2022-2023 Huawei ICT Competition

Global Final

Network Track

Lab Exam

Issue: 1.0

Huawei Technologies Co., LTD.

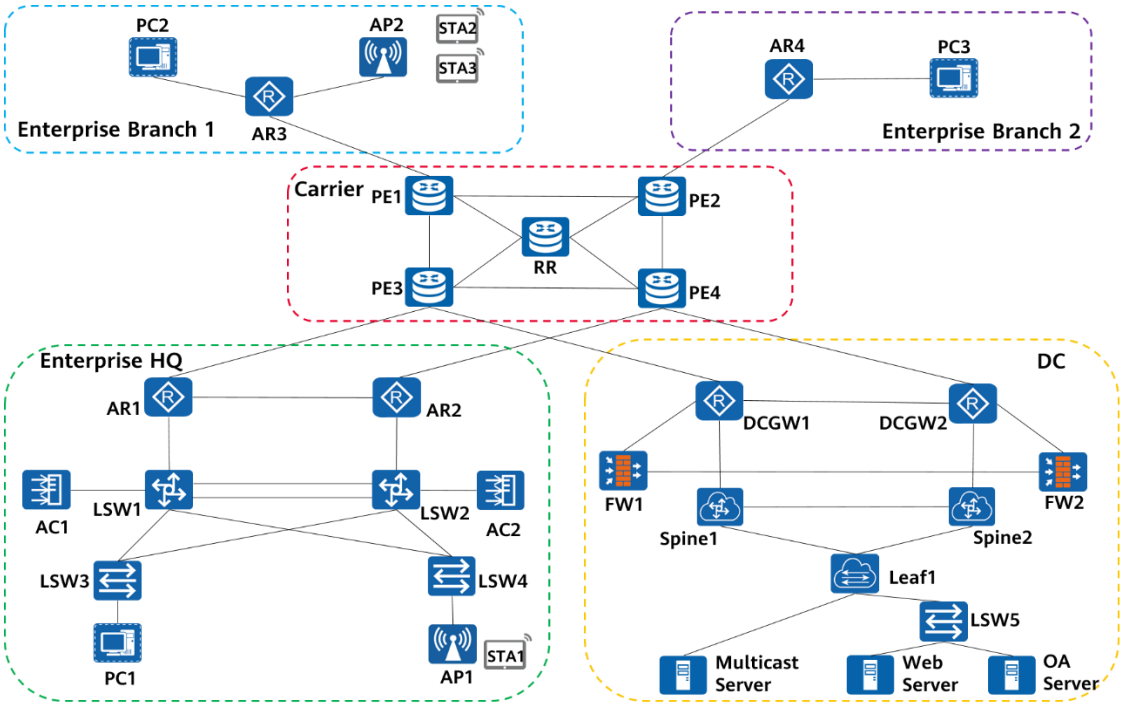
1 Background

A large enterprise has three sites: headquarters (HQ), branch 1, and branch 2. These sites communicate with each other through a carrier's metropolitan area network (MAN). The enterprise also has its service servers hosted in the carrier's data center (DC) equipment room. The service servers deployed include OA, web, and multicast servers used to meet internal OA and external communication requirements.

The enterprise HQ, branch 1, and DC communicate with each other through the carrier's MPLS VPN. Enterprise branch 2 establishes an IPsec tunnel to the HQ over the Internet to access intranet services. Users on the Internet access the web server deployed at the DC through public IP addresses. The enterprise HQ, branch 1, and branch 2 are added to the multicast group to receive video streams from the multicast server at the DC.

2 Network Topology

Figure 2-1 IP network topology



1. The following devices are used in the lab environment:
   - Five routers: PE1, PE2, PE3, PE4, and RR
   - Four AR2220 routers: AR1, AR2, AR3, and AR4
   - Two USG6000V firewalls: FW1 and FW2
   - Two NE40Es: DCGW1 and DCGW2
   - Four S5700 switches: LSW1, LSW2, Spine1, and Spine2
   - Three S3700 switches: LSW3, LSW4, and LSW5

- One CE12800: Leaf1
- Two AC6605s: AC1 and AC2
- Two AP5030s: AP1 and AP2
- Three PCs: PC1, PC2, and PC3
- Three servers: OA Server, Web Server, and Multicast Server
- Three STAs: STA1, STA2, and STA3

2. Device login modes

- On the computer where the ENSP Server is installed, click the icon of a device to log in to the device.
- On the computer where the remote terminal is installed, log in to a device using the IP address of the computer where the ENSP Server is installed and the corresponding port number of the device.

Table 2-1 Device login port number plan

Device	Port Number	Device	Port Number
FW1	2001	RR	2013
FW2	2002	AR1	2014
DCGW1	2003	AR2	2015
DCGW2	2004	AR3	2016
PE1	2005	AR4	2017
PE2	2006	LSW1	2018
PE3	2007	LSW2	2019
PE4	2008	LSW3	2020
Spine1	2009	LSW4	2021
Spine2	2010	LSW5	2022
AC1	2011	Leaf1	2023
AC2	2012		

The user name and password for logging in to FW1 and FW2 are **admin** and **Huawei@123**, respectively.

Ensure that you can log in to the involved devices.

