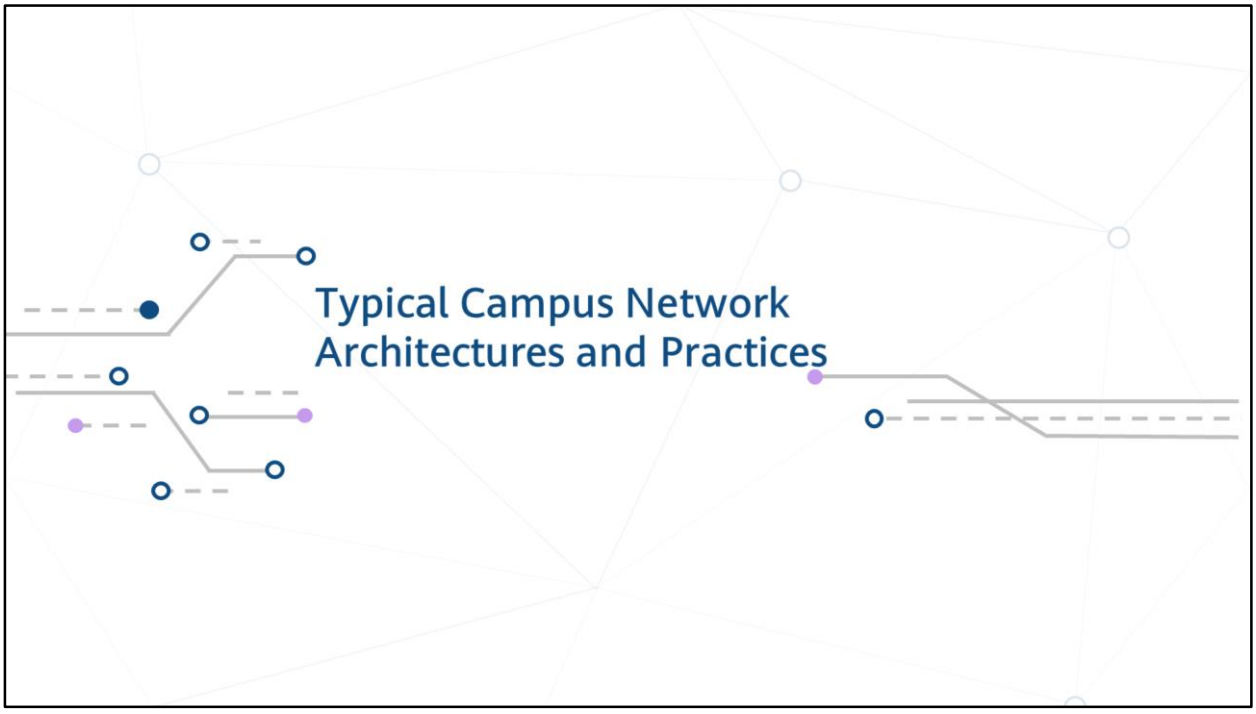

Typical Campus Network
Architectures and Practices

Foreword

- A broad range of places, such as campuses, office spaces, and shopping malls, are covered by networks. You can access internal resources of your school, access internal printers of your company to print documents, or access the Internet to browse news through the networks.
- These networks belong to campus networks and are generally constructed by enterprises or organizations. Campus networks not only improve the operational efficiency of enterprises, but also provide network access services for external users.
- This chapter describes the basic architecture of a campus network and details how to build a campus network.

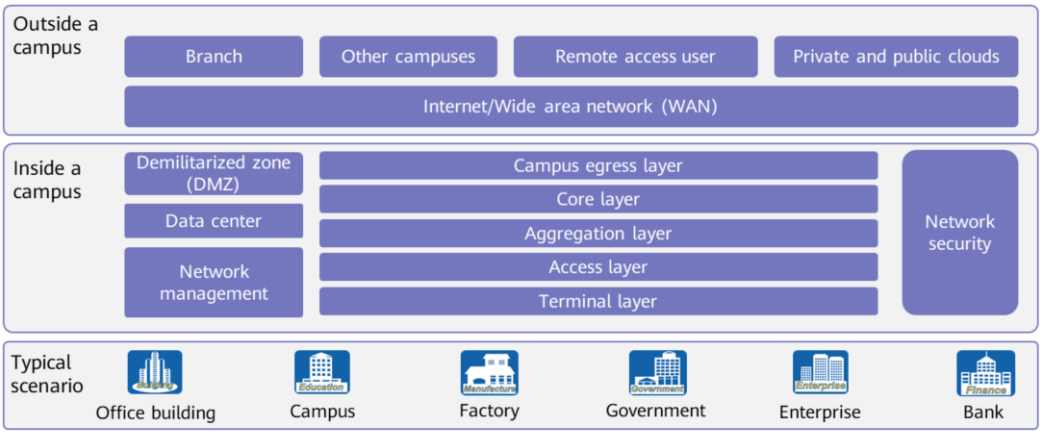
Objectives

- Upon completion of this course, you will be able to:
  - Understand the definition of campus networks.
  - Understand the typical networking architectures of campus networks.
  - Master the planning and design methods of small campus networks.
  - Master the deployment and implementation methods of small campus networks.
  - Understand the small campus network O&M concepts.
  - Understand the small campus network optimization concepts.
  - Independently complete a campus network project.

