**Configuring a Campus Network**

Student Version



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



# Configuring a Campus Network

## Background

Communication networks are ubiquitous in the information society, and campus networks are always a core part. Campuses are everywhere, including factories, government buildings and facilities, shopping malls, office buildings, school campuses, and parks. According to statistics, 90% of urban residents work and live in campuses, 80% of gross domestic product (GDP) is created in campuses, and each person stays in campuses for 18 hours every day. Campus networks, as the infrastructure for campuses to connect to the digital world, are an indispensable part of campus construction and play an increasingly important role in daily working, R&D, production, and operation management.

In this lab activity, you will create a campus network to understand common technologies and their applications on campus networks.

## Objectives

Upon completion of this task, you will be able to:

Understand common campus network concepts and architecture

Understand common network technologies

Understand the lifecycle of campus networks

Be familiar with campus network planning and design, deployment and implementation, network O&M, and network optimization

Be familiar with the process for implementing a campus network project

## Topology

A network needs to be constructed in an office building. The office building has six floors. Currently, three floors have been put in use: the reception hall on the first floor, administrative department and general manager's office on the second floor, R&D department and marketing department on the third floor. The core equipment room is deployed on the first floor, and a small room is deployed on each of the other floors to house network devices.

Set up a project team to complete the network construction.

## Lab Tasks

### Requirement Collection and Analysis

What information should be obtained from the company? Please list at least five items.

Example: The number of terminals to be connected to the enterprise network.

1.

2.

3.

4.

5.

Analyze the collected requirements.

1. Project Budget

The budget is tight. The requirements need to be implemented at minimum costs.

1. Types of Terminals to Be Connected

Both wired and wireless terminals will be deployed.

1. Number of Terminals

First floor: 10 wired terminals and 100 wireless terminals Second and third floors: 200 wired terminals and 50 wireless terminals

1. Network Management Mode

SNMP is used for unified network management.

1. Volume and Trend of Network Traffic

Most of the traffic is internal traffic. 100 Mbit/s wired access is required. There are no other special requirements.

1. Availability Requirements

The Layer 3 network needs some redundancy and failover capabilities.

1. Security Requirements

Network traffic needs to be controlled.

1. Internet Access Mode

Egress devices on the campus network use static IP addresses to connect to the Internet.

1. Network Expansion Requirements

When other floors are put into use, there should be no need to replace existing devices.

### Planning and Design

1. **Device Selection and Physical Topology Design (Optional)**

**Background:**

The following table lists the total number of terminals on the network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Floor** | **First Floor** | **Second Floor** | **Third Floor** | **Other Floors (Reserved)** |
| Wired terminals | 10 | 200 | 200 | 500 |
| Wireless terminals | 100 | 50 | 50 | 200 |
| Remarks | Guest wireless terminals + servers | Computers + mobile phones | | |

The traffic from wireless terminals is the Internet access traffic. Each client has a rate of 2 Mbit/s.

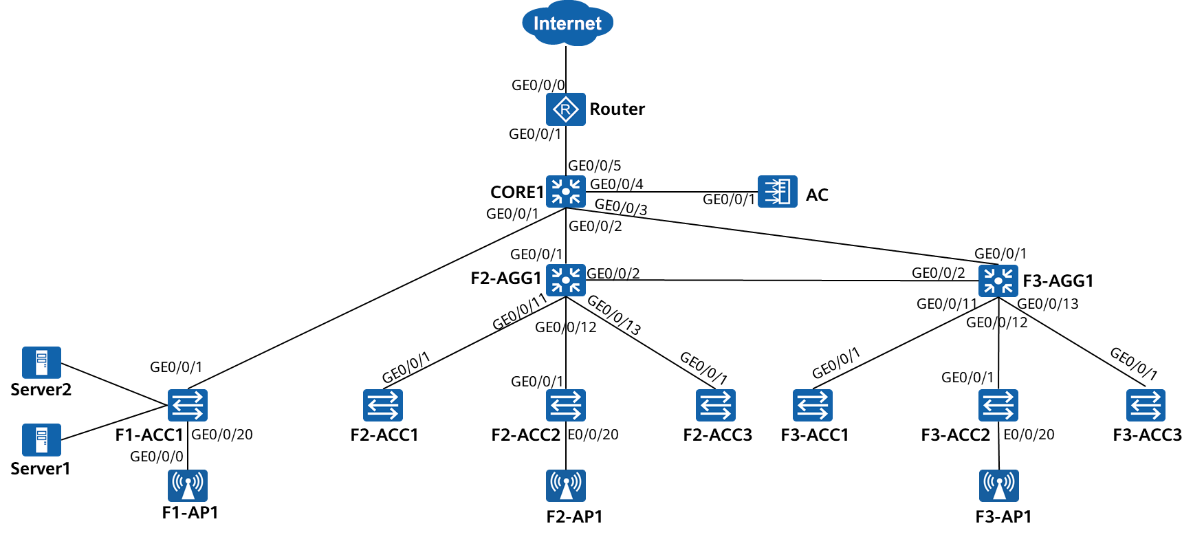
Ensure that computers have a rate of 100 Mbit/s and servers have a rate of 1000 Mbit/s.

