# Huawei ICT Competition 2018-2019

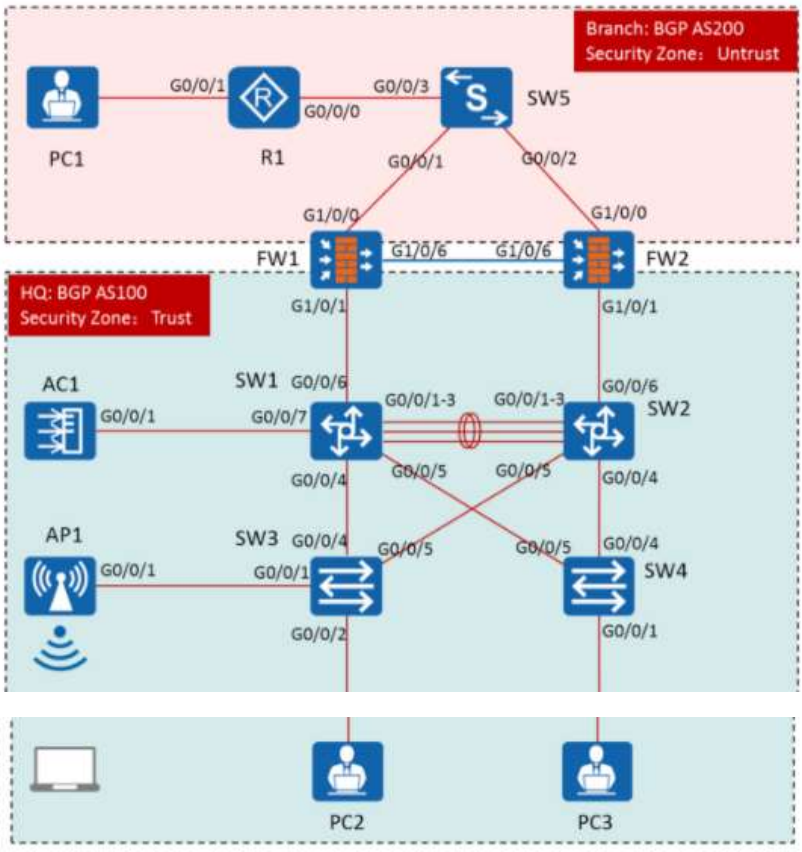
# Regional Final


Huawei Technologies Co., LTD.

# 1 Background

This experiment simulates the interconnection between a large and medium-sized company headquarters and branches. In order to ensure the security of the campus network and the demands of internal staff for wireless office, firewalls and WLANs need to be deployed at the company headquarters.

# 2 Integrated network topology




Picture 2-1 Experimental topology

# 3 VLAN & IP address planning table

Table 3-1 VLAN Planning Table

| Device name | Interface name | Port link type | PVID | Allow-pass VLAN |
|---|---|---|---|---|
| SW1 | Eth-Trunk1(G0/0/1-G0/0/3) | Trunk | 1 | 20 30 |
| | | Trunk | 1 | 20 30 |
| | | Trunk | 1 | 20 30 |
| | G0/0/4 | Hybrid | 1 | 15 20 |
| | G0/0/5 | Trunk | 1 | 30 |
| | G0/0/6 | Access | 10 | 10 |
| | G0/0/7 | Trunk | 1 | 20 50 |
| SW2 | Eth-Trunk1(G0/0/1-G0/0/3) | Trunk | 1 | 20 30 |
| | G0/0/4 | Trunk | 1 | 30 |
| | G0/0/5 | Trunk | 1 | 20 |
| | G0/0/6 | Access | 10 | 10 |
| SW3 | G0/0/1 | Trunk | 15 | 15 |
| | G0/0/2 | Access | 20 | 20 |
| | G0/0/4 | Hybrid | 1 | 15 20 |
| | G0/0/5 | Trunk | 1 | 20 |
| SW4 | G0/0/1 | Access | 30 | 30 |
| | G0/0/4 | Trunk | 1 | 30 |
| | G0/0/5 | Trunk | 1 | 30 |
| AC | G0/0/1 | Trunk | 1 | 20 50 |

Table 3-2 IP address planning table

| Device name | Interface name | IP address |
|---|---|---|
| R1 | Loopback 0 | 7.7.7.7/32 |
| | G0/0/0 | 10.1.127.7/24 |
| | G0/0/1 | 10.1.70.7/24 |
| SW1 | VLANif 10 | 10.1.13.3/24 |
| | VLANif 15 | 10.1.15.1/24 |
| | VLANif 20 | 10.1.20.13/24 |
| | VLANif 30 | 10.1.30.13/24 |
| | VLANif 50 | 10.1.50.1/24 |
| | Loopback 0 | 3.3.3.3/32 |
| SW2 | VLANif 10 | 10.1.24.4/24 |
| | VLANif 20 | 10.1.20.14/24 |
| | VLANif 30 | 10.1.30.14/24 |
| | Loopback 0 | 4.4.4.4/32 |
| SW3 | VLANif15 | 10.1.15.2/24 |
| AC1 | VLANif 50 | 10.1.50.2/24 |
| | Loopback 0 | 8.8.8.8/32 |
| FW1 | G1/0/0 | 10.1.127.1/24 |
| | G1/0/1 | 10.1.13.1/24 |
| | G1/0/6 | 10.1.12.1/24 |
| | Loopback 0 | 1.1.1.1/32 |