Contents

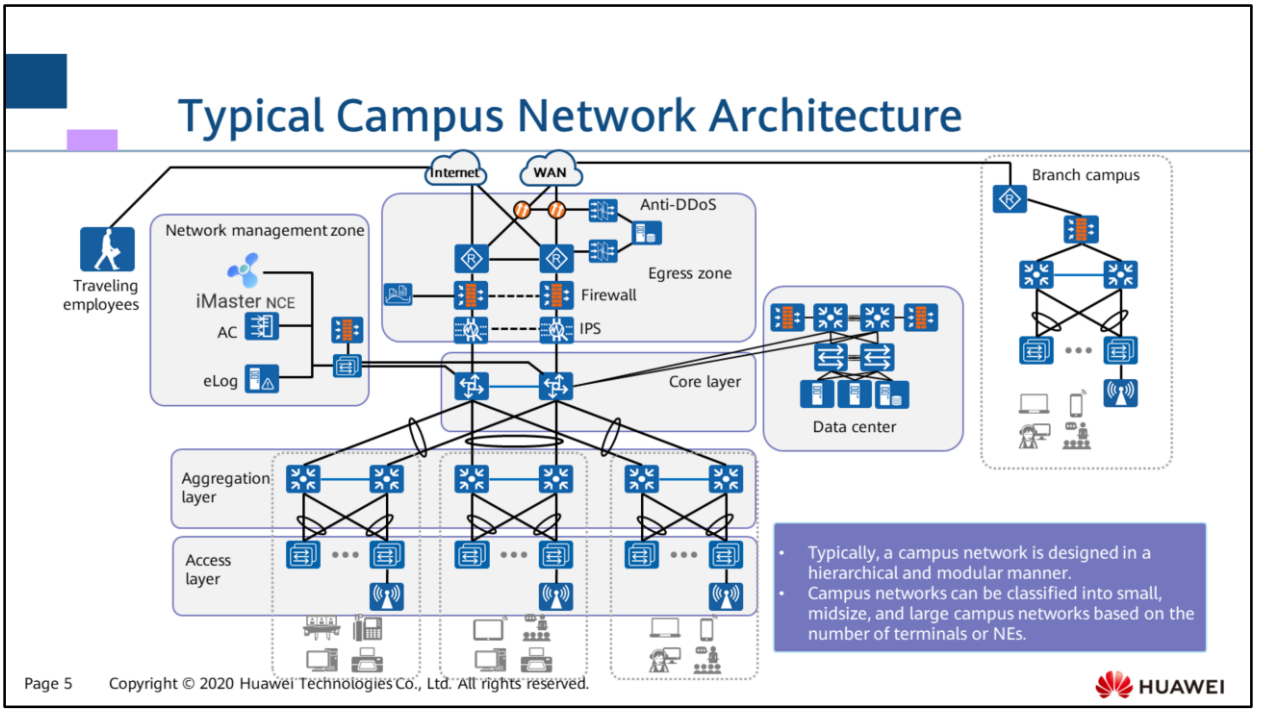
HUAWEI

What Is a Campus Network?



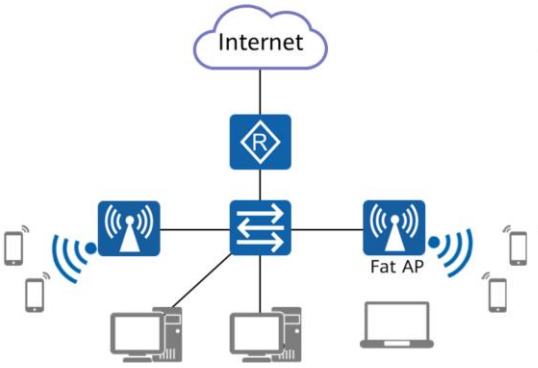
A campus network is a local area network (LAN) that connects people and things in a specified area. Typically, a campus network has only one management entity. If there are multiple management entries in an area, the area is considered to have multiple campus networks.

- The campus network scale is flexible depending on actual requirements. It can be a small office home office (SOHO), a school campus, enterprise campus, park, or shopping center. However, the campus network cannot be scaled out infinitely. Typically, large campuses, such as university campuses and industrial campuses, are limited within several square kilometers. Such campus networks can be constructed using local area network (LAN) technology. A campus network beyond this scope is usually considered as a metropolitan area network (MAN) and is constructed using the WAN technology.
- Typical LAN technologies used on campus networks include IEEE 802.3-compliant Ethernet (wired) technologies and IEEE 802.11-compliant Wi-Fi (wireless) technologies.



- Typical layers and areas of a campus network:
  - **Core layer**: is the backbone area of a campus network, which is the data switching core. It connects various parts of the campus network, such as the data center, management center, and campus egress.
  - **Aggregation layer**: is a middle layer of a campus network, and completes data aggregation or switching. Some fundamental network functions, such as routing, QoS, and security, are also provided at this layer.
  - **Access layer**: As the edge of a campus network, this layer connects end users to the campus network.
  - **Egress area**: As the edge that connects a campus network to an external network, this area enables mutual access between the two networks. Typically, a large number of network security devices, such as intrusion prevention system (IPS) devices, anti-DDoS devices, and firewalls, are deployed in this area to defend against attacks from external networks.
  - **Data center area**: has servers and application systems deployed to provide data and application services for internal and external users of an enterprise.
  - **Network management area**: Network management systems, including the SDN controller, WAC, and eLog (log server), are deployed in this area to manage and monitor the entire campus network.

Typical Architecture of Small Campus Networks

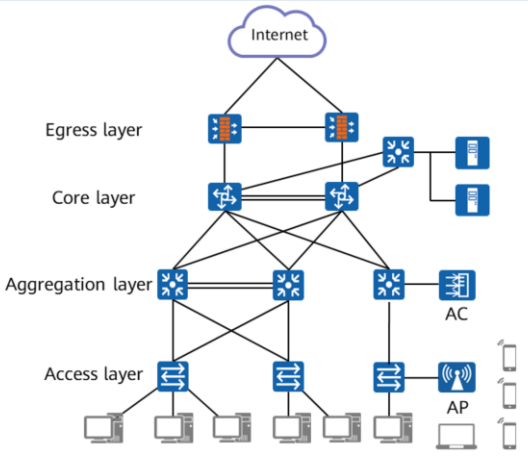


Network topology of a chain cafe

- Small campus networks are typically deployed in scenarios where the number of access users is small (several or dozens of users). A small campus network can cover only one location, has a simple architecture, and is constructed to enable mutual access between internal resources.
- Characteristics of small campus networks:
  - Small number of users
  - Only one location
  - Simple network architecture
  - Simple network requirements

Number of terminals	< 200
Number of NEs	< 25

Typical Architecture of Midsize Campus Networks



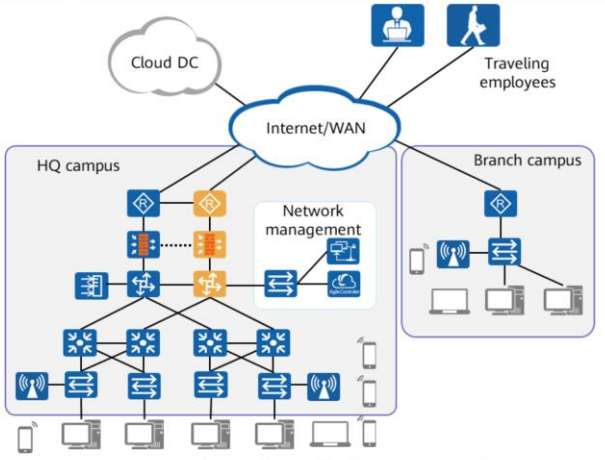
Network topology of a foreign trade company

- A midsize campus network supports access of hundreds to thousands of users.
- The modular design is introduced to midsize campus networks, that is, the networks can be partitioned by function. However, the number of function modules is small. In most cases, a midsize campus network is flexibly partitioned based on service requirements.
- Characteristics of midsize campus networks:
  - Midsize network scale

Number of terminals	200 to 2000
Number of NEs	25 to 100

  - Most commonly used
  - Function partition
  - Typical three-layer network architecture: core, aggregation, and access

