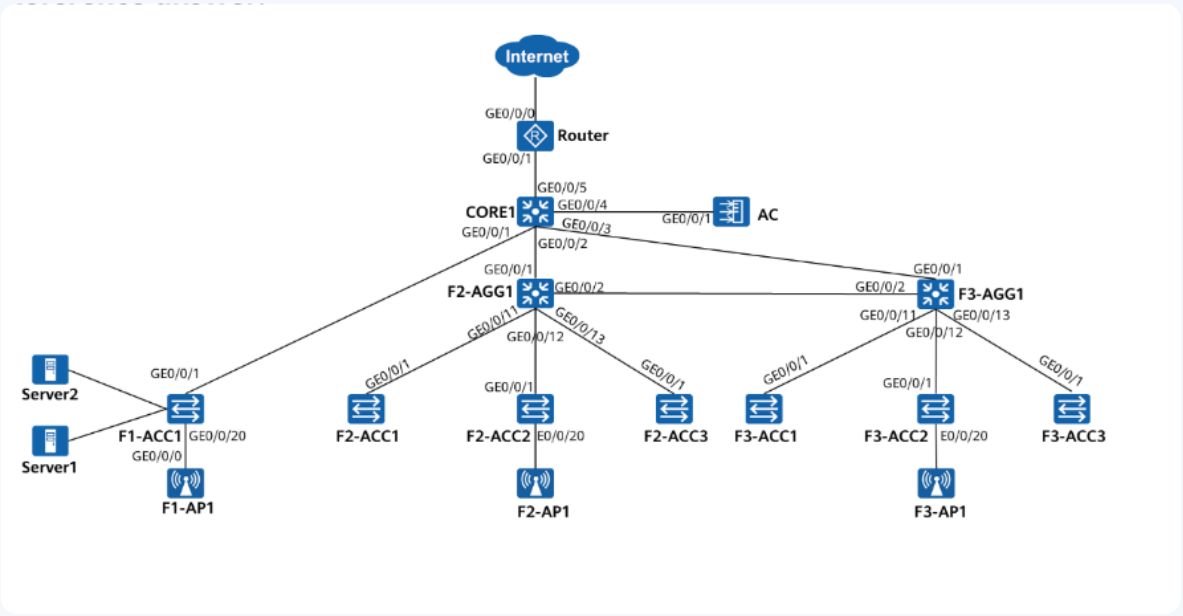
Lab9

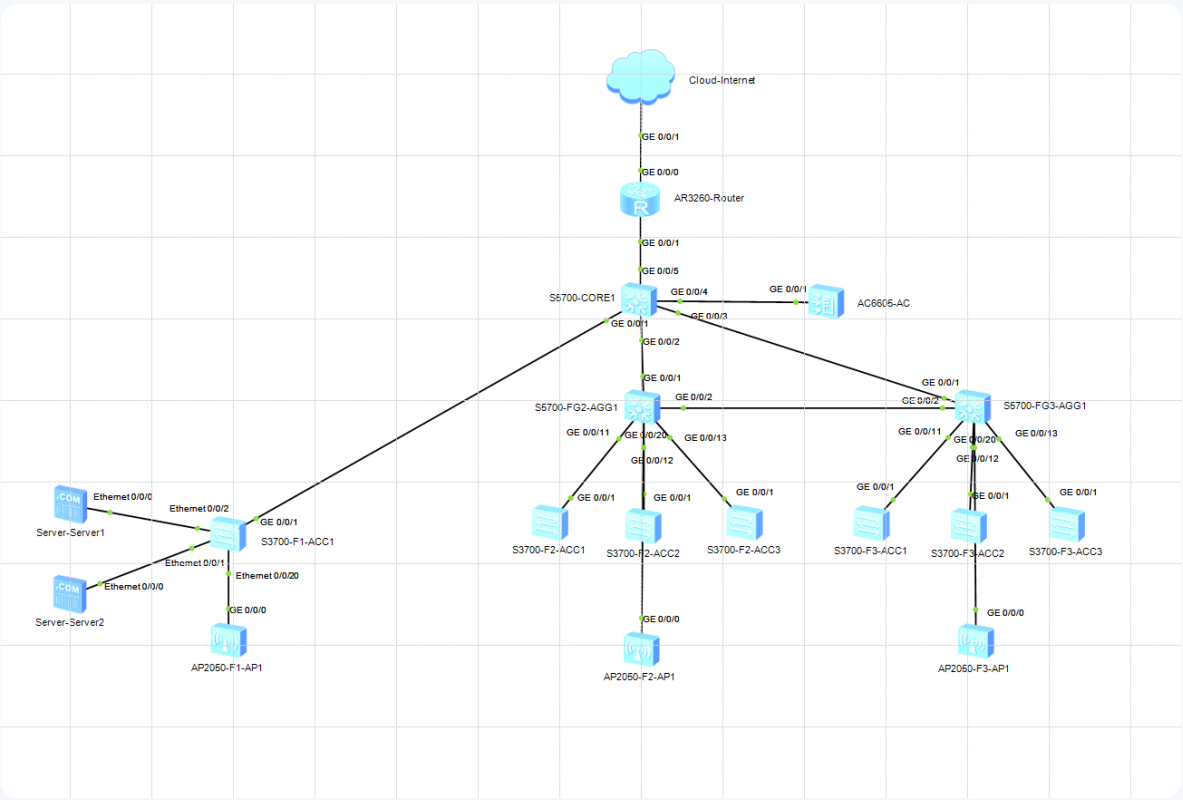
1 Lab9 Configuring a Campus Network

1.1 Introduction

- Campus networks are crucial for digital connectivity in various settings such as factories, government buildings, shopping malls, etc.
- They support daily work, R&D, production, and management activities.
- The lab activity involves creating a campus network to understand common technologies and their practical applications.

1.2 Networking Topology





- Network construction is needed for a six-floor office building with three floors currently in use.
- Core equipment is on the first floor; networking devices are on each floor.

1.2.1 Requirement Collection and Analysis

Collect information such as:

1. Number of wired/wireless terminals
2. Project budget
3. Terminal types
4. Network management mode (e.g., SNMP)
5. Traffic volume and patterns
6. Redundancy and failover requirements
7. Security needs
8. Internet access method
9. Future expansion plans

1.2.2 Planning and Design Task

Design a physical topology for the network considering:

- Device selection based on terminal counts (wired: 10+200+200+500; wireless: 100+50+50+200)
- Ensure bandwidth requirements (100 Mbit/s for computers, 2 Mbit/s per wireless client)
- Deploy at least three dual-band APs per floor for quality wireless access

1.3 Layer 2 Network Design

Requirements:

1. **Wired Network VLANs:**
    - Assign ports GE0/0/1 to GE0/0/10 on the core equipment room's access switch to a single VLAN for server connectivity.
    - In the general manager's office on the second floor (connected via F2-ACC2), create a unique VLAN separate from the administrative department's VLAN.

