and high performance. It is highly reliable, easy to install and maintain, and features advantages such as flexible networking and energy conservation.

Trademark Notice

HUAWEI , HUAWEI, and are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO.,LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129,P.R.China
Tel: +86 755 28780808

www.huawei.com