| | | |
|---|---|---|
| FW1 | G1/0/0 | 10.1.127.1/24 |
| | G1/0/1 | 10.1.13.1/24 |
| | G1/0/6 | 10.1.12.1/24 |
| | Loopback 0 | 1.1.1.1/32 |
| FW2 | G1/0/0 | 10.1.127.2/24 |
| | G1/0/1 | 10.1.24.2/24 |
| | G1/0/6 | 10.1.12.2/24 |
| | Loopback 0 | 2.2.2.2/32 |
| PC1 | / | 10.1.70.1/24 |

Table 3-3 Device login information table

| Device name | Management address | user | password |
|---|---|---|---|
| Firewall | 192.168.0.1:8443 | admin | Password: Huawei@123 |

**Note:** Please follow the instruction to configure the device name, policy ID, pool name, etc. Do not make other naming by yourself. **Otherwise, you will not get any points at that configuration.**

## 3.1 VLAN

Configure VLAN information according to the contents of the VLAN planning table.

- The link type of the interconnect interface of SW1, SW2, SW3, SW4, and AC1 is configured as a trunk.
- The trunk link of the interconnect switches only releases the corresponding VLAN.
- The interfaces G0/0/4 of SW1 and SW3 are set to the Hybrid interface.

### 3.2 IP Address

Please follow the address information given in the exam planning topology and IP address planning table to connect and configure the IP addresses of the corresponding network devices and interfaces.

# 4 Router and Switch

## 4.1 Link Aggregation

In order to ensure the link reliability between SW1 and SW2, the link aggregation is set up on SW1 and SW2.

- SW1 and SW2 are connected to each other through GE0/0/1, GE0/0/2, and GE0/0/3. These three interfaces are bundled into one logical interface.
- SW1 is the actor (SW2 priority is 200).
- The maximum available bandwidth between the two devices is 2G, and the GE0/0/3 interface is the backup link.


- Enable preemption and then set the delay to 10 seconds.
- The links between SW1 and SW2 should realize the load balance base on the source and destination MAC.

## 4.2 MSTP

To prevent loops between SW1, SW2, SW3 and SW4, we need to configure the STP protocol:

- The STP mode is MSTP, and the domain name is ***huawei.***
- VLAN 20 belongs to Instance 1; VLAN 30 belongs to Instance 2;
- In Instance 1, SW1 is the primary root bridge and SW2 is the backup root bridge.
- In Instance 2, SW2 is the primary root bridge, and SW1 is the backup root bridge.
- The GE0/0/2 of SW3 and GE0/0/1 of SW4 is directly connected to the PC. After the interface is UP, it needs to be in the forwarding state immediately. After the port receives the BPDU, the interface needs to be automatically shut down.

## 4.3 VRRP

To ensure the reliability of the service network segment, you need to implement VRRP load balancing mode on SW1 and SW2:

- VLAN 20 uses VRRP backup group 20, and the virtual IP address is 10.1.20.254.
- In VRRP backup group 20, SW1 is the master, the priority is 120, the preemption delay is 60 seconds. SW2 is used as the backup, the default priority is used.
- VLAN 30 uses VRRP backup group 30, and the virtual IP address is 10.1.30.254. In VRRP backup group 30, SW2 is the master, the priority is 120, the preemption delay is 60 seconds. SW1 is used as the backup, and

the default priority is used.

## 4.4 OSPF

To implement Layer 3 interworking within the headquarters network, the IGP uses the OSPF routing protocol.

- SW1 (VLANif10, VLANif15, VLANif 20, VLANif30, Loopback 0), SW2 (VLANif10, VLANif 20, VLANif30, Loopback 0), FW1 (GE1/0/0, GE1/0/1, Loopback 0), FW2 (GE1/0/0, GE1/0/1, Loopback 0) are all in area 0.
- The process ID is 1, and the router-id is the IP address of loopback 0.
- **All 32 bits of the address must be exactly matched.**
- To improve the security of the network, configure the area authentication on the OSPF network. The authentication mode is MD5 (Key value is 1) and the plain password is ***Huawei***.

## 4.5 IS-IS

AC1 runs IS-IS to communicate with SW1.

- All IS-IS process numbers are unified to 100 and the area ID is 49.0001.
- AC1 and SW1 are all level 2 device.
- The P2P network type is required between AC1 and SW1, and the negotiation mode must be 3-ways handshake.

## 4.6 IGP

In order to make the entire network reachable, importing routes on AC1 and SW1.

- Import the loopback interface of AC1 into IS-IS.
- Import OSPF and IS-IS route to each other, and make the entire network reachable.

## 4.7 Security Zone

Configure the security zone of the FW1 and FW2.

- Add G1/0/1 to the Trust zone.

- Add G1/0/0 to the Untrust zone.
- Add G1/0/6 to the DMZ zone.