Typical Architecture of Large Campus Networks

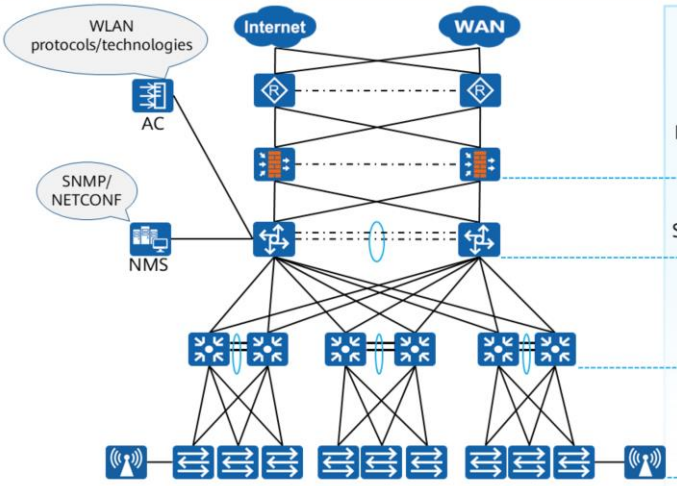


Network topology of a large enterprise

- A large campus network can cover multiple buildings and connect to multiple campuses in a city through WANs. Typically, a large campus network provides access services and allows traveling employees to access their company's internal network through technologies such as Virtual Private Network (VPN).
- Characteristics of large campus networks:
  - Wide coverage
  - Large number of users
  - Complex network requirements
  - Comprehensive function modules
  - Complex network architecture

Number of terminals	> 2000
Number of NEs	> 100

Main Protocols and Technologies of Campus Networks



Common protocols/technologies

NAT, OSPF, static routing, and PPPoE — Egress zone

Stacking, OSPF, static routing, and ACL — Core layer

DHCP, stacking, link aggregation, spanning tree protocol, OSPF, and static routing — Aggregation layer

VLAN, spanning tree, link aggregation, and AAA — Access layer

HUAWEI

Contents

HUAWEI

Networking Requirements

- A company (with about 200 employees) plans to build a brand-new campus network to meet service development requirements. The network requirements are as follows:
  - Meet the current services requirements of the company.
  - Use a simple network topology for easy O&M.
  - Provide wired access for employees and wireless access for guests.
  - Implement simple network traffic management.
  - Ensure network security.

Campus Network Project Lifecycle

1 Planning and design

- Device model selection
- Physical topology
- Logical topology
- Technologies and protocols

2 Deployment and implementation

- Device installation
- Single UPS commissioning
- Joint commissioning test
- Network migration and integration

3 Network O&M

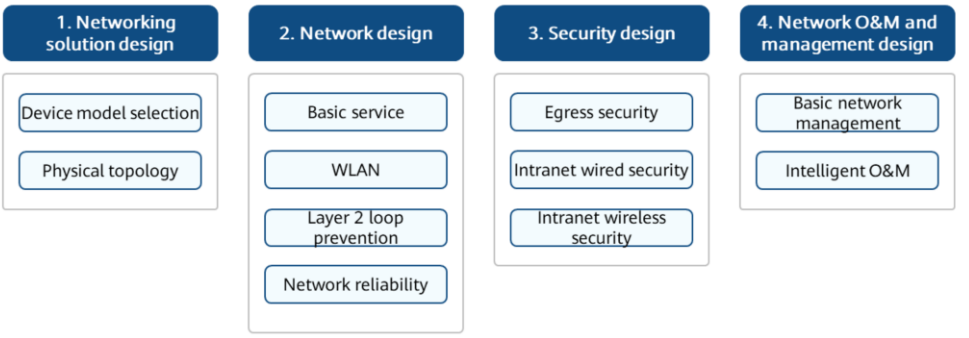
- Routine maintenance
- Software and configuration backup
- Centralized monitoring via the network management system (NMS)
- Software upgrade

4 Network optimization

- Network security improvement
- Software and configuration backup
- User experience improvement

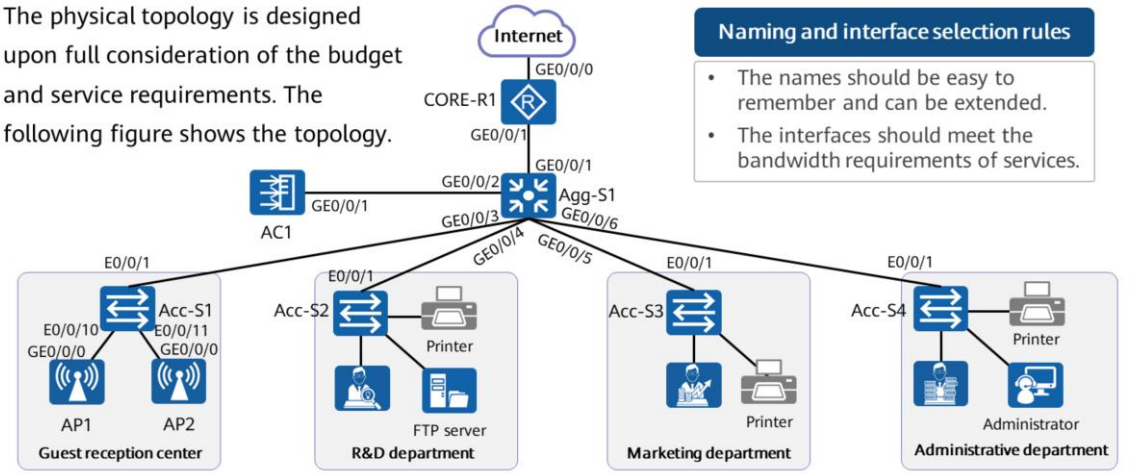
- A campus network project starts from network planning and design. Comprehensive and detailed network planning will lay a solid foundation for subsequent project implementation.
- Project implementation is a specific operation procedure for engineers to deliver projects. Systematic management and efficient process are critical to successful project implementation.
- Routine O&M and troubleshooting are required to ensure the normal running of network functions and support smooth provisioning of user services.
- As users' services develop, the users' requirements on network functions increase. If the current network cannot meet service requirements, or potential problems are found while the network is running, the network needs to be optimized.

Small Campus Network Design



Networking Solution Design

The physical topology is designed upon full consideration of the budget and service requirements. The following figure shows the topology.



Naming and interface selection rules

- The names should be easy to remember and can be extended.
- The interfaces should meet the bandwidth requirements of services.

HUAWEI

- The entire network uses a three-layer architecture.
  - The S3700 is deployed as the access switch to provide 100 Mbit/s network access for employees' PCs and printers.
  - The S5700 is deployed at the aggregation layer as the gateway of the Layer 2 network.
  - The AR2240 is deployed at the core and egress of a campus network.
- Note: Agg is short for aggregation, indicating a device at the aggregation layer. Acc is short for Access, indicating an access device.