- On the third floor, allocate ports E0/0/1 to E0/0/10 on switches F3-ACC1 and F3-ACC3 to the marketing department's VLAN; assign ports E0/0/11 to E0/0/20 for R&D department use.
- Designate all ports from E0/0/1 to E0/0/19 on F3-ACC2 for marketing department VLAN access.

2. **Wireless Network VLANs:**
    - Ensure wireless terminals across different floors are assigned distinct VLANs.
    - Implement individual wireless network management VLANs specific to each floor.
      Proposed VLAN Structure:

- **Servers:** VLAN 100
- **General Manager's Office (second floor):** VLAN 101
- **Administrative Department (second floor):** VLAN 102
- **Marketing Department (third floor):** VLAN 103
- **R&D Department (third floor):** VLAN 104
- **Wireless Terminals:**
    - **First Floor:** VLAN 105
    - **Second Floor:** VLAN 106
    - **Third Floor:** VLAN 107
- **Layer 2 Management:**
    - **First Floor:** VLAN 1
    - **Second Floor:** VLAN 2
    - **Third Floor:** VLAN 3
- **Additional Interconnection and Management:**
    - **F2-AGG1 to CORE1 Link:** VL201
        - **F3-AGG1 to CORE1 Link**: VL202
        - **F2-AGG1 to F3-AGG1 Link:** VL203
        - **CORE1to Router Link :** VL204
- **Wireless Network Management VLANS :**

- **First Floor :** VL205
- **Second Floor :** VL206
- **ThirdFloor :** VL207

VLAN ID	Description
1	Management VLAN - 1st Floor Layer 2 Devices
2	Management VLAN - 2nd Floor Layer 2 Devices
3	Management VLAN - 3rd Floor Layer 2 Devices
100	Servers VLAN
101	General Manager's Office VLAN
102	Administrative Department VLAN
103	Marketing Department VLAN
104	R&D Department VLAN
105	Wireless Terminals VLAN - 1st Floor
106	Wireless Terminals VLAN - 2nd Floor
107	Wireless Terminals VLAN - 3rd Floor
201	Interconnect F2-AGG1 to CORE1
202	Interconnect F3-AGG1 to CORE1
203	Interconnect F2-AGG1 to F3-AGG1
204	Interconnect CORE1 to Router
205	Wireless Network Management VLAN - 1st Floor
206	Wireless Network Management VLAN - 2nd Floor
207	Wireless Network Management VLAN - Third Floor

1.3.1 CORE1 Switch Configuration

Markdown

```
[CORE1]interface GigabitEthernet0/0/1
[CORE1-GigabitEthernet0/0/1]port link-type trunk
[CORE1-GigabitEthernet0/0/1]port trunk allow-pass vlan
100 105 205
```

```
ORE1-GigabitEthernet0/0/1]interface
gabitEthernet0/0/2
ORE1-GigabitEthernet0/0/2]port link-type access
ORE1-GigabitEthernet0/0/2]port default vlan 201
ORE1-GigabitEthernet0/0/2]interface
gabitEthernet0/0/3
ORE1-GigabitEthernet0/0/3]port link-type access
ORE1-GigabitEthernet0/0/3]port default vlan 202
ORE1-GigabitEthernet0/0/3]interface
GigabitEthernet0/0/4
[CORE1-GigabitEthernet0/0/4]port link-type access
[CORE1-GigabitEthernet0/0/4]port default vlan 205
[CORE1-GigabitEthernet0/0/4]interface
GigabitEthernet0/0/5
[CORE1-GigabitEthernet0/0/5]port link-type access
[CORE1-GigabitEthernet0/0/5]port default vlan 204
```

Code Explanation

- Sets the port to trunk mode.
- Allows VLANs 100, 105, and 205 to pass through, which are server VLAN, wireless terminals on the first floor, and wireless network management on the first floor respectively.
- Configures the port as an access port with a specified default VLAN for interconnections between switches and routers.
- Each interface is assigned to a different VLAN for segregating traffic.

1.3.2 F2-AGG1 Switch Configuration

Markdown

```
[F2-AGG1]interface GigabitEthernet0/0/1
[F2-AGG1-GigabitEthernet0/0/1]port link-type access
[F2-AGG1-GigabitEthernet0/0/1]port default vlan 201
```

```
[F2-AGG1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F2-AGG1-GigabitEthernet0/0/2]port link-type access
[F2-AGG1-GigabitEthernet0/0/2]port default vlan 203
[F2-AGG1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/11
[F2-AGG1-GigabitEthernet0/0/11]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/11]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/11]port trunk allow-pass vlan 2 102
[F2-AGG1-GigabitEthernet0/0/11]interface GigabitEthernet0/0/12
[F2-AGG1-GigabitEthernet0/0/12]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/12]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/12]port trunk allow-pass vlan 2 101 106 206
[F2-AGG1-GigabitEthernet0/0/12]interface GigabitEthernet0/0/13
[F2-AGG1-GigabitEthernet0/0/13]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/13]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/13]port trunk allow-pass vlan 2 102
```

Code Explanation

- Configures the port as an access port for interconnection with CORE1 (vlan 201).
- Configured as trunk ports to manage traffic from multiple VLANs - General Manager's Office (vlan 101), Administrative Department (vlan 102), and Wireless Networks (vlans 106 & 206).
- Sets up links to other switches for aggregation purposes.
- Assigns appropriate VLANs for these inter-switch connections.
- Configures ports in trunk mode with allowed VLANs for different departments.
- PVID (Primary VLAN ID) is used where untagged frames are assigned this VLAN.

1.3.3 F3-AGG1 Switch Configuration

```
[F3-AGG1]interface GigabitEthernet0/0/1
[F3-AGG1-GigabitEthernet0/0/1]port link-type access
[F3-AGG1-GigabitEthernet0/0/1]port default vlan 202
[F3-AGG1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F3-AGG1-GigabitEthernet0/0/2]port link-type access
[F3-AGG1-GigabitEthernet0/0/2]port default vlan 203
[F3-AGG1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/11
[F3-AGG1-GigabitEthernet0/0/11]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/11]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/11]port trunk allow-pass vlan 3 103 to 104
[F3-AGG1-GigabitEthernet0/0/11]interface GigabitEthernet0/0/12
[F3-AGG1-GigabitEthernet0/0/12]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/12]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/12]port trunk allow-pass vlan 3 103 107 207
[F3-AGG1-GigabitEthernet0/0/12]interface GigabitEthernet0/0/13
[F3-AGG1-GigabitEthernet0/0/13]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/13]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/13]port trunk allow-pass vlan 3 103 to 104
```

Code Explanation

- Similar configuration logic applies here as with F2-AGG1 but this time for third-floor departments like Marketing (vlan 103) and R&D (vlan 104), along with Wireless Networks (vlans 107 & 207).

- Specifies ports in trunk mode with permitted VLANs for different departments on the third floor.

