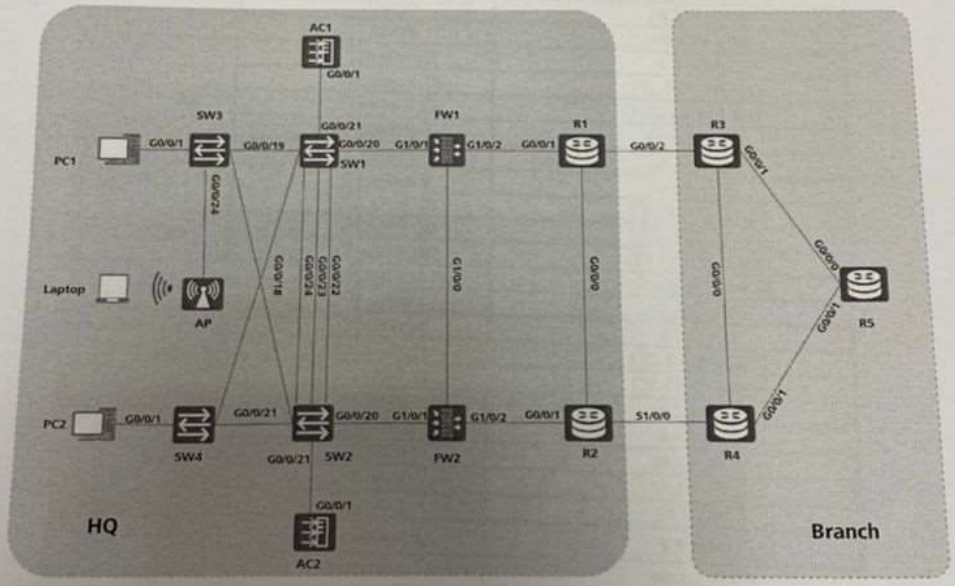
1 Backgroud

This experiment simulates the interconnection between the headquarter and branch of a large company. To ensure the reliability of the connection between the headquarter and branch, ethernet link and serial link are deployed between the headquarter and branch, The private link is the primary link, and the VPN link is the backup link.

As the rapid development of campus network construction, employees are facing increasingly serious security issues of the campus network while enjoying variable network resources, the NGFW can be deployed on the campus network to reduce security threats and help implement effective network management. To meet staff's requirements of wireless office, WLAN devices need to be deployed at the company's headquarter.

2 Network Topology

Figure 2-1 Experiment topology of the IP network



The experiment uses the following devices:

- Two USG6350 firewalls (FW1-FW2)
- Five AR2220E routers (R1-R5)
- Four S5720-36C-PWR-EI-AC switches (SW1-SW4)
- Two wireless access controller AC6005 (AC1-AC2)
- One wireless access point AP4050 (AP1)
- Two wired terminals (PC1, PC2)

- One wireless terminal (Laptop)

Table 2-1 IP address plan

Device Name	Interface Name	IP Address
R1	Loopback0	1.1.1.1/32
	G0/0/0	10.1.1.1/30
	G0/0/1	10.1.1.5/30
	G0/0/2	100.1.13.1/30
R2	Loopback0	2.2.2.2/32
	G0/0/0	10.1.1.2/30
	G0/0/1	10.1.1.9/30
	S1/0/0	200.1.24.1/30
R3	Loopback0	3.3.3.3/32
	G0/0/0	10.2.34.1/30
	G0/0/1	10.2.35.1/30
	G0/0/2	100.1.13.2/30
R4	Loopback0	4.4.4.4/32
	G0/0/0	10.2.34.2/30
	G0/0/1	10.2.45.1/30
	S1/0/0	200.1.24.2/30
R5	Loopback0	5.5.5.5/32
	Loopback100	192.168.100.1/32
	Loopback200	192.168.200.1/32
	G0/0/0	10.2.35.2/30
	G0/0/1	10.2.45.2/30
SW1	Loopback0	6.6.6.6/32
	VLANIF 10	172.16.10.253/24
	VLANIF 20	172.16.20.253/24
	VLANIF 100	172.16.100.254/24
	VLANIF 101	172.16.101.254/24
	VLANIF1	10.1.1.18/30
SW2	Loopback0	7.7.7.7/32
	VLANIF 10	172.16.10.252/24
	VLANIF 20	172.16.20.252/24
	VLANIF1	10.1.1.22/30
FW1	Loopback0	8.8.8.8/32
	G1/0/0	10.1.1.13/30
	G1/0/1	10.1.1.17/30
	G1/0/2	10.1.1.6/30
FW2	Loopback0	9.9.9.9/32
	G1/0/0	10.1.1.14/30
	G1/0/1	10.1.1.21/30
	G1/0/2	10.1.1.10/30
AC1	VLANIF 101	172.16.101.1/24
	VLANIF 102	172.16.102.1/30
AC2	VLANIF 101	172.16.101.2/24
	VLANIF 102	172.16.102.2/30