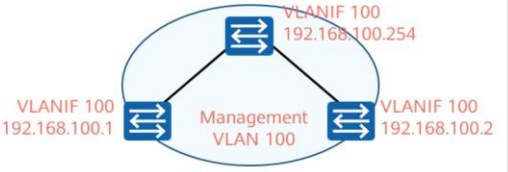
Basic Service Design: VLAN Design

- You are advised to assign consecutive VLAN IDs to ensure proper use of VLAN resources.
- VLANs can be classified into service VLANs, management VLANs, and interconnection VLANs as required.
- Typically, VLANs are assigned based on interfaces.

Service VLAN design

- VLAN assignment by geographic area
- VLAN assignment by logical area
- VLAN assignment by personnel structure
- VLAN assignment by service type

Management VLAN design



In most cases, Layer 2 switches use VLANIF interface addresses as management addresses. It is recommended that all switches on the same Layer 2 network use the same management VLAN and their management IP addresses be on the same network segment.

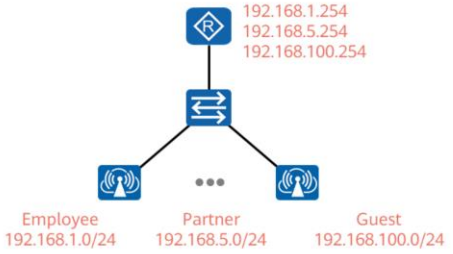
VLAN Planning

- A management VLAN is reserved for Layer 2 devices.
- VLANs are classified into the guest VLAN, R&D department VLAN, marketing department VLAN, and administrative department VLAN.
- Layer 3 switches need to be connected to routers through VLANIF interfaces. Therefore, interconnection VLANs need to be reserved.
- A VLAN is established for CAPWAP tunnels between APs and ACs.

VLAN ID	VLAN Description
1	Guest VLAN or WLAN service VLAN
2	R&D department VLAN
3	Marketing department VLAN
4	Administrative department VLAN
100	Management VLAN of Layer 2 devices
101	Management VLAN of WLAN services
102	Interconnection VLAN between Agg-S1 and CORE-R1

Basic Service Design: IP Address Design

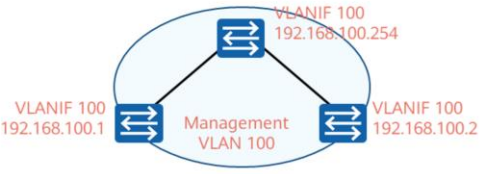
Service IP address



The service IP addresses are the IP addresses of servers, hosts, or gateways.

- It is recommended that the gateway IP addresses use the same rightmost digits, such as .254.
- The IP address ranges of different services must be clearly distinguished. The IP addresses of each type of service terminals must be continuous and can be aggregated.
- An IP address segment with a 24-bit mask is recommended.

Management IP address



Layer 2 devices use VLANIF interface IP addresses as the management IP addresses. It is recommended that all Layer 2 switches connected to a gateway use on the same network segment.

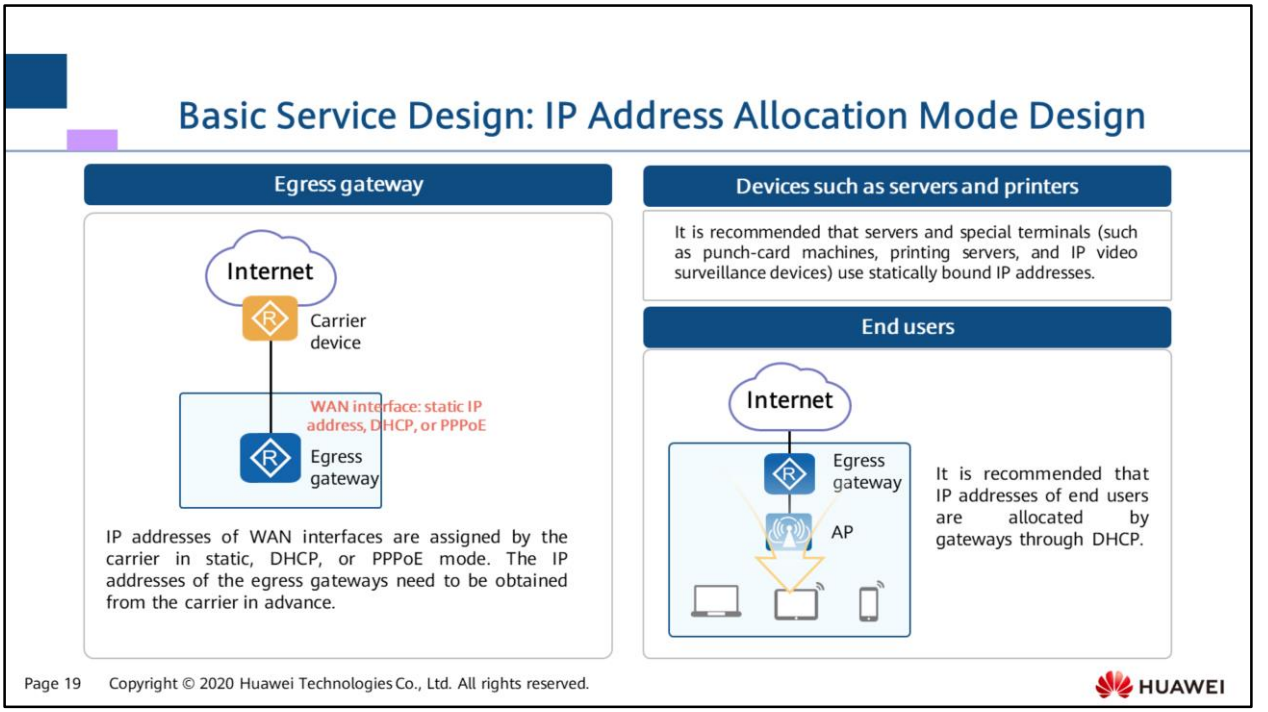
IP address for network device interconnection

It is recommended that the interconnection IP addresses use a 30-bit mask, and core devices use smaller host IP addresses.

IP Address Planning

- Reserve sufficient IP addresses based on the number of clients to be accessed and plan network segments and gateway addresses for each type of service.
- Plan network segments for management IP addresses.
- Divide network segments for interconnection IP addresses.