1.3.4 Access Switches Configuration

1.3.4.1 Specific Floor Configurations

Each floor has its specific configuration based on departmental requirements:

1.3.4.1.1 First Floor Access Switches (F1-ACC1-2)

Markdown

```
[F1-ACC1]interface GigabitEthernet0/0/1
[F1-ACC1-GigabitEthernet0/0/1]port link-type trunk
[F1-ACC1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 105 205
[F1-ACC1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F1-ACC1-GigabitEthernet0/0/2]port link-type access
[F1-ACC1-GigabitEthernet0/0/2]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/3
[F1-ACC1-GigabitEthernet0/0/3]port link-type access
[F1-ACC1-GigabitEthernet0/0/3]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/4
[F1-ACC1-GigabitEthernet0/0/4]port link-type access
[F1-ACC1-GigabitEthernet0/0/4]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/4]interface GigabitEthernet0/0/5
```

```
[F1-ACC1-GigabitEthernet0/0/5]port link-type access
[F1-ACC1-GigabitEthernet0/0/5]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/5]interface
GigabitEthernet0/0/6
[F1-ACC1-GigabitEthernet0/0/6]port link-type access
[F1-ACC1-GigabitEthernet0/0/6]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/6]interface
GigabitEthernet0/0/7
[F1-ACC1-GigabitEthernet0/0/7]port link-type access
[F1-ACC1-GigabitEthernet0/0/7]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/7]interface
GigabitEthernet0/0/8
[F1-ACC1-GigabitEthernet0/0/8]port link-type access
[F1-ACC1-GigabitEthernet0/0/8]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/8]interface
GigabitEthernet0/0/9
[F1-ACC1-GigabitEthernet0/0/9]port link-type access
[F1-ACC1-GigabitEthernet0/0/9]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/9]interface
GigabitEthernet0/0/10
[F1-ACC1-GigabitEthernet0/0/10]port link-type access
[F1-ACC1-GigabitEthernet0/0/10]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/10]interface
GigabitEthernet0/0/20
[F1-ACC1-GigabitEthernet0/0/20]port link-type trunk
[F1-ACC1-GigabitEthernet0/0/20]port trunk pvid vlan 205
[F1-ACC1-GigabitEthernet0/0/20]port trunk allow-pass
vlan 105 205
```

Code Explanation

- Configured primarily for server connections (`vlan 100`) and wireless terminals (`vlan 105`).
- Configuration same idea for F1-ACC2

1.3.4.1.2 Second Floor Access Switches (F2-ACC1-3)

Markdown

```
[F2-ACC1]interface Ethernet0/0/1
[F2-ACC1-Ethernet0/0/1]port link-type access
[F2-ACC1-Ethernet0/0/1]port default vlan 102
[F2-ACC1-Ethernet0/0/1]interface Ethernet0/0/2
[F2-ACC1-Ethernet0/0/2]port link-type access
[F2-ACC1-Ethernet0/0/2]port default vlan 102
[F2-ACC1-Ethernet0/0/2]interface Ethernet0/0/3
[F2-ACC1-Ethernet0/0/3]port link-type access
[F2-ACC1-Ethernet0/0/3]port default vlan 102
[F2-ACC1-Ethernet0/0/3]interface Ethernet0/0/4
[F2-ACC1-Ethernet0/0/4]port link-type access
[F2-ACC1-Ethernet0/0/4]port default vlan 102
[F2-ACC1-Ethernet0/0/4]interface Ethernet0/0/5
[F2-ACC1-Ethernet0/0/5]port link-type access
[F2-ACC1-Ethernet0/0/5]port default vlan 102
[F2-ACC1-Ethernet0/0/5]interface Ethernet0/0/6
[F2-ACC1-Ethernet0/0/6]port link-type access
[F2-ACC1-Ethernet0/0/6]port default vlan 102
[F2-ACC1-Ethernet0/0/6]interface Ethernet0/0/7
[F2-ACC1-Ethernet0/0/7]port link-type access
[F2-ACC1-Ethernet0/0/7]port default vlan 102
[F2-ACC1-Ethernet0/0/7]interface Ethernet0/0/8
[F2-ACC1-Ethernet0/0/8]port link-type access
[F2-ACC1-Ethernet0/0/8]port default vlan 102
[F2-ACC1-Ethernet0/0/8]interface Ethernet0/0/9
[F2-ACC1-Ethernet0/0/9]port link-type access
[F2-ACC1-Ethernet0/0/9]port default vlan 102
[F2-ACC1-Ethernet0/0/9]interface Ethernet0/0/10
[F2-ACC1-Ethernet0/0/10]port link-type access
[F2-ACC1-Ethernet0/0/10]port default vlan 102
[F2-ACC1-Ethernet0/0/10]interface Ethernet0/0/11
[F2-ACC1-Ethernet0/0/11]port link-type access
[F2-ACC1-Ethernet0/0/11]port default vlan 102
```

```
[F2-ACC1-Ethernet0/0/11]interface Ethernet0/0/12
[F2-ACC1-Ethernet0/0/12]port link-type access
[F2-ACC1-Ethernet0/0/12]port default vlan 102
[F2-ACC1-Ethernet0/0/12]interface Ethernet0/0/13
[F2-ACC1-Ethernet0/0/13]port link-type access
[F2-ACC1-Ethernet0/0/13]port default vlan 102
[F2-ACC1-Ethernet0/0/13]interface Ethernet0/0/14
[F2-ACC1-Ethernet0/0/14]port link-type access
[F2-ACC1-Ethernet0/0/14]port default vlan 102
[F2-ACC1-Ethernet0/0/14]interface Ethernet0/0/15
[F2-ACC1-Ethernet0/0/15]port link-type access
[F2-ACC1-Ethernet0/0/15]port default vlan 102
[F2-ACC1-Ethernet0/0/15]interface Ethernet0/0/16
[F2-ACC1-Ethernet0/0/16]port link-type access
[F2-ACC1-Ethernet0/0/16]port default vlan 102
[F2-ACC1-Ethernet0/0/16]interface Ethernet0/0/17
[F2-ACC1-Ethernet0/0/17]port link-type access
[F2-ACC1-Ethernet0/0/17]port default vlan 102
[F2-ACC1-Ethernet0/0/17]interface Ethernet0/0/18
[F2-ACC1-Ethernet0/0/18]port link-type access
[F2-ACC1-Ethernet0/0/18]port default vlan 102
[F2-ACC1-Ethernet0/0/18]interface Ethernet0/0/19
[F2-ACC1-Ethernet0/0/19]port link-type access
[F2-ACC1-Ethernet0/0/19]port default vlan 102
[F2-ACC1-Ethernet0/0/19]interface Ethernet0/0/20
[F2-ACC1-Ethernet0/0/20]port link-type access
[F2-ACC1-Ethernet0/0/20]port default vlan 102
[F2-ACC1-Ethernet0/0/20]interface Ethernet0/0/21
[F2-ACC1-Ethernet0/0/21]port link-type access
[F2-ACC1-Ethernet0/0/21]port default vlan 102
[F2-ACC1-Ethernet0/0/21]interface Ethernet0/0/22
[F2-ACC1-Ethernet0/0/22]port link-type access
[F2-ACC1-Ethernet0/0/22]port default vlan 102
[F2-ACC1-GigabitEthernet0/0/1]interface
GigabitEthernet0/0/1
[F2-ACC1-GigabitEthernet0/0/1]port link-type trunk
```

```
[F2-ACC1-GigabitEthernet0/0/1]port trunk pvid vlan 2
[F2-ACC1-GigabitEthernet0/0/1]port trunk allow-pass
vlan 2 102
```