To improve wireless access quality, at least three dual-band APs are required on each floor.

**Task:**

Design the physical topology of the network in the sequence of access layer, aggregation layer, core layer, and egress area and select devices accordingly.

**Reference answer:**



The device interface numbers are as follows:

|  |  |
| --- | --- |
| **Device** | **Interfaces** |
| F2-ACC1, F2-ACC2, F2-ACC3, F3-ACC1, F3-ACC2, and F3-ACC | E0/0/1~E0/0/222  GE0/0/1~GE0/0/2 |
| F1-ACC1, F2-AGG1, F3-AGG1, and CORE1 | GE0/0/1~GE0/0/24 |
| AC | GE0/0/1~GE0/0/8 |
| F1-AP1, F2-AP1, and F3-AP1 | GE0/0/0~GE0/0/1 |
| Router | GE0/0/0~GE0/0/2 |



The *Practices in Campus Network Projects* in the HCIA-Datacom certification textbook details the network design and topology design process based on the preceding requirements. This part is omitted in this document. In actual networking, there are a large number of access switches and APs. To simplify the networking and facilitate subsequent tests, a simplified network topology is used in this document.

1. **Layer 2 Network Design**

**Background:**

VLAN creation on the wired network:

1. Access switch ports GE0/0/1 to GE0/0/10 in the core equipment room connect to servers and are assigned to the same VLAN.
2. On the second floor, F2-ACC2 is connected to the general manager's office, and other switches are connected to the administrative department. The two departments belong to different VLANs.
3. On the third floor, E0/0/1 to E0/0/10 of F3-ACC1 and F3-ACC3 belong to the marketing department, and E0/0/11 to E0/0/20 belong to the R&D department.
4. E0/0/1 to E0/0/19 of F3-ACC2 belong to the marketing department.

VLAN creation on the wireless network:

1. Wireless terminals on different floors must be assigned to different VLANs.
2. The wireless network management VLAN of each floor is different.



Device interconnection VLANs and device management VLANs need to be reserved.

**Task:**

Fill in the Layer 2 network planning table based on the existing information and requirements.

| **VLAN ID** | **Description** |
| --- | --- |
| Example: 1 | Layer 2 device management VLAN |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Reference answer:**

| **VLAN ID** | **Description** |
| --- | --- |
| 1 | Layer 2 device management VLAN on the first floor |
| 2 | Layer 2 device management VLAN on the second floor |
| 3 | Layer 2 device management VLAN on the third floor |
| 100 | VLAN for servers |
| 101 | VLAN for the General Manager's Office |
| 102 | VLAN for the Administrative Department |
| 103 | VLAN for the Marketing Department |
| 104 | VLAN for the R&D Department |
| 105 | VLAN for the wireless terminals on the first floor |
| 106 | VLAN for the wireless terminals on the second floor |
| 107 | VLAN for the wireless terminals on the third floor |
| 201 | VLAN for the interconnection between F2-AGG1 and CORE1 |
| 202 | VLAN for the interconnection between F3-AGG1 and CORE1 |
| 203 | VLAN for the interconnection between F2-AGG1 and F3-AGG1 |
| 204 | VLAN for the interconnection between CORE1 and the router |
| 205 | Wireless network management VLAN on the first floor |
| 206 | Wireless network management VLAN on the second floor |
| 207 | Wireless network management VLAN on the third floor |