IP Network Segment/Mask	Gateway Address	Network Segment Description
192.168.1.0/24	192.168.1.254	Network segment to which wireless access guests belong, with the gateway located on Agg-S1
192.168.2.0/24	192.168.2.254	Network segment to which the R&D department belongs, with the gateway located on Agg-S1
192.168.3.0/24	192.168.3.254	Network segment to which the marketing department belongs, with the gateway located on Agg-S1
192.168.4.0/24	192.168.4.254	Network segment to which the administrative department belongs, with the gateway located on Agg-S1
192.168.100.0/24	192.168.100.254	Management network segment of Layer 2 devices, with the gateway located on Agg-S1
192.168.101.0/24	N/A	Management network segment of WLAN services
192.168.102.0/30	N/A	Network segment between Agg-S1 and CORE-R1
1.1.1.1/32	N/A	Loopback interface address on CORE-R1, which is used as the management IP address

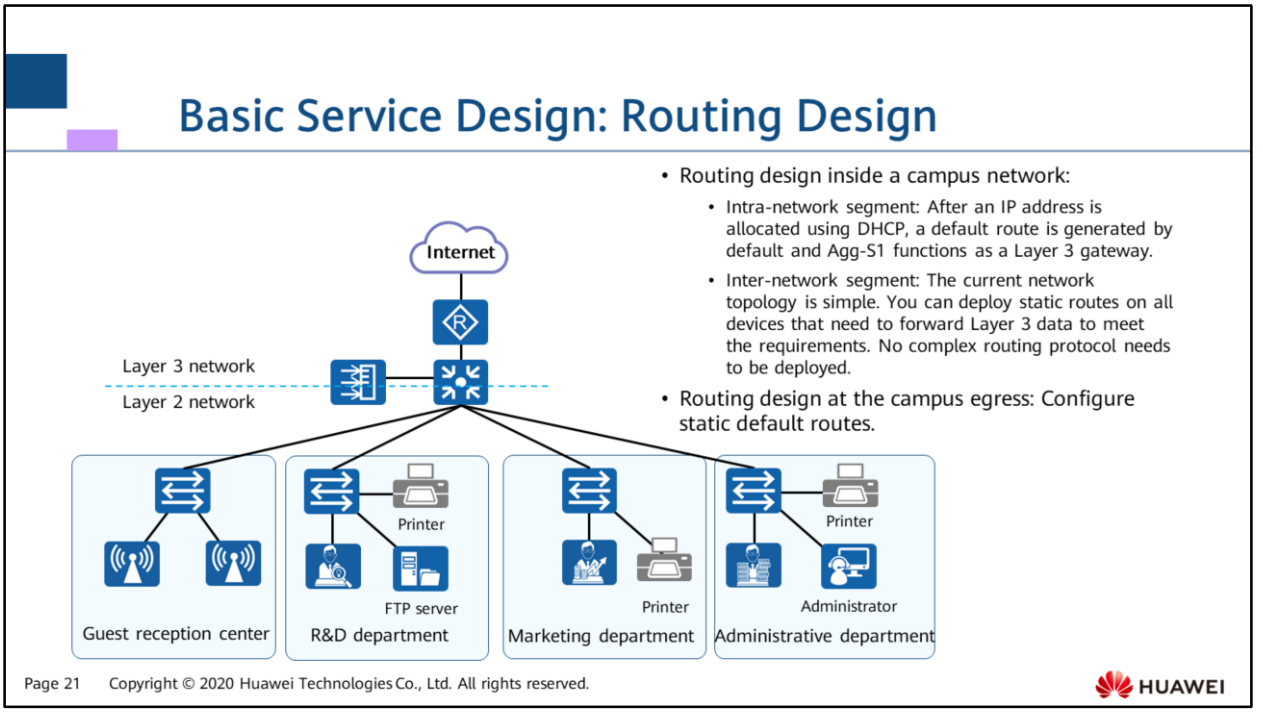


- Dynamic IP address assignment or static IP address binding can be used for IP address assignment. On a small or midsize campus network, IP addresses are assigned based on the following principles:
- IP addresses of WAN interfaces on egress gateways are assigned by the carrier in static, DHCP, or PPPoE mode. The IP addresses of the egress gateways need to be obtained from the carrier in advance.
- It is recommended that servers and special terminals (such as punch-card machines, printing servers, and IP video surveillance devices) use statically bound IP addresses.
- User terminal: It is recommended that the DHCP server be deployed on the gateway to dynamically assign IP addresses to user terminals such as PCs and IP phones using DHCP.

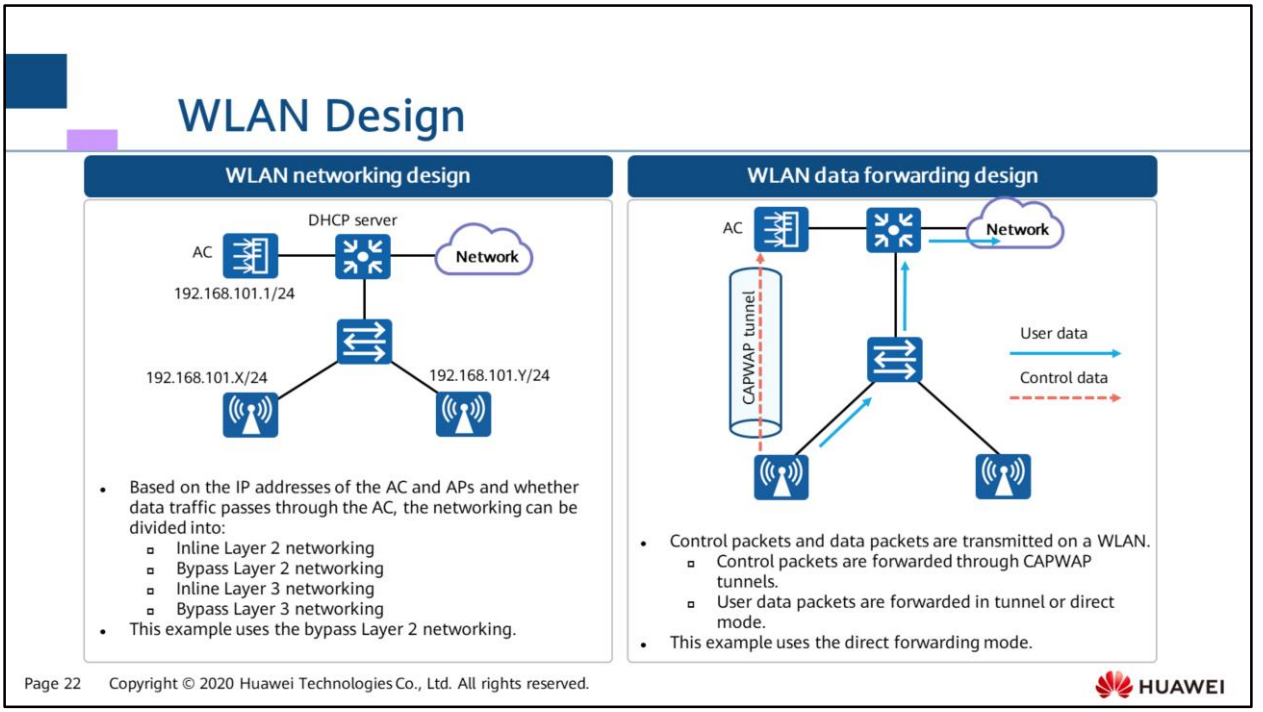
IP Address Allocation Mode Planning

- The egress gateway obtains an IP address through PPPoE.
- All terminals obtain IP addresses through DHCP. The servers and printers are assigned fixed IP addresses.
- IP addresses of all network devices (except APs) are statically configured.