Code Explanation

- Configured for General Manager's Office (`vlan 101`) and Administrative Department (`vlan 102`). Separate wireless network configurations are also included (`vlans 106 & 206`).
- Configuration same idea for F2-ACC2 and F2-ACC3

1.3.4.1.3 Third Floor Access Switches (F3-ACCX)

Markdown

```
[F3-ACC1]interface Ethernet0/0/1
[F3-ACC1-Ethernet0/0/1]port link-type access
[F3-ACC1-Ethernet0/0/1]port default vlan 103
[F3-ACC1-Ethernet0/0/1]interface Ethernet0/0/2
[F3-ACC1-Ethernet0/0/2]port link-type access
[F3-ACC1-Ethernet0/0/2]port default vlan 103
[F3-ACC1-Ethernet0/0/2]interface Ethernet0/0/3
[F3-ACC1-Ethernet0/0/3]port link-type access
[F3-ACC1-Ethernet0/0/3]port default vlan 103
[F3-ACC1-Ethernet0/0/3]interface Ethernet0/0/4
[F3-ACC1-Ethernet0/0/4]port link-type access
[F3-ACC1-Ethernet0/0/4]port default vlan 103
[F3-ACC1-Ethernet0/0/4]interface Ethernet0/0/5
[F3-ACC1-Ethernet0/0/5]port link-type access
[F3-ACC1-Ethernet0/0/5]port default vlan 103
[F3-ACC1-Ethernet0/0/5]interface Ethernet0/0/6
[F3-ACC1-Ethernet0/0/6]port link-type access
[F3-ACC1-Ethernet0/0/6]port default vlan 103
[F3-ACC1-Ethernet0/0/6]interface Ethernet0/0/7
[F3-ACC1-Ethernet0/0/7]port link-type access
```

```
[F3-ACC1-Ethernet0/0/7]port default vlan 103
[F3-ACC1-Ethernet0/0/7]interface Ethernet0/0/8
[F3-ACC1-Ethernet0/0/8]port link-type access
[F3-ACC1-Ethernet0/0/8]port default vlan 103
[F3-ACC1-Ethernet0/0/8]interface Ethernet0/0/9
[F3-ACC1-Ethernet0/0/9]port link-type access
[F3-ACC1-Ethernet0/0/9]port default vlan 103
[F3-ACC1-Ethernet0/0/9]interface Ethernet0/0/10
[F3-ACC1-Ethernet0/0/10]port link-type access
[F3-ACC1-Ethernet0/0/10]port default vlan 103
[F3-ACC1-Ethernet0/0/10]interface Ethernet0/0/11
[F3-ACC1-Ethernet0/0/11]port link-type access
[F3-ACC1-Ethernet0/0/11]port default vlan 104
[F3-ACC1-Ethernet0/0/11]interface Ethernet0/0/12
[F3-ACC1-Ethernet0/0/12]port link-type access
[F3-ACC1-Ethernet0/0/12]port default vlan 104
[F3-ACC1-Ethernet0/0/12]interface Ethernet0/0/13
[F3-ACC1-Ethernet0/0/13]port link-type access
[F3-ACC1-Ethernet0/0/13]port default vlan 104
[F3-ACC1-Ethernet0/0/13]interface Ethernet0/0/14
[F3-ACC1-Ethernet0/0/14]port link-type access
[F3-ACC1-Ethernet0/0/14]port default vlan 104
[F3-ACC1-Ethernet0/0/14]interface Ethernet0/0/15
[F3-ACC1-Ethernet0/0/15]port link-type access
[F3-ACC1-Ethernet0/0/15]port default vlan 104
[F3-ACC1-Ethernet0/0/15]interface Ethernet0/0/16
[F3-ACC1-Ethernet0/0/16]port link-type access
[F3-ACC1-Ethernet0/0/16]port default vlan 104
[F3-ACC1-Ethernet0/0/16]interface Ethernet0/0/17
[F3-ACC1-Ethernet0/0/17]port link-type access
[F3-ACC1-Ethernet0/0/17]port default vlan 104
[F3-ACC1-Ethernet0/0/17]interface Ethernet0/0/18
[F3-ACC1-Ethernet0/0/18]port link-type access
[F3-ACC1-Ethernet0/0/18]port default vlan 104
[F3-ACC1-Ethernet0/0/18]interface Ethernet0/0/19
[F3-ACC1-Ethernet0/0/19]port link-type access
```

```
[F3-ACC1-Ethernet0/0/19]port default vlan 104
[F3-ACC1-Ethernet0/0/19]interface Ethernet0/0/20
[F3-ACC1-Ethernet0/0/20]port link-type access
[F3-ACC1-Ethernet0/0/20]port default vlan 104
[F3-ACC1-Ethernet0/0/20]interface GigabitEthernet0/0/1
[F3-ACC1-GigabitEthernet0/0/1]port link-type trunk
[F3-ACC1-GigabitEthernet0/0/1]port trunk pvid vlan 3
[F3-ACC1-GigabitEthernet0/0/1]port trunk allow-pass
vlan 3 103 to 104
```

Code Explanation

- Configured similarly with departments separated into Marketing (`vlan 103`) and R&D (`vlan104`). The wireless networks have their respective VLAN IDs (`vlans107 &207`).
- Configuration same idea for F3-ACC2 and F3-ACC3

1.4 Layer 3 Network Design

Layer 3 Network Design

- **Address Range:** 192.168.0.0/16
- **First Floor:**
  - **Servers:** Static IPs, Gateway = CORE1
  - **Wireless devices/APs:** DHCP by CORE1
  - **Access Switches:** Static management IPs, Gateway = CORE1
- **Second & Third Floors:**
  - **All Devices/APs:** DHCP by respective aggregation switch
  - **Access Switches:** Static management IPs, Gateway = respective aggregation switch
- **Routing Protocol:** OSPF for network-wide connectivity
- Internet Access through the router

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
192.168.1.0/24	Static addresses	CORE1	Default route to CORE1	L2 management network, first floor
192.168.2.0/24	Static addresses	F2-AGG1	Default route to F2-AGG1	L2 management network, second floor
192.168.3.0/24	Static addresses	F3-AGG	Default route to F3-AGG	L2 management network, third floor
192.168.100.0/24	Static addresses	CORE1	OSPF through gateway devices	Server network
192.168.101.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	General Manager's Office network
192.168.102.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	Administrative Department network
192.168.103.0/24	DHCP (F3-AGG1)	F3-AGG1	OSPF through gateway devices	Marketing Department network
192.168.104.0/24	DHCP (F3-AGG1)	F3-AGG1	OSPF through gateway devices	R&D Department network
192.168.105.0/24	DHCP (CORE1)	CORE1	OSPF through gateway devices	Wireless terminals network, first floor

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
192.168.106.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	Wireless terminals network, second floor
192.168.107.0/24	DHCP (F3-AGG1)	F3-AGG1	Advertised in OSPF through gateway devices	Wireless terminals on the third floor
192.168.201.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F2-AGG1 and CORE1
192.168.202.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F3-AGG1 and CORE1
192.168.203.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F2-AGG1 and F3-AGG1
192.168.204.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between CORE1 and router
192.168.205.0/24	DHCP (CORE1)	CORE1	Advertised in OSPF through gateway devices	Wireless network management network on the first floor
192.168.206.0/24	DHCP (F2-AGG1)	F2-AGG1	Advertised in OSPF through gateway devices	Wireless network management network on the second floor
192.168.207.0/24	DHCP (F3-AGG1)	F3-AGG1	Advertised in OSPF through	Wireless network management

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
			gateway devices	network on the third floor

1.4.1 Router Configuration

> Configures OSPF for dynamic routing across different network segments defined by their respective VLANs.