- The interface of the firewall which is connected to the Trust area need to enable the Ping Service.

## 4.8 Firewall Security Policy and Hot Standby

To ensure the reliability of the firewall, deploy the hot-standby between FW1 and FW2.

- FW1 is the active device and FW2 is the standby.
- The VRRP/VGMP function is enabled on the G1/0/0 interface.
- The VRRP group number is 12, and the virtual IP address is 10.1.127.10.
- The G1/0/6 interface is the HRP heartbeat interface.
- The routes between headquarters and branches are required to be reachable. The data traffic needs to be released from the trust zone to the untrust zone (Policy name is **trust_untrust**).

- The untrust zone to trust zone must be matched exactly (Policy name is **untrust_trust**), allow the PC1 to visit PC2 and PC3.

## 4.9 BGP

To implement network interworking between the headquarters and branches, the BGP protocol is used.

- The AS number of the headquarters is 100.
- FW1, SW1, and SW2 use the logical interface (Loopback 0) to establish the IBGP neighbor relationships.
- FW2, SW1, and SW2 use the logical interface (Loopback 0) to establish the IBGP neighbor relationships.
- The AS number of the branch is 200. R1 and the Firewall use the physical interface to establish the EBGP neighbor relationships.
- Authentication is used to establish a neighbor relationship. The simple password is ***Huawei***.
- Make sure SW1 and SW2 can learn the correct EBGP routes.

## 4.10 BFD

In order to quickly detect communication failures between the headquarters network，deploy BFD on the headquarters network.

- Configure static BFD session ***Huawei*** on the FW1. The local discriminator is 10.
- Configure static BFD session ***Huawei*** on the FW2. The local discriminator is 20.
- Configure Interworking between BFD and Hot Standby
- Configure BFD to detect the protocol status of OSPF.

## 4.11 Telnet、ACL

To facilitate the maintenance of devices SW1 and SW2 inside the intranet headquarters, administrator can enable Telnet service on SW1 and SW2.

SW1:

- Maximum 5 terminals are allowed to telnet the SW1 at the same time.
- The authentication mode of SW1 is set to AAA. The authentication user name is ***Huawei***, and the simple password is ***Huawei@2019.***
- User Huawei has the highest privilege level.
- Configure basic ACL 2000 to allow users on the 10.1.20.0 network segment to telnet SW1.

SW2:

- Maximum 3 terminals are allowed to telnet the SW1 at the same time.
- The authentication mode of SW2 is password. The authentication simple password is **Admin@2019**, and the privilege level is the lowest one.
- Configure basic ACL 2000 to allow users on the 10.1.30.0 network segment to telnet SW2.

## 4.12 WLAN

### 4.12.1 DHCP

Configure Layer 3 interworking between APs, ACs, and neighboring network devices. All APs and wireless terminals obtain an IP address through DHCP. Use the global mode on the SW1 to configure DHCP services for APs and STAs. The global address pool names are ***ap*** and ***huawei***.

Table 3-3 WLAN DHCP allocation table

| Project | Data |
| --- | --- |
| AP Management VLAN | VLAN15 |
| STA Service VLAN | VLAN20 |
| DHCP Server | SW1 acts as a DHCP server to assign an IP address to the AP.<br>SW1 acts as a DHCP server to assign an IP address to the STA. The default gateway of the STA is 10.1.20.13. |
| IP address pool of the AP | Name: AP, 10.1.15.0/24 (Except 10.1.15.2) |
| IP address pool of the STA | Name: STA, 10.1.20.0/24 |
| Source IP address of the AC | 8.8.8.8 |

### 4.12.2 AP on-line Configuration

| Configuration Item | Data |
| --- | --- |
| AP authentication mode | **MAC-Auth** |
| AP-group | Group-Name: ***huawei***<br>AP-Name: ***AP1*** |
| Regulatory domain profile | Name: **huaweiq'**<br>Country code: ***MY*** |
| SSID template | SSID profile: ***huawei***, SSID Name: ***huawei*** |

| | |
|---|---|
| Security template | Security Name: ***huawei,*** WPA2 authentication,<br>Encryption Mode: aes-tkip, the password is ***Huawei@123*** |
| VAP template | VAP Name: ***huawei***<br>Forward-mode: tunnel<br>Service-VLAN: VLAN **20** |

- Configure the WLAN management VLAN. The ap-name is ***AP1*** and ap-group name is ***huawei.***
- Configure AP authentication mode as MAC address authentication.

### 4.12.3 Configuration and Delivery

Configure WLAN service parameters to implement STA access to the WLAN network.

Configure the security policy of WPA2. The password is ***Huawei@123***. Encryption method is aes-tkip.

The SSID is ***huawei*** and the service forwarding mode is tunnel forwarding.

### 4.13 SNMP

Configure SNMPv2c on SW1.

Set read community as ***Admin@2019***, and write community as ***Huawei@2019***.

Activate the function of the agent to send alarms and specify the interface for alarm notification as **G0/0/6**.

# 5 Verification

After all the configurations are completed, STA will be able to automatically obtain the IP address, and all the terminals can communicate with each other.