1. **Layer 3 Network Design**

**Background:**

The address range is network 192.168.0.0/16. The requirements are as follows:

1. First floor:
2. The servers use static IP addresses. IP addresses of wireless stations and APs are allocated by CORE1 through DHCP. The gateway is on CORE1.
3. The management IP addresses of the access switches are static IP addresses, and the gateway is on CORE1.
4. Second and third floors:
5. The IP addresses of all wired terminals, wireless terminals, and wireless APs are allocated by the aggregation switch of the corresponding floor(s) through DHCP. The gateway is deployed on the aggregation switches.
6. The management IP addresses of the access switches are static IP addresses, and the gateway is on the aggregation switch of the corresponding floor(s).

OSPF is used on the entire network to enable connectivity between service networks. All terminals access the Internet through the router.

**Task:**

Fill in the Layer 3 network planning table based on the existing information and requirements.

| **IP Network** | **Address Assignment Method and Gateway** | **Routing Mode** | **Network Description** |
| --- | --- | --- | --- |
| 192.168.1.0/24 | DHCP; 192.168.1.254 | OSPF | Layer 2 device management network |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Reference answer:**

| **IP Network** | **Address Assignment Method and Gateway** | **Routing Configuration** | **Network Description** |
| --- | --- | --- | --- |
| 192.168.1.0/24 | Static addresses; CORE1 | Default route pointing to CORE1 | Layer 2 device management network on the first floor |
| 192.168.2.0/24 | Static addresses; F2-AGG1 | Default route pointing to F2-AGG1 | Layer 2 device management network on the second floor |
| 192.168.3.0/24 | Static addresses; F3-AGG | Default route pointing to F3-AGG | Layer 2 device management network on the third floor |
| 192.168.100.0/24 | Static addresses; CORE1 | Advertised in OSPF through gateway devices | Network of servers |
| 192.168.101.0/24 | Assigned by F2-AGG1 through DHCP; F2-AGG1 | Network of the General Manager's Office |
| 192.168.102.0/24 | Network of the Administrative Department |
| 192.168.103.0/24 | Assigned by F3-AGG1 through DHCP; F3-AGG1 | Network of the Marketing Department |
| 192.168.104.0/24 | Network of the R&D Department |
| 192.168.105.0/24 | Assigned by CORE1 through DHCP; CORE1 | Network of the wireless terminals on the first floor |
| 192.168.106.0/24 | Assigned by F2-AGG1 through DHCP; F2-AGG1 | Network of the wireless terminals on the second floor |
| 192.168.107.0/24 | Assigned by F3-AGG1 through DHCP; F3-AGG1 | Network of the wireless terminals on the third floor |
| 192.168.201.0/30 | Static addresses; no gateway needed | OSPF is enabled, neighbor relationship is established,  and the default route is advertised by the router | Network for the interconnection between F2-AGG1 and CORE1 |
| 192.168.202.0/30 | Network for the interconnection between F3-AGG1 and CORE1 |
| 192.168.203.0/30 | Network for the interconnection between F2-AGG1 and F3-AGG1 |
| 192.168.204.0/30 | Network for the interconnection between CORE1 and the router |
| 192.168.205.0/24 | Assigned by CORE1 through DHCP; CORE1 | Advertised in OSPF through gateway devices | Wireless network management network on the first floor |
| 192.168.206.0/24 | Assigned by F2-AGG1 through DHCP; F2-AGG1 | Wireless network management network on the second floor |
| 192.168.207.0/24 | Assigned by F3-AGG1 through DHCP; F3-AGG1 | Wireless network management network on the third floor |

1. **WLAN Design**

**Background:**

All APs are managed by the AC in a unified manner, and the AC has limited forwarding performance.

1. APs on the first floor are registered at Layer 2.
2. All APs on the second and third floors register with the AC at Layer 3. The AC's gateway is CORE1.

Create an SSID for each floor.

1. The WPA-WPA2+PSK+AES security policy is used.
2. Each floor has a different SSID and password.

**Task:**

Fill in the WLAN network planning table based on the existing information and requirements.