Markdown

```
[Router]ospf 1
[Router-ospf-1]area 0.0.0.0
[Router-ospf-1-area-0.0.0.0]network 192.168.204.0
0.0.0.3
```

Code Explanation

- **area 0.0.0.0**: Specifies the OSPF area as area 0, which is typically the backbone area in OSPF.
- **network 192.168.204.0 0.0.0.3**: Includes the interface with an IP address within the specified range (192.168.204.0-2) to OSPF area 0.

1.4.2 CORE1 Configuration

> Acts as a central point of connectivity between different VLANs and performs inter-VLAN routing using SVIs.

Markdown

```
[CORE]interface Vlanif1
```

```
[CORE1-Vlanif1]ip address 192.168.1.254 255.255.255.0
[CORE1-Vlanif1]interface Vlanif100
[CORE1-Vlanif100]ip address 192.168.100.254
255.255.255.0
[CORE1-Vlanif100]interface Vlanif201
[CORE1-Vlanif201]ip address 192.168.201.1
255.255.255.252
[CORE1-Vlanif201]interface Vlanif202
[CORE1-Vlanif202]ip address 192.168.202.1
255.255.255.252
[CORE1-Vlanif202]interface Vlanif204
[CORE1-Vlanif204]ip address 192.168.204.2
255.255.255.252
[CORE1-Vlanif204]ospf 1
[CORE1-ospf-1]area 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0]network 192.168.1.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.100.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.105.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.205.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.201.0
0.0.0.3
[CORE1-ospf-1-area-0.0.0.0]network 192.168.202.0
0.0.0.3
[CORE1-ospf-1-area-0.0.0.0]network 192.168.204.0
0.0.0.3
```

Code Explanation

- **CORE1**: The core switch/router in the network, handling inter-VLAN routing and OSPF for Layer 3 communication.
- **interface VlanifX**: Each `Vlanif` command configures an SVI (Switched Virtual Interface) for a particular VLAN, assigning an IP address and subnet mask to that VLAN interface.

- **Example:**
- **Vlanif1**: This is the VLAN interface for VLAN ID 1, which is for Layer 2 de| IP Network	Address Assignment	Gateway	Routing Configuration	Network Description
  Enables OSPF routing protocol with process ID of `1`.
- Each **network** command adds respective networks to OSPF, allowing routers to share routes within these networks.

1.4.3 F2-AGG1 Configuration

> Aggregate connections from access switches on their respective floors and perform routing functions within their scope of responsibility.

Markdown

```
[FG2-AGG1]ip pool admin
[FG2-AGG1-ip-pool-admin]gateway-list 192.168.102.254
[FG2-AGG1-ip-pool-admin]network 192.168.102.0 mask
255.255.255.0
[FG2-AGG1-ip-pool-admin]ip pool manager
[FG2-AGG1-ip-pool-manager]gateway-list 192.168.101.254
[FG2-AGG1-ip-pool-manager]network 192.168.101.0 mask
255.255.255.0
[FG2-AGG1-ip-pool-manager]interface Vlanif2
[FG2-AGG1-Vlanif2]ip address 192.168.2.254
255.255.255.0
[FG2-AGG1-Vlanif2]interface Vlanif101
[FG2-AGG1-Vlanif101]ip address 192.168.101.254
255.255.255.0
[FG2-AGG1-Vlanif101]dhcp select global
[FG2-AGG1-Vlanif102]interface Vlanif102
[FG2-AGG1-Vlanif102]ip address 192.168.102.254
255.255.255.0
[FG2-AGG1-Vlanif102]dhcp select global
```

```
[FG2-AGG1-Vlanif102]interface Vlanif201
[FG2-AGG1-Vlanif201]ip address 192.168.201.2
255.255.255.252
[FG2-AGG1-Vlanif201]interface Vlanif203
[FG2-AGG1-Vlanif203]ip address 192.168.203.1
255.255.255.252
[FG2-AGG1-Vlanif203]ospf 1
[FG2-AGG1-ospf-1]area 0.0.0.0
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.2.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.101.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.102.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.106.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.201.0
0.0.0.3
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.203.0
0.0.0.3
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.206.0
0.0.0.255
```

Code Explanation

- Defines DHCP pools for different departments on the second floor with specific gateway-list and network ranges.
- Similar to CORE1, defines interfaces and assigns IP addresses with gateways for different VLANs on F2-AGG1.
- Enables OSPF within specified areas and includes necessary networks into OSPF similar to CORE1's configuration but specific to F2-AGG1's connected networks.

1.4.4 F3-AGG1 Configuration

> Aggregate connections from access switches on their respective floors and perform routing functions within their scope of responsibility.

Markdown

```
[FG3-AGG1]ip pool marketing
[FG3-AGG1-ip-pool-marketing]gateway-list 192.168.103.254
[FG3-AGG1-ip-pool-marketing]network 192.168.103.0 mask 255.255.255.0
[FG3-AGG1-ip-pool-marketing]ip pool rd
[FG3-AGG1-ip-pool-id]gateway-list 192.168.104.254
[FG3-AGG1-ip-pool-id]network 192.168.104.0 mask 255.255.255.0
[FG3-AGG1-ip-pool-id]interface Vlanif3
[FG3-AGG1-Vlanif3]ip address 192.168.3.254 255.255.255.0
[FG3-AGG1-Vlanif3]interface Vlanif103
[FG3-AGG1-Vlanif103]ip address 192.168.103.254 255.255.255.0
[FG3-AGG1-Vlanif103]dhcp select global
[FG3-AGG1-Vlanif103]interface Vlanif104
[FG3-AGG1-Vlanif104]ip address 192.168.104.254 255.255.255.0
[FG3-AGG1-Vlanif104]dhcp select global
[FG3-AGG1-Vlanif104]interface Vlanif202
[FG3-AGG1-Vlanif202]ip address 192.168.202.2 255.255.255.252
[FG3-AGG1-Vlanif202]interface Vlanif203
[FG3-AGG1-Vlanif203]ip address 192.168.203.2 255.255.255.252
[FG3-AGG1-Vlanif203]ospf 1
[FG3-AGG1-ospf-1]area 0.0.0.0
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.103.0 0.0.0.255
```

```
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.104.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.107.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.202.0 0.0.0.3
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.203.0 0.0.0.3
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.207.0 0.0.0.255
```

Code Explanation

- This section mirrors F2-AGG1's approach but applies it to third-floor configurations, establishing DHCP pools and defining interfaces with correct IP addressing and gateways aligned with third-floor requirements.
- Defines DHCP pools for different departments on the second floor with specific gateway-list and network ranges.
- Similar to CORE1, defines interfaces and assigns IP addresses with gateways for different VLANs on F3-AGG1.
- Enables OSPF within specified areas and includes necessary networks into OSPF similar to CORE1's configuration but specific to F3-AGG1's connected networks.