Table 2-2 Device login information

Device Name	Management Address	User	Password
Firewall	https://192.168.0.1:8443	admin	Huawei@123

2.1 Configuration tasks

2.1.1 Task 1: Link aggreation

To ensure link reliability between SW1 and SW2, bundle all the interfaces directly connecting SW1 and SW2 into a Layer 2 logical interface.

1. Configure member links of the logical interface to perform load balancing based on the source and destination MAC addresses.
2. Configure SW1 as the Actor (with a priority of 100), and configure G0/0/22 and G0/0/23 as active interfaces (with a priority of 100),configure G0/0/24 as backup interface .
3. Enable the preemption function, and set the preemption delay to 10 seconds.

2.1.2 Task 2: VLAN

Create VLANs required on SW1 to SW4 according to **Figure 2-1** ,**Table 2-1** and **Table 2-3.**

Configure the type of link on SW1 to SW4 to allow users who use the service to communicate, and only allow the necessary VLANs to pass.

Table 2-3 VLAN Information

Device Name	Port	Link-type	VLAN parameters
SW1	GE0/0/21	Trunk	PVID:1 Allow-pass: VLAN 101 102
	GE0/0/18 GE0/0/19 Eth-trunk1	Trunk	PVID:1 Allow-pass: VLAN 10 20 100 101 102
SW2	GE0/0/21	Trunk	PVID:1 Allow-pass: VLAN 101 102
	GE0/0/18 GE0/0/19 Eth-trunk1	Trunk	PVID:1 Allow-pass: VLAN 10 20 100 101 102
SW3	GE0/0/1	Access	PVID:10

	GE0/0/24	Trunk	PVID:101 Allow-pass: VLAN100 101
	GE0/0/18 GE0/0/19	Trunk	PVID:1 Allow-pass: VLAN 10 20 100 101 102
SW4	GE0/0/1	Access	PVID:20
	GE0/0/18 GE0/0/19	Trunk	PVID:1 Allow-pass: VLAN 10 20 100 101 102

2.1.3 Task 3: IP Addressing

Configure network devices' names and interfaces' IP addresses according to **Figure 2-1** and **Table 2-1**.

2.1.4 Task 4: MSTP, VRRP, BFD and DHCP

Configure STP to prevent loops between SW1, SW2, SW3 and SW4.

1. Set the STP mode to MSTP. Configure region name as **HuaweiICT**.
2. Map VLAN 10 100 101 to MSTI 1 and VLAN 20 102 to MSTI 2.
3. Configure SW1 as the root bridge and SW2 as the secondary root bridge in MSTI 1, and configure SW2 as the root bridge and SW1 as the secondary root bridge in MSTI 2.
4. The interfaces connected to terminals can transit from Disable to Forwarding without any delay to implement fast convergence.

To ensure the reliability of network segments, configure VRRP on SW1 and SW2 to load balance services.

1. Configure VRRP group 1 with the virtual IP address of 172.16.10.254 in VLAN 10 and VRRP group 2 with the virtual IP address of 172.16.20.254 in VLAN 20.
2. In VRRP group 1, configure SW1 as the VRRP master device, with the priority being 140. SW2 is the VRRP backup device and keep the default priority.
3. In VRRP group 2, configure SW2 as the VRRP master device, with the priority being 140. SW1 is the VRRP backup device and keep the default priority.
4. Enable the preempt function and set the preemption delay time to 20s in VRRP group 1 and group 2.