IP Network Segment/Interface	Allocation Mode	Allocation Mode Description
192.168.1.0/24 192.168.2.0/24 192.168.3.0/24 192.168.4.0/24	DHCP	Allocated by Agg-S1. Agg-S1 allocates fixed IP addresses to fixed devices such as servers and printers.
192.168.100.0/24	Static	Device management IP addresses, which are statically configured
192.168.101.0/24	DHCP	IP addresses of ACs are statically configured, and IP addresses of APs are allocated by Agg-S1.
192.168.102.0/30	Static	Interconnection IP address, which is statically configured
GE0/0/0 on CORE-R1	PPPoE	IP address assigned by the carrier



- The routing design of a small or midsize campus network includes design of internal routes and the routes between the campus egress and the Internet or WAN devices.
- The internal routing design of a small or midsize campus network must meet the communication requirements of devices and terminals on the campus network and enable interaction with external routes. As the campus network is small in size, the network structure is simple.
    - AP: After an IP address is assigned through DHCP, a default route is generated by default.
    - Switch and gateway: Static routes can be used to meet requirements. No complex routing protocol needs to be deployed.
- The egress routing design meets the requirements of intranet users for accessing the Internet and WAN. When the egress device is connected to the Internet or WAN, you are advised to configure static routes on the egress device.

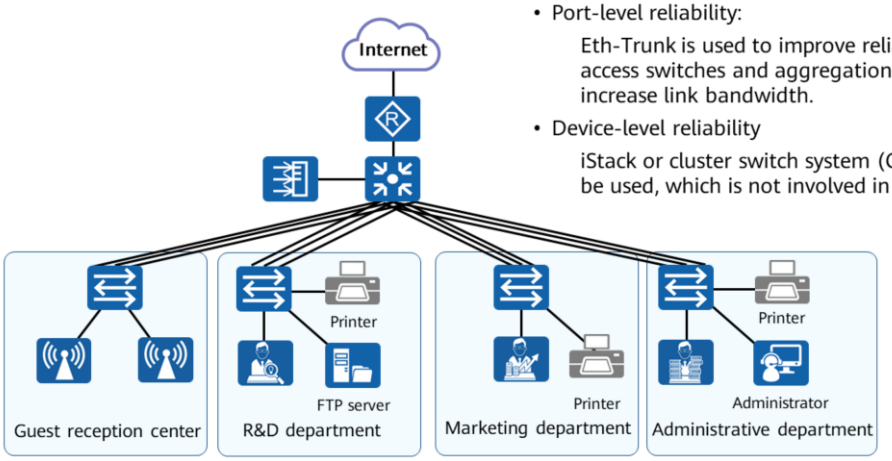


- In addition to planning the networking and data forwarding mode, you also need to perform the following operations:
  - **Network coverage design**: You need to design and plan areas covered by Wi-Fi signals to ensure that the signal strength in each area meets user requirements and to minimize co-channel interference between neighboring APs.
  - **Network capacity design**: You need to design the number of APs required based on the bandwidth requirements, number of terminals, user concurrency rate, and per-AP performance. This ensures that the WLAN performance can meet the Internet access requirements of all terminals.
  - **AP deployment design**: Based on the network coverage design, modify and confirm the actual AP deployment position, deployment mode, and power supply cabling principles based on the actual situation.
  - In addition, WLAN security design and roaming design are required.

WLAN Data Plan

Item	Value
Management VLAN for APs	VLAN 101
Service VLAN for STAs	VLAN 1
DHCP server	Agg-S1 functions as a DHCP server to allocate IP addresses to APs and STAs. The default gateway address of STAs is 192.168.1.254.
IP address pool for APs	192.168.101.2 to 192.168.101.253/24
IP address pool for STAs	192.168.1.1 to 192.168.1.253/24
Source interface address of the AC	VLANIF 101: 192.168.101.1/24
AP group	Name: **ap-group1** Referenced profiles: VAP profile **WLAN-Guest** and regulatory domain profile **default**
Regulatory domain profile	Name: **default** Country code: CN
SSID profile	Name: **WLAN-Guest** SSID name: **WLAN-Guest**
Security profile	Name: **WLAN-Guest** Security policy: WPA-WPA2+PSK+AES Password: **WLAN@Guest123**
VAP profile	Name: **WLAN-Guest** Forwarding mode: direct forwarding Service VLAN: VLAN 1 Referenced profiles: SSID profile **WLAN-Guest** and security profile **WLAN-Guest**

Reliability Design



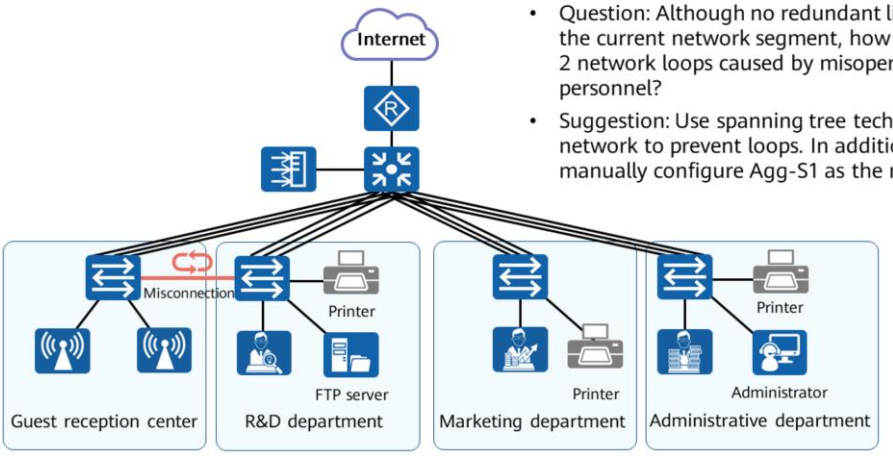
- Port-level reliability:

  Eth-Trunk is used to improve reliability between access switches and aggregation switches and increase link bandwidth.

- Device-level reliability

  iStack or cluster switch system (CSS) technology can be used, which is not involved in this networking.