1.4.5 Access Switches (ACC) Configuration Example (F1-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F1-ACC1]interface Vlanif1
[F1-ACC1-Vlanif1]ip address 192.168.1.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 1.

1.4.6 Access Switches (ACC) Configuration Example (F2-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC1]interface Vlanif2
[F2-ACC1-Vlanif2]ip address 192.168.2.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.7 Access Switches (ACC) Configuration Example (F2-ACC2)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC2]interface Vlanif1
```

```
[F2-ACC2-Vlanif1]interface Vlanif2
[F2-ACC2-Vlanif2]ip address 192.168.2.2 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.8 Access Switches (ACC) Configuration Example (F2-ACC3)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC3]interface Vlanif2
[F2-ACC3-Vlanif2]ip address 192.168.2.3 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.9 Access Switches (ACC) Configuration Example (F3-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC1]interface Vlanif3
```

```
[F3-ACC1-Vlanif3]ip address 192.168.3.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.4.10 Access Switches (ACC) Configuration Example (F3-ACC2)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC2]interface Vlanif3
[F3-ACC2-Vlanif3]ip address 192.168.3.2 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.4.11 Access Switches (ACC) Configuration Example (F3-ACC3)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC3]interface Vlanif3
[F3-ACC3-Vlanif3]ip address 192.168.3.3 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.5 WLAN Design

Design a WLAN with the following requirements:

- Centralized management of all APs by an Access Controller (AC) with limited forwarding capacity.
- APs on the first floor connect to the AC at Layer 2, while those on the second and third floors connect at Layer 3 via gateway CORE1.
- Implement unique SSIDs for each floor with WPA-WPA2+PSK+AES security, each having a distinct password.

Item	First Floor	Second Floor
WLAN		
AP Management VLAN	VLAN205	VLAN206
Service VLAN	VLAN105	VLAN106
DHCP Server	CORE1	F2-AGG1
AC's Source IP	**VLANIF205:**192.168.205.253/24	**VLANIF205:**192.168.205.253/
AP Group Name	WLAN-F1	WLAN-F2
Profiles		
VAP Profile	**Name:** WLAN-F1	**Name:** WLAN-F2
Regulatory Domain	- **Country code:** CN (default)	- **Country code**: CN (default)
SSID Profile	- **SSID name:** WLAN-F1	- **SSID name:** WLAN-F2

Item	First Floor	Second Floor
Security Profile	- WPA-WPA2+PSK+AES	- WPA-WPA2+PSK+AES
- Password:	--WLAN@Guest123	--WLAN@Employee2
- Forwarding Mode	--direct forwarding	--direct forwarding

1.5.1 CORE1 Configuration

Markdown

```
[CORE1]vlan batch 100 105 201 to 202 204 to 205
[CORE1]dhcp enable
[CORE1]ip pool ap-f1
[CORE1-ip-pool-ap-f1]gateway-list 192.168.205.254
[CORE1-ip-pool-ap-f1]network 192.168.205.0 mask
255.255.255.0
[CORE1-ip-pool-ap-f1]excluded-ip-address
192.168.205.253
[CORE1-ip-pool-sta-f1]ip pool sta-f1
[CORE1-ip-pool-sta-f1]gateway-list 192.168.105.254
[CORE1-ip-pool-sta-f1]network 192.168.105.0 mask
255.255.255.0
[CORE1-ip-pool-sta-f1]interface Vlanif105
[CORE1-Vlanif105]ip address 192.168.105.254
255.255.255.0
[CORE1-Vlanif105]dhcp select global

```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on CORE1.

- Defines an IP address pool named `ap-f1` for AP management on the first floor.
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the first floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN105, which is designated for wireless terminals on the first floor, and configures it to use global DHCP settings.

1.5.2 F2-AGG1 Configuration

Markdown

```
[F2-AGG1]vlan batch 2 101 to 102 106 201 203 206
[F2-AGG1]dhcp enable
[F2-AGG1]ip pool ap-f2
[F2-AGG1-ip-pool-ap-f2]gateway-list 192.168.206.254
[F2-AGG1-ip-pool-ap-f2]network 192.168.206.0 mask
255.255.255.0
[F2-AGG1-ip-pool-ap-f2]option 43 sub-option 3 ascii
192.168.205.253
[F2-AGG1-ip-pool-ap-f2]ip pool sta-f2
[F2-AGG1-ip-pool-sta-f2]gateway-list 192.168.106.254
[F2-AGG1-ip-pool-sta-f2]network 192.168.106.0 mask
255.255.255.0
[F2-AGG1-ip-pool-sta-f2]interface Vlanif106
[F2-AGG1-Vlanif106]ip address 192.168.106.254
255.255.255.0
[F2-AGG1-Vlanif106]dhcp select global
[F2-AGG1-Vlanif206]interface Vlanif206
[F2-AGG1-Vlanif206]ip address 192.168.206.254
255.255.255.0
```

```
15 [F2-AGG1-Vlanif206]dhcp select global
```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on F2-AGG1.
- Defines an IP address pool named `ap-f2` for AP management on the second floor.AP management (`ap-f2`) and service network (`sta-f2`).
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the second floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN106 and VLAN206, which is designated for wireless terminals and management on the second floor, and configures it to use global DHCP settings.

1.5.3 F3-AGG1 Configuration

Markdown

```
1 [F3-AGG1]vlan batch 3 103 to 104 107 202 to 203 207
2 [F3-AGG1]dhcp enable
3 [F3-AGG1]ip pool ap-f3
4 [F3-AGG1-ip-pool-ap-f3]gateway-list 192.168.207.254
5 [F3-AGG1-ip-pool-ap-f3]network 192.168.207.0 mask
  255.255.255.0
6 [F3-AGG1-ip-pool-ap-f3]option 43 sub-option 3 ascii
  192.168.205.253
7 [F3-AGG1-ip-pool-ap-f3]ip pool sta-f3
8 [F3-AGG1-ip-pool-sta-f3]gateway-list 192.168.107.254
```

```
[F3-AGG1-ip-pool-sta-f3]network 192.168.107.0 mask
255.255.255.0
[F3-AGG1-ip-pool-sta-f3]interface Vlanif107
[F3-AGG1-Vlanif107]ip address 192.168.107.254
255.255.255.0
[F3-AGG1-Vlanif107]dhcp select global
[F3-AGG1-Vlanif207]interface Vlanif207
[F3-AGG1-Vlanif207]ip address 192.168.207.254
255.255.255.0
dhcp select global
```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on F3-AGG1.
- Defines an IP address pool named `ap-f3` for AP management on the second floor.AP management (`ap-f3`) and service network (`sta-f3`).
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the thrid floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN107 and VLAN207, which is designated for wireless terminals and management on the thrid floor, and configures it to use global DHCP settings.