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **WLAN on the First Floor** | **WLAN on the Second Floor** | **WLAN on the Third Floor** |
| AP management VLAN |  |  |  |
| Service VLAN |  |  |  |
| DHCP server |  |  |  |
| IP address of the AC's source interface |  |  |  |
| AP group |  |  |  |
| Regulatory domain profile |  |  |  |
| SSID profile |  |  |  |
| Security profile |  |  |  |
| VAP profile |  |  |  |
| Other configurations |  |  |  |

**Reference answer:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **WLAN on the First Floor** | **WLAN on the Second Floor** | **WLAN on the Third Floor** |
| AP management VLAN | VLAN205 | VLAN206 | VLAN207 |
| Service VLAN | VLAN105 | VLAN106 | VLAN107 |
| DHCP server | CORE1 assigns IP addresses to APs and STAs. | F2-AGG1 assigns IP addresses to APs and STAs. | F3-AGG1 assigns IP addresses to APs and STAs. |
| IP address of the AC's source interface | VLANIF205: 192.168.205.253/24 | | |
| AP group | Name: WLAN-F1 VAP profile: WLAN-F1  Regulatory domain profile: default | Name: WLAN-F2 VAP profile: WLAN-F2  Regulatory domain profile: default | Name: WLAN-F3 VAP profile: WLAN-F3  Regulatory domain profile: default |
| Regulatory domain profile | Name: default Country code: CN | | |
| SSID profile | Name: WLAN-F1 SSID name: WLAN-F1 | Profile name: WLAN-F2  SSID name: WLAN-F2 | Profile name: WLAN-F3  SSID name: WLAN-F3 |
| Security profile | Name: WLAN-F1 Security policy: WPA-WPA2+PSK+AES Password: WLAN@Guest123 | Name: WLAN-F2  Security policy: WPA-WPA2+PSK+AES Password: WLAN@Employee2 | Name: WLAN-F3  Security policy: WPA-WPA2+PSK+AES Password: WLAN@Employee3 |
| VAP profile | Name: WLAN-F1 Forwarding mode: direct forwarding Service VLAN: VLAN: 105 Profiles:  SSID profile: WLAN-F1; Security profile: WLAN-F1 | Name: WLAN-F2 Forwarding mode: direct forwarding Service VLAN: 106 Profiles:  SSID profile: WLAN-F2  Security profile: WLAN-F2 | Name: WLAN-F3 Forwarding mode: direct forwarding Service VLAN: VLAN: 107 Profiles:  SSID profile: WLAN-F3  Security profile: WLAN-F3 |

1. **Security and Egress Design**

**Background:**

The guest SSID is not allowed to access the intranet of the company.

Only wireless terminals can access the Internet.

The router uses a static IP address to access the Internet. The carrier assigns IP addresses 1.1.1.1 to 1.1.1.10 (with a 24-bit mask) to the router. The next-hop IP address for the router to access the Internet is 1.1.1.254.

A web server in the enterprise needs to provide services for external users. The private IP address of the web server is 192.168.100.1 and the port number is 80. To ensure server security, NAT mapping is provided only for web services.

**Task:**

Fill in the security and egress planning table based on the existing information and requirements.

|  |  |
| --- | --- |
| **Requirement** | **Implementation** |
|  |  |
|  |  |
|  |  |
|  |  |

**Reference answer:**

|  |  |
| --- | --- |
| **Requirement** | **Implementation** |
| Intranet access control applicable to guests | Configure a traffic filter or a traffic policy on CORE1. |
| Internet access control | Configure NAT on the router and disable address translation for the specified networks. |
| Web server mapping | Configure NAT server on the router interface. |

1. **Network Management Design**

**Background:**

SNMPv3 is used to communicate with the NMS, and authentication and encryption are configured to enhance security.

All devices except the router and AC communicate with the NMS at 192.168.100.2/24 through the management VLAN.

Routers communicate with the NMS through GE0/0/1.

The AC communicates with the NMS through VLANIF 205.

All devices must be able to report SNMP alarms to the NMS.

**Task:**

Based on the preceding requirements, optimize the device configurations in the deployment and implementation phase.

### Implementation

1. **Configuration Scheme**

Fill in the configuration scheme for each device according to the planning and design scheme.