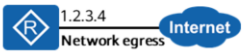
Layer 2 Loop Prevention



- Question: Although no redundant link is introduced to the current network segment, how can we prevent Layer 2 network loops caused by misoperations of office personnel?
- Suggestion: Use spanning tree technology on the Layer 2 network to prevent loops. In addition, you are advised to manually configure Agg-S1 as the root bridge.

Egress NAT Design

Static NAT

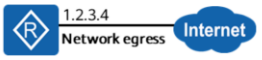


NAT mapping table

Private IP Address	Public IP Address
192.168.1.1	1.2.3.1
192.168.1.2	1.2.3.2

- Static NAT applies to scenarios where a large number of static IP addresses are configured and clients need to use fixed IP addresses.

Dynamic NAT

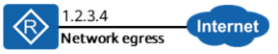


NAT address pool

1.2.3.1	Not in use
1.2.3.2	Not in use
1.3.3.3	Not in use

- Dynamic NAT introduces the address pool concept. Available IP addresses in the address pool are allocated to clients for Internet access.

NAPT and Easy IP



NAT mapping table

Private IP Address:Port Number	Public IP Address:Port Number
192.168.1.10:80	1.2.3.4:10335

- NAPT translates port numbers based on dynamic NAT to improve public address usage.
- Easy IP applies to scenarios where IP addresses of outbound network interfaces are dynamically allocated.

NAT Server

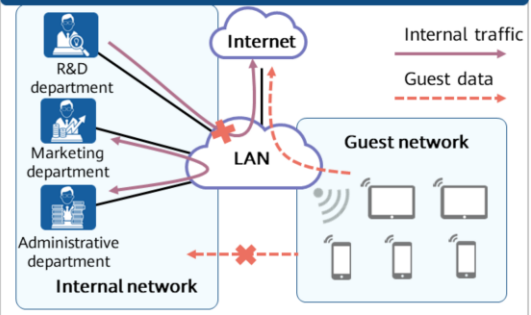
NAT mapping table

Private IP Address:Port Number	Public IP Address:Port Number
192.168.1.1:10321	1.2.3.4:1025
192.168.1.2:17087	1.2.3.4:1026

The NAT server applies to scenarios where a server on the intranet needs to externally provide services.

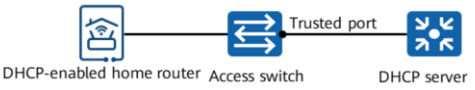
Security Design

Traffic Control



- Different departments can access each other but cannot access the Internet.
- Guests can access the Internet but cannot access the internal network.
- You can use technologies such as traffic policing and traffic filtering to isolate the internal network from the external network and use NAT to control the internal network's access to the Internet.

DHCP Security



- On a campus network, employees often connect unauthorized DHCP-enabled wireless routers to the network, causing private address disorders, address conflicts, and Internet access failures.
- In most cases, DHCP snooping is enabled on access switches to prevent this issue.

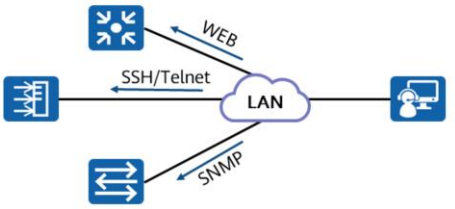
Network Management Security

- When network devices are managed through Telnet or the web system, you can use access control list (ACL) technology to allow only users with fixed IP addresses to log in to the devices.
- For the centralized NMS, SNMPv3 supports identity authentication and encryption, significantly enhancing the NMS security.

- Note: Security design in this case is implemented depending only on routers or switches.

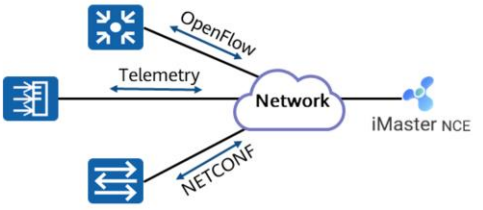
Network O&M and Management Design

Traditional Device Management



- When the network administrator and devices' IP addresses are routable to each other, you can manage the devices through Telnet, the web system, or SSH.
- When there are a large number of devices on a network, you can deploy an SNMP-based unified NMS for network O&M and management.

Management Based on iMaster NCE



- In addition to the SNMP-based traditional NMS, Huawei iMaster NCE can also be used for network management and O&M to implement autonomous network driving.

Small Campus Network Deployment and Implementation

- The project deployment and implementation process must include:
  - Solution formulation
  - Device installation
  - Network commissioning
  - Network migration and integration
  - Transfer-to-maintenance (ETM) training
  - Project acceptance
- The specific process is determined based on the actual situation.

Configuration Scheme (1)

1. Connect network devices using physical cables, configure link aggregation, and add interface description. For details, see the following two tables.

Device	Interface	Configuration
Acc-S1	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 1
	E0/0/10	Description: to AP1
	E0/0/11	Description: to AP2
Acc-S2	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 2
Acc-S3	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 3
Acc-S4	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 4
AC1	GE0/0/1	Description: to Agg-S1's GE0/0/2
CORE-R1	GE0/0/1	Description: to Agg-S1's GE0/0/1

Device	Interface	Configuration
Agg-S1	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/3, GE0/0/7, GE0/0/8 Description: to Acc-S1's eth-trunk 1
	Eth-trunk 2	Mode: LACP-static Trunkport: GE0/0/4, GE0/0/9, GE0/0/10 Description: to Acc-S2's eth-trunk 1
	Eth-trunk 3	Mode: LACP-static Trunkport: GE0/0/5, GE0/0/11, GE0/0/12 Description: to Acc-S3's eth-trunk 1
	Eth-trunk 4	Mode: LACP-static Trunkport: GE0/0/6, GE0/0/13, GE0/0/14 Description: to Acc-S4's eth-trunk 1
	GE0/0/1	Description: to CORE-R1's GE0/0/1
	GE0/0/2	Description: to AC1's GE0/0/1

Configuration Scheme (2)

2. Assign VLANs based on interfaces. For details, see the following two tables.

Device	Interface	Type	Configuration
Acc-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1, 100, 101
	E0/0/10		PVID:101 Allow-pass VLAN 1, 101
	E0/0/11		
Acc-S2	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 2, 100
	Other ports	Access	Default VLAN 2
Acc-S3	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 3, 100
	Other ports	Access	Default VLAN 3
Acc-S4	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 4, 100
	Other ports	Access	Default VLAN 4

Device	Interface	Type	Configuration
Agg-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1, 100, 101
	Eth-trunk 2	Trunk	PVID:100 Allow pass VLAN 2, 100
	Eth-trunk 3	Trunk	PVID:100 Allow pass VLAN 3, 100
	Eth-trunk 4	Trunk	PVID:100 Allow pass VLAN 4, 100
	GE0/0/2	Access	Default VLAN 101
	GE0/0/1	Access	Default VLAN 102
AC1	GE0/0/1	Access	Default VLAN 101

Configuration Scheme (3)

3. Allocate IP addresses to STAs and APs using DHCP and statically configure IP addresses for network devices. For details, see the following two tables.