1.5.4 Access Controller (AC) Configuration

Markdown

```
[AC]vlan batch 205
[AC]interface Vlanif205
```

```
[AC-Vlanif205]ip address 192.168.205.253 255.255.255.0
[AC]q
[AC]capwap source interface vlanif205
[AC]wlan
[AC-wlan-view]security-profile name WLAN-F1
[AC-wlan-sec-prof-WLAN-F1]security wpa-wpa2 psk pass-phrase WLAN@Guest123 aes
[AC-wlan-sec-prof-WLAN-F1]security-profile name WLAN-F2
[AC-wlan-sec-prof-WLAN-F2]security wpa-wpa2 psk pass-phrase WLAN@Employee2 aes
[AC-wlan-sec-prof-WLAN-F2]security-profile name WLAN-F3
[AC-wlan-sec-prof-WLAN-F3]security wpa-wpa2 psk pass-phrase WLAN@Employee3 aes
[AC-wlan-sec-prof-WLAN-F3]ssid-profile name WLAN-F1
[AC-wlan-ssid-prof-WLAN-F1]ssid WLAN-F1
[AC-wlan-ssid-prof-WLAN-F1]ssid-profile name WLAN-F2
[AC-wlan-ssid-prof-WLAN-F2]ssid WLAN-F2
[AC-wlan-ssid-prof-WLAN-F2]ssid-profile name WLAN-F3
[AC-wlan-ssid-prof-WLAN-F3]ssid WLAN-F3
[AC-wlan-ssid-prof-WLAN-F3]vap-profile name WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]service-vlan vlan-id 105
[AC-wlan-vap-prof-WLAN-F1]ssid-profile WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]security-profile WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]vap-profile name WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]service-vlan vlan-id 106
[AC-wlan-vap-prof-WLAN-F2]ssid-profile WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]security-profile WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]vap-profile name WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]service-vlan vlan-id 107
[AC-wlan-vap-prof-WLAN-F3]ssid-profile WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]security-profile WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]ap-group name WLAN-F1
[AC-wlan-ap-group-WLAN-F1]radio 0
[AC-wlan-group-radio-WLAN-F1/0]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/0]radio 1
```

```
[AC-wlan-group-radio-WLAN-F1/1]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/1]radio 2
[AC-wlan-group-radio-WLAN-F1/2]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/2]ap-group name WLAN-F2
[AC-wlan-ap-group-WLAN-F2]radio 0
[AC-wlan-group-radio-WLAN-F2/0]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/0]radio 1
[AC-wlan-group-radio-WLAN-F2/1]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/1]radio 2
[AC-wlan-group-radio-WLAN-F2/2]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/2]ap-group name WLAN-F3
[AC-wlan-ap-group-WLAN-F3]radio 0
[AC-wlan-group-radio-WLAN-F3/0]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/0]radio 1
[AC-wlan-group-radio-WLAN-F3/1]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/1]radio 2
[AC-wlan-group-radio-WLAN-F3/2]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/2]ap-id 0 type-id 60 ap-mac xxx
[AC-wlan-ap-0]ap-name F1-AP1
[AC-wlan-ap-0]ap-group WLAN-F1
[AC-wlan-ap-0]ap-id 1 type-id 60 ap-mac xxx
[AC-wlan-ap-1]ap-name F2-AP1
[AC-wlan-ap-1]ap-group WLAN-F2
[AC-wlan-ap-1]ap-id 2 type-id 60 ap-mac xxx
[AC-wlan-ap-2]ap-name F3-AP1
[AC-wlan-ap-2]ap-group WLAN-F3
```

Code Explanation

- Sets up the management interface for wireless networks on the first floor with specific security profiles per SSID, including WPA2 Personal encryption and pre-shared keys.
- `capwap source interface vlanif205` : Sets the source interface of CAPWAP control messages sent by AC to APs.
- For each AP group corresponding to a different floor (`WLAN-F1` , `WLAN-F2` , `WLAN-F3`), Virtual AP profiles are assigned along with SSID profiles that define network names and security settings.
- `security-profile` : Defines security settings like WPA/WPA2 PSK and AES encryption keys per floor SSID.
- `ssid-profile` : Associates SSID names with profiles created earlier in the config.
- `vap-profile` : Configures virtual access points with forwarding modes along with their respective service VLAN IDs.
- `ap-id ... type-id ... ap-mac ...` : Registers each AP by specifying its ID, type, MAC address, and associates it with a predefined group according to its location.

1.5.5 F1-ACC1,F2-ACCx,F3-ACCx

> For each ACC device (`F1-ACC1` , `F2-ACCx` , `F3-ACCx`), create relevant VLAN batches that match their respective locations within the building structure:

Example: `F2-ACC1`

Markdown

```
[F2-ACC1]vlan batch 2 102
```

> This assigns specific VLAN IDs required by that access point's location within the building structure.

1.6 Security and Egress Design

Requirements :

1. Guest WiFi access is restricted to the Internet only, no intranet access.
2. Only wireless devices can connect to the Internet.
3. Router has a static IP range of 1.1.1.1 to 1.1.1.10/24 with a gateway of 1.1.1.254.
4. External users must access an internal web server at 192.168.100.1 on port 80, using NAT for security and restricted to web services only.

Requirement Title	Implementation Detail	Applicable Device
Intranet Access Control	Configure a traffic filter or policy on CORE1 for guest access control.	CORE1
Internet Access Control	Enable NAT on the router but disable address translation for specific networks.	Router
Web Server Mapping	Configure NAT server on the router interface to manage web server accessibility.	Router