**Router:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| IP address configuration |  |
| OSPF |  |
| Egress configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**CORE1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| OSPF configuration |  |
| DHCP configuration |  |
| Access control |  |
| SNMP configuration |  |
| Other configurations |  |

**F2-AGG1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLAN configuration on interfaces |  |
| VLANIF interface configuration |  |
| OSPF configuration |  |
| DHCP configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F3-AGG1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLAN configuration on interfaces |  |
| VLANIF interface configuration |  |
| OSPF configuration |  |
| DHCP configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**AC:**

| **Item** | **Configuration** |
| --- | --- |
| Basic configuration |  |
| Wired network configuration |  |
| Wireless network configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F1-ACC1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F2-ACC1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F2-ACC2:**

| **Item** | **Configuration** |
| --- | --- |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F2-ACC3:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F3-ACC1:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F3-ACC2:**

| **Item** | **Configuration** |
| --- | --- |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**F3-ACC3:**

|  |  |
| --- | --- |
| **Item** | **Configuration** |
| Basic configuration |  |
| VLAN configuration |  |
| VLANIF interface configuration |  |
| Routing configuration |  |
| SNMP configuration |  |
| Other configurations |  |

**Configuration**

Set up the lab environment and complete related configurations according to the preceding configuration schemes within 40 minutes.

1. **Project Acceptance**

After the device configuration is complete, what items need to be verified for acceptance? How are they verified? Please list at least five items.

1.

2.

3.

4.

5.

**Reference answer:**

1. Verify whether the wireless clients can detect wireless signals and access the network successfully.
2. Verify whether the OSPF neighbor relationship is normal.
3. Verify the connectivity within networks.
4. Verify the connectivity between networks.
5. Verify the access control for wireless guests.
6. Verify the Internet access control.
7. Verify whether the NMS can manage network devices.

### Network O&M

1. **O&M Handover**

After the project is delivered, how do you arrange the maintenance work in the future? Discuss with your team and list at least five maintenance items.

**Reference answer:**

| **Recommended Maintenance Interval** | **Check Item** | **Check Method** | **Evaluation Criteria** |
| --- | --- | --- | --- |
| Daily | Power connections | Observation | The power cable is correctly and securely connected to the specified position of the device. The power supply indicator on the device should be steady on (green). |
| Device temperature | <HUAWEI> display temperature | The temperature of each module falls between the upper limit and lower limit. |
| Alarm information | <HUAWEI> display alarm urgent | Alarms are recorded, and major or more severe alarms are immediately analyzed and processed. |
| CPU usage | <HUAWEI> display cpu-usage | The CPU usage of each module is normal. If the CPU usage exceeds 80% frequently or persistently, adequate attention is required. |
| Memory usage | <HUAWEI> display memory-usage | Memory usage is normal. If the value of **Memory Using Percentage** exceeds 60%, adequate attention is required. |
| Weekly | Ambient temperature in the equipment room | Instrument measurement | The long-term operating temperature of the equipment room ranges from 0°C to 50°C, and the short-term operating temperature ranges from –5°C to 55°C. |
| Ambient humidity in the equipment room | Instrument measurement | The ambient humidity in the equipment room should range from 10% RH to 90% RH. |
| Monthly | Device position | Observation and instrument measurement | The device is placed stably in a flat position in a well ventilated, dry, and clean environment. |
| Routing table | <HUAWEI> display ip routing-table | On all devices running the same routing protocol at the same layer of a network, the number of routes should not vary widely. |
| Configuration backup | NA | The configuration information of the devices must be backed up every month. |
| Password change | NA | The device login passwords must be changed every month. |

### Network Optimization

1. **Performance Optimization**

With the development of the enterprise, the internal traffic, especially the traffic between the second and third floors, increases sharply. The capacity of the link between aggregation switches is insufficient for such a large amount of traffic. How can the link be optimized?

**Reference answer:**

1. You can add physical links between F2-AGG1 and F3-AGG1 and configure Ethernet link aggregation.
2. Change the OSPF costs to implement load balancing so that some traffic can be forwarded through CORE1.

## Appendix

The commands and references listed in this document are for reference only. The correct commands and references are subject to your product model and version.

References:

1. AR600 and AR6000 Product Documentation
2. S2720, S5700, and S6700 Series Ethernet Switches Product Documentation
3. Wireless Access Controller (AC and Fit AP) Product Documentation
4. Typical Campus Network Architectures and Practices

Reference links:

http://support.huawei.com/

http://e.huawei.com/