Run DHCP services on SW1 based on the global address pool

1. The address pool name is 10, and the gateway address is the 172.16.10.254, DNS server address is 8.8.8.8. PC1 needs to dynamically obtain an IP address from the IP address pool 10;

2. The address pool name is 20, and the gateway address is the 172.16.20.254, DNS server address is 8.8.8.8. PC2 needs to dynamically obtain an IP address from the IP address pool 20.

2.1.5 Task 5: Security Zone

Bind G1/0/0 interfaces on FW1 and FW2 to the **DMZ** zone, G1/0/1 interface to the **trust** zone, and G1/0/2 interfaces to the **untrust** zone.

2.1.6 Task 6: Firewall Security Policy and HRP

1. Configure firewalls to work in load balancing mode .
2. Specify GE1/0/0 on the FW1 and FW2 as the heartbeat interface and enable hot standby.

   Configure quick session backup on both FWs in case of inconsistent forward and return packet paths. After hot standby relationship is established, the security policy on FW1 will be automatically backed up to FW2.
3. Configure security policies to allow traffic ,requirement as below:
   a) From trust zone to the untrust zone
   b) From subnets of PC1 and PC2 (172.16.10.0/24 and 172.16.20.0/24) .

2.1.7 Task 7: OSPF

1. Run OSPF on devices according to the information provided in Table 2-4. The network command with the parameter that completely matches the 32-bit mask is required.

Table 2-4 OSPF Information

Device Name	Interface	Area ID
R1	Loopback0	0
	G0/0/0	
	G0/0/1	
R2	Loopback0	0
	G0/0/0	
	G0/0/1	
FW1	Loopback0	0
	G1/0/2	
	G1/0/1	1
FW2	Loopback0	0
	G1/0/2	
	G1/0/1	1
SW1	Loopback0	1
	VLANIF 1	

	VLANIF 10	2
	VLANIF 20	
	VLANIF 100	
SW2	Loopback0	1
	VLANIF 1	
	VLANIF 10	2
	VLANIF 20	
	Loopback1	

2. Configure the ospf router ID by devices' loopback0 address (For example , the router ID of R1 is 1.1.1.1.)
3. Disable SW1's VLANIF 10 from sending OSPF packets to PC1.
4. Set the network type of the link between FW1 and R1 to P2P.

2.1.8 Task 8: IS-IS

1. Enable IS-IS process on R3 R4 and R5.Configure the system ID of IS-IS using the device ID (For example , the system ID of R3 is 0000.0000.0003.).
2. Set the process ID to 1. Configure them in area 49.0002 , set R3 and R4 as level 1-2 Routers, configure R5 as Level-1 routers.
3. Run IS-IS on R3 (Loopback 0, G0/0/0 and G0/0/1), R4 (Loopback 0,G0/0/0 and G0/0/1), R5(Loopback 0, Loopback 100, Loopback200, G0/0/0 and G0/0/1) on the Branch network.
4. Configure IS-IS parameters on R3 according to the following information:
    a) The maximum delay for generating LSPs is 1s, the initial delay is 100 ms, and the incremental time is 100 ms.
    b) Enable the fast LSP extension feature. The maximum delay for SPF calculation is 1s, the initial delay is 100 ms, and the incremental delay is 100 ms.

2.1.9 Task 9: IPSEC VPN

1. Configure advanced ACL 3000 to define the protected traffic from headquarters to branches (source: 172.16.0.0/16, destination: 192.168.0.0/16) on R1.
2. Configure advanced ACL 3001 to define the protected traffic from branch and to headquarters (source: 192.168.0.0/16, destination:172.16.0.16/24) on R3.
3. Configure IPsec VPN according to the information provided in Table 2-5

Table 2-5 OSPF Information

Device	IPsec Configuration	
R1 R3	IKE peer	Version：v2 Authentication mode: pre-shared key authentication Pre-shared key: Huawei@ICT Local ID type: IP address Remote ID type: IP address

Device	IPsec Configuration	
	IPsec policy	Name: ICT Mode: isakmp
	IPsec proposal	Name: Huawei-ICT Security protocol: ESP Encapsulation mode: tunnel encapsulation Encryption algorithm: AES-256 Authentication algorithm: SHA2-256
	IKE proposal	No.: 1 DH group: group14 Authentication mode: pre-shared key authentication

4. Apply IPSec profiles to outbound interfaces(G0/0/2), and import data flows to be protected by IPSec .

2.1.10 Task 10: PPP

1. R2 and R4 are connected through serial interface, configure PPP authentication between R2 and R4.
    a) Set R2 as the authenticate end, and configure R4 as the authenticated end .
    b) The username is **huawei**, and password is **Huawei@ICT**.
    c) Authentication-mode is CHAP.