1.6.1 Router Configuration

Markdown

```
[Router]acl number 2000
[Router-acl-basic-2000]rule 5 permit source 192.168.105.0 0.0.0.255
[Router-acl-basic-2000]rule 10 permit source 192.168.106.0 0.0.0.255
[Router-acl-basic-2000]rule 15 permit source 192.168.107.0 0.0.0.255
[Router-acl-basic-2000]q
[Router]nat address-group 1 1.1.1.2 1.1.1.10
```

```
[Router]interface GigabitEthernet0/0/0
[Router-GigabitEthernet0/0/0]ip address 1.1.1.1 255.255.255.0
[Router-GigabitEthernet0/0/0]nat server protocol tcp global current-interface 8080 inside 192.168.100.1 www
[Router-GigabitEthernet0/0/0]nat outbound 2000 address-group 1
[Router-GigabitEthernet0/0/0]q
[Router]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

IP	Description
192.168.105.0/24	Network of the wireless terminals on the first floor
192.168.106.0/24	Network of the wireless terminals on the second floor
192.168.107.0/24	Network of the wireless terminals on the third floor

Code Explanation

- **ACL (Access Control List)**: Defines a set of rules that filter traffic based on IP addresses.
- `rule` **lines:** Permit traffic from the specified wireless VLANs (for guests).
- **NAT Address Group**: Defines a range of public IP addresses `(1.1.1.2 to 1.1.1.10)` for NAT (Network Address Translation) to use when translating private IP addresses to public ones.
- Configures the IP address for `GigabitEthernet interface 0/0/0` on the router for network subnet for public network.
- Configures static NAT to map the internal web server's private IP (`192.168.100.1`) and port (`80`) to an external IP on port `8080` .
- `nat outbound` : Applies NAT to traffic matched by ACL `2000` , using the defined address group.
- Enables dynamic NAT for outbound traffic, using the defined address group for translation `(1.1.1.2 to 1.1.1.10)` .
- Configures a default static route with next-hop IP address as `1.1.1.254` (ISP Gateway).

1.6.2 CORE Switch Configuration

```Markdown
[CORE]acl number 3000
[CORE-acl-basic-2000]rule 5 deny ip source 192.168.105.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
[CORE-acl-basic-2000]rule 10 permit ip
```

Code Explanation

- Defines an ACL with ID `30000` that denies guest VLAN traffic (`192.168.105.0`).
- Allows all other IP traffic by default, ensuring guests cannot access internal networks but can reach other destinations (typically, this means internet access only).

1.6.3 Aggregation and Access Layer Switches

> For switches `F2-AGG` , `F3-AGG` , and access layer switches (`F-ACC`), static routes are configured:

1.6.4 F1-ACC1 Switch Example

```Markdown
[F1-ACC1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
```

> - Sets a default static route pointing to its uplink gateway at `192.168.1.254` . Replace `1` with appropriate floor number and device number based on your topology like `F2` number is `2` .

1.6.5 AC Configuration (Wireless Access Controller)

```Markdown
[AC]ip route-static 0.0.0.0 0.0.0.0 192.168.205.25
```

- Sets a default static route pointing to its uplink gateway at `192.168.205.25` .

1.7 Network Management Design

Requirement:

- Utilize SNMPv3 with authentication and encryption for NMS communication.
- Devices use management VLAN to reach NMS at 192.168.100.2/24, except routers and AC.
- Routers interface with NMS via GE0/0/1.
- AC connects to NMS using VLANIF 205.
- All devices should send SNMP alarms to the NMS.

1.7.1 Router Configuration

```Markdown
[Router]snmp-agent sys-info version v3
[Router]snmp-agent group v3 datacom privacy
[Router]snmp target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datacom
[Router]snmp target-host trap-paramsname datacom v3 securityname test privacy
[Router]snmp usm-user v3 test datacom authentication-mode md5 huaweilab privacy-mode aes128 huaweilab
[Router]snmp-agent trap source GigabitEthernet0/0/1
```

```
[Router]snmp-agent trap enable
[Router]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162.
- Configures trap parameters with a security name of `test` and privacy (encryption) enabled.
- Sets up a user-based security model (USM) user named `test` in group `datacom`. Authentication uses MD5 with the password `huaweilab`, and encryption uses AES128 with the same password.
- Sets the source interface for sending traps to NMS as GigabitEthernet0/0/1.
- Enables the device to send traps to the NMS server.

1.7.2 CORE1 and Other Switches Configuration (Similar for F2/F3-AGG1, F1/F2/F3-ACC1/ACC2/ACC3)

Markdown

```
[CORE1]snmp-agent sys-info version v3
[CORE1]snmp-agent group v3 datacom privacy
[CORE1]snmp-agent target-host trap address udp-domain
192.168.100.2 params securityname datacom v3
[CORE1]snmp usm-user v3 test datacom authentication-
mode md5 huaweilab privacy-mode aes128 huaweilab
[CORE1]snmp-agent trap source vlanif1
[CORE1]snmp-agent trap enable
[CORE1]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162. under security under datacom name
- Sets up a user-based security model (USM) user named `test` in group `datacom`. Authentication uses MD5 with the password `huaweilab`, and encryption uses AES128 with the same password.
- Enables the device to send traps to the NMS server.
- Replace `vlanif1` 1 with VLAN interface number specific to each device; sets this as the source for SNMP traps.

1.7.2.1 Device-Specific Configurations

Device	Trap Source Interface	NMS Communication Path
Router	GE0/0/1	Directly through GE0/0/1
CORE1	VLANIF1	Via management VLAN1
F2-AGG1	VLANIF2	Via management VLAN2
F3-AGG1	VLANIF3	Via management VLAN3
AC	VLANIF205	Via specific VLANIF205
F1-ACC1	VLANIF1	Via management VLANIF1
F2-ACC2	VLANIF2	Via management VLANIF2
F2-ACC3	VLANIF2	Via management VLANIF2
F3-ACC1	VLANIF3	Via management VLANIF3
F3-ACC2	VLANIF3	Via management VLANIF3
F3-ACC3	VLANIF3	Via management VLANIF3

1.7.3 AC (Access Controller) Configuration

```
[AC]snmp-agent sys-info version v3
[AC]snmp-agent group v3 datacom privacy
[AC]snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datacom v3
[AC]snmp usm-user v3 test datacom authentication-mode md5 huaweilab privacy-mode aes128 huaweilab
[AC]snmp-agent trap source vlanif205
[AC]snmp-agent trap enable
[AC]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162. under security under datacom name
- Sets up a user-based security model (USM) user named `test` in group `datacom` . Authentication uses MD5 with the password `huaweilab` , and encryption uses AES128 with the same password.
- Enables the device to send traps to the NMS server.
- Sets VLAN interface 205 as the source of SNMP traps for communication with NMS.

1.8 Quiz

Question1

In your project, you have three devices (CORE1, F2-AGG1, and F3-AGG1) that are connected in a circle, which is called a physical ring. To avoid any

issues with data loops (where data could go around in circles forever), you've put each connecting link into its own separate VLAN (a virtual network within your physical network).

✓ **Answer1**

- You thought that by doing this, you wouldn't have any loops because each VLAN is like a separate path. However, during testing, you found that two of the devices are not talking to each other properly - they're not becoming neighbors as they should.
- The problem is that even though you've separated the links into different VLANs to stop loops at the network layer, there's still a loop at the physical layer - the actual cables and devices are still forming a ring. Normally, Spanning Tree Protocol (STP) helps prevent these kinds of loops by blocking some paths. But STP doesn't understand VLAN tags - it just sees one big network.
- So what's likely happening here is that STP has blocked one of your links to prevent a loop. But since you've already separated the paths with VLANs (which STP isn't aware of), this block is unnecessary and it's stopping your devices from communicating.
- The solution? Since you've already organized loop prevention with VLANs, you can safely turn off STP on the links between these three devices. This will allow them to talk to each other without STP blocking any of them. Just make sure that your VLAN-based separation really prevents all possible loops before disabling STP to avoid any potential issues.