Device	Interface	Address/Mask
Agg-S1	VLANIF 1	192.168.1.254/24
	VLANIF 2	192.168.2.254/24
	VLANIF 3	192.168.3.254/24
	VLANIF 4	192.168.4.254/24
	VLANIF 100	192.168.100.254/24
	VLANIF 101	192.168.101.254/24
	VLANIF 102	192.168.102.2/30
CORE-R1	GE0/0/1	192.168.102.1/30
	GE0/0/0	Automatic obtaining via PPPoE
	Loopback0	1.1.1.1/32

Device	Interface	Address/Mask
Acc-S1	VLANIF 100	192.168.100.1/24
Acc-S2	VLANIF 100	192.168.100.2/24
Acc-S3	VLANIF 100	192.168.100.3/24
Acc-S4	VLANIF 100	192.168.100.4/24
AC1	VLANIF 101	192.168.1.101/24

Configuration Scheme (4)

4. Configure the IP address allocation mode. For details about DHCP, see the following table.

Network Segment	Other Parameters	Remarks
192.168.1.0/24	Gateway:192.168.1.254 DNS:192.168.1.254	Agg-S1 functions as a DHCP server.
192.168.2.0/24	Gateway:192.168.2.254 DNS:192.168.2.254	Agg-S1 functions as a DHCP server. Fixed IP addresses are allocated to printer (1) and the FTP server.
192.168.3.0/24	Gateway:192.168.3.254 DNS:192.168.3.254	Agg-S1 functions as a DHCP server. A fixed IP address is allocated to printer (2).
192.168.3.0/24	Gateway:192.168.4.254 DNS:192.168.4.254	Agg-S1 functions as a DHCP server. Fixed IP addresses are allocated to printer (3) and the network administrator.
192.168.101.0/24	N/A	Agg-S1 functions as a DHCP server. The IP address (192.168.101.1) occupied by the AC is not allocated.

Configuration Scheme (5)

5. Configure routes. Static routes are used because the network scale is small and the number of NEs is also small. For details, see the following table.

Device	Route Configuration	Remarks
Acc-S1	0.0.0.0 0 192.168.100.254	Route that enables the network administrator to access Layer 2 switches across network segments.
Acc-S2		
Acc-S3		
Acc-S4		
AC1	0.0.0.0 0 192.168.101.254	Route that enables the administrator to access AC1 across network segments.
Agg-S1	0.0.0.0 0 192.168.102.1	Route that matches the traffic destined for the Internet
CORE-R1	192.168.0.0 20 192.168.102.2	Aggregated route for the core router to access the intranet
	Default route	Route pointing to an interface on the external network

Configuration Scheme (6)

6. Configure network management. Set the network management mode to Telnet-based remote management and authentication mode to Authentication, Authorization, and Accounting (AAA). For details, see the following table.

Device	Management Mode	Authentication Mode	Remarks
Acc-S1	Telnet	AAA	The user name and password must be complex and different. In addition, record them.
Acc-S2			
Acc-S3			
Acc-S4			
Agg-S1			
CORE-R1			
AC1			
AP1&AP2	Centralized control and management by the AC	N/A	N/A

7. Network egress configuration

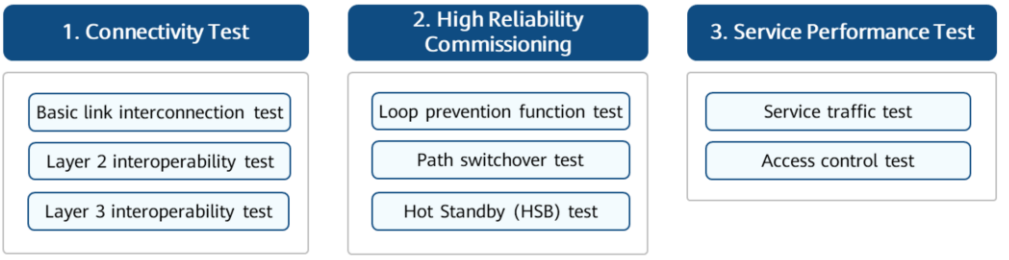
Device	Interface	Access Mode	NAT Mode	Remarks
CORE-R1	GE0/0/0	PPPoE	Easy IP	User name: **PPPoEUser123** Password: **Huawei@123**

Configuration Scheme (7)

8. Configure the WLAN as planned.
9. Perform security-related configurations. For details, see the following table.

Module	Related Technology	Configuration
Traffic monitoring	Traffic policy, NAT, and ACL	1. Configure an advanced ACL to block the traffic from 192.168.1.0/24 to the service network segment on the intranet and allow other traffic to pass through. Configure a traffic filtering policy to reference this ACL and apply the policy to an interface. 2. Configure a basic ACL to permit only the traffic from 192.168.1.0/24 and apply this ACL to the NAT configuration on an outbound network interface.
Network management security	AAA and ACL	Configure a basic ACL to permit only the packets whose source IP address is the administrator's IP address and wildcard mask is 0, and apply the ACL to the VTY interfaces of all managed devices.
DHCP security	DHCP snooping	Enable DHCP snooping on all access switches and configure the uplink interfaces as trusted interfaces.

Small Campus Network Commissioning



Small Campus Network O&M

- After a small campus network is provisioned, it enters the O&M phase. Common O&M methods include:
  - Device environment check
  - Basic device information check
  - Device running status check
  - Service check
  - Alarm handling
- When the network scale reaches a certain level, the network management software can be used for network management and O&M to improve efficiency.

Small Campus Network Optimization

- Network optimization can comprehensively improve the reliability and robustness of networks and better support the development of enterprise services. Common network optimization solutions include but are not limited to:
  - Device performance optimization, such as hardware upgrade and software version update
  - Basic network optimization, such as network architecture optimization and routing protocol adjustment
  - Service quality optimization, such as preferential forwarding of voice and video services
- Formulate an appropriate network optimization solution based on network requirements and actual conditions.

Quiz

1. What is the complete lifecycle of a campus network?
2. What is the function of a management IP address?

1. Network planning and design, deployment and implementation, O&M, and optimization
2. IP address used by the network administrator to manage a device

Summary

- This chapter describes the concepts, types, and common technologies of campus networks.
- Understand the lifecycle of campus networks:
  - Planning and design
  - Deployment and implementation
  - Network O&M
  - Network optimization
- Based on the previous courses, this course focuses on the planning, design, deployment, and implementation of campus networks and details how to establish a small campus network.