2.1.11 Task 11: BGP

1. BGP runs between HQ network (AS 100) and branch network (AS 200).
2. EBGP connection is established between R1 and R3, R2 and R4 so that these devices can exchange routing information.
    a) R1 and R3 establish EBGP connection by the interface G0/0/2
    b) R2 and R4 establish EBGP connection by the interface S1/0/0.
3. IBGP are established among R1, R2, FW1 and FW2 by loopback 0. There is no IBGP neighbor relationship between FW1 and FW2.
4. IBGP full-mesh connections are established between R3, R4 and R5 by loopback 0.
5. Configure R1 and R2 to advertise route 172.16.10.0/24 and 172.16.20.0/24 into BGP. Configure R5 to advertise route 192.168.100.1/32 and 192.168.200.1/32 into BGP so that the two ASs can communicate with each other. All routes are generated by command **"network"**

2.1.12 Task 12: Traffic Diversion

1. Using the Local-preference attribute on R3 to control traffic path:
    a) From the Loopback 100 of R5 to PC1 through R5-R3-R1-FW1-SW1-SW3.
    b) Match routes by IP-prefix tool.
    c) When the link between R3 and R5 is down, traffic goes through R5-R4-R3-R1-FW1-SW1-SW3.
2. Using the AS_Path attribute on R4 to control traffic path:
    a) From the Loopback 200 of R5 to PC2 through SW4-SW2-FW2-R2-R4-R5.

b) Match routes by IP-prefix tool

c) When the link between R4 and R5 is down, traffic from the Loopback 200 of R5 to access PC2 goes through R5-R4-R2-FW2-SW2-SW4.

2.1.13 Task 13: QoS

1. Configure interface-based traffic policing on G0/0/2 of R3 inbound, the CIR set to 9000Kbps.
2. Configure interface-based traffic shaping on G0/0/0 of R5, the CIR set to 8000Kbps.

2.1.14 Task 14: WLAN

I. DHCP

1. Configure SW1 as the DHCP server and configure a global address pool named **AP** to assign IP addresses to AP1 and AP2 in VLAN 101.
2. Configure SW1 as the DHCP server and configure a global address pool named **laptops** to assign an IP address to PC2 in VLAN 100. The DNS address is 8.8.8.8.
3. Configure VLANs to implement goals above.

Table 2-1 WLAN data planning

Item	Data
Management VLAN for APs	VLAN 101
Service VLAN for PC2	VLAN 100
Backup VLAN for ACs	VLAN 102
DHCP server	SW1 functions as the DHCP server to assign IP addresses for APs and PC2. AP gateway: 172.16.101.254/24 PC2 gateway: 172.16.100.254/24
AC source interface	VLANIF 101
Management IP address of AC1	VLANIF 101: 172.16.101.1/24
Management IP address of AC2	VLANIF 101: 172.16.101.2/24
Active AC (AC1)	priority: 0
Standby AC (AC2)	priority: 1
AC1 tunnel IP address and port number	IP address: VLANIF 102, 172.16.102.1/30 Port number: 10241
AC2 tunnel IP address and port number	IP address: VLANIF 102, 172.16.102.2/30 Port number: 10241

Item	Data
AP group	Name: huawei Reference profiles: VAP profile **huawei** and regulatory domain profile **huawei**
Regulatory domain profile	Name: huawei Country code: CN

*Notice :all the other template or policy should be named as **huawei** .*

II. HSB Between ACs

1. Connect AC1 and AC2 to the network and configure HSB between ACs in dual-link mode.
2. AC2 backs up information from AC1 so that AC2 can immediately provide WLAN services if AC1 fails. Services are not interrupted during the switchover.

III. Configuration and Delivery

1. AC authenticate AP by their MAC addresses.
2. Configure to release WLAN signals: **huawei-ICTX** (X is the group name, If the group name is 01, so the SSID is huawei-guest01.).
3. Configure the authentication mode as **WPA-PSK & aes** and the password as **Huawei@ICT2019**, and the data forwarding mode as **direct forwarding**.