3 Configuration Objectives

The service objectives of the configuration tasks are as follows:

1. An IPv4/IPv6 dual-stack wired service network is deployed at the enterprise HQ and branch 1, and an IPv4 single-stack wired service network is deployed at branch 2.
2. An IPv4 wireless service network is deployed at the enterprise HQ and branch 1.
3. At the enterprise HQ, the wired and wireless networks communicate with the IPv4 and IPv6 Internet through the egress router of the HQ. Network address translation (NAT) is required for IPv4 Internet access traffic before the traffic is forwarded to the Internet, and IPv6 Internet access traffic is directly routed and forwarded to the Internet.
4. At branch 1, the wired and wireless networks communicate with the IPv4 and IPv6 Internet through the egress router of the branch. NAT is required for IPv4 Internet access traffic before the traffic is forwarded to the Internet, and IPv6 Internet access traffic is directly routed and forwarded to the Internet.
5. At branch 2, the wired network communicates with the IPv4 Internet through the egress router of the branch. NAT is required for IPv4 Internet access traffic before the traffic is forwarded to the Internet.
6. The enterprise's OA, web, and multicast servers are deployed in the carrier's cloud DC equipment room to meet daily OA and external communication requirements. The OA server is used for daily OA and can be accessed only by internal employees. The web server is used for external communication and can be accessed by any user on the Internet. The multicast server is used for internal video conferences. Firewalls are deployed at the DC to perform security filtering for specific services.
7. The enterprise HQ, branch 1, and DC are connected through the carrier's MPLS VPN to implement intranet communication between the wired service network and wireless service network, as well as access to the OA server at the DC.
8. Enterprise branch 2 establishes an IPsec tunnel to the HQ through the Internet to implement IPv4 service access to the HQ, branch 1, and OA server at the DC.
9. Users on the Internet can access the web server deployed at the DC through the Internet.
10. Multicast protocols are deployed on the entire network so that the enterprise HQ, branch 1, and branch 2 can join multicast groups to receive video streams from the multicast server at the DC.

4 Configuration Tasks

4.1 Task 1: Basic Data Configuration

4.1.1 VLAN Configuration

According to Table 4-1, configure the VLAN link type and VLAN parameters on LSW1 to LSW5, Spine1, Spine2, AC1, and AC2, and configure sub-interfaces and sub-interface VLAN IDs on FW1, FW2, AR1 to AR4, and PE1 to PE4.

For the GigabitEthernet0/0/2.*X* sub-interface, the value of *X* is the VLAN ID planned for the sub-interface. For example, if the sub-interface is GigabitEthernet0/0/2.20, its VLAN ID is 20.

Table 4-1 VLAN information

Device Name	Interface	Link Type	VLAN Parameter
LSW1	ETH-Trunk 1 (GigabitEthernet0/0/1 GigabitEthernet0/0/2)	Trunk	PVID: 1 Allow-pass: VLANs 2301, 2303, 2305, 2306, 2307, and 2308
	GigabitEthernet0/0/3	Trunk	PVID: 1 Allow-pass: VLAN 2301
	GigabitEthernet0/0/4	Trunk	PVID: 1 Allow-pass: VLANs 2301, 2306, 2307, and 2308
	GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2305
	GigabitEthernet0/0/6	Access	PVID: VLAN 2302
LSW2	ETH-Trunk 1 (GigabitEthernet0/0/1 GigabitEthernet0/0/2)	Trunk	PVID: 1 Allow-pass: VLANs 2301, 2303, 2305, 2306, 2307, and 2308
	GigabitEthernet0/0/3	Trunk	PVID: 1 Allow-pass: VLANs 2301, 2306, 2307, and 2308
	GigabitEthernet0/0/4	Trunk	PVID: 1 Allow-pass: VLAN 2301
	GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2305
	GigabitEthernet0/0/6	Access	PVID: 2304
LSW3	GigabitEthernet0/0/1	Trunk	PVID: 1 Allow-pass: VLAN 2301
	GigabitEthernet0/0/2	Trunk	PVID: 1 Allow-pass: VLAN 2301
	Ethernet0/0/1	Access	PVID: 2301
LSW4	GigabitEthernet0/0/1	Trunk	PVID: 1 Allow-pass: VLANs 2306, 2307,

Device Name	Interface	Link Type	VLAN Parameter
			and 2308
	GigabitEthernet0/0/2	Trunk	PVID: 1 Allow-pass: VLANs 2306, 2307, and 2308
	Ethernet0/0/1	Trunk	PVID: 2306 Allow-pass: VLANs 2306, 2307, and 2308
LSW5	GigabitEthernet0/0/1	Trunk	PVID: 1 Allow-pass: VLAN 10
	Ethernet0/0/1	Access	PVID: 10
	Ethernet0/0/2	Access	PVID: 10
AC1	GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2305
AC2	GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2305
Spine1	GigabitEthernet0/0/1	Access	PVID: 78
	GigabitEthernet0/0/2	Access	PVID: 79
	GigabitEthernet0/0/4	Access	PVID: 57
Spine2	GigabitEthernet0/0/1	Access	PVID: 78
	GigabitEthernet0/0/3	Access	PVID: 89
	GigabitEthernet0/0/4	Access	PVID: 68
Leaf1	GigabitEthernet1/0/4.10		VLAN 10
FW1	GigabitEthernet1/0/1.10 GigabitEthernet1/0/1.20 GigabitEthernet1/0/1.30		VLAN 10 VLAN 20 VLAN 30
DCGW1	Ethernet1/0/0.56 Ethernet1/0/1.10 Ethernet1/0/1.20 Ethernet1/0/1.30 Ethernet1/0/3.35		VLAN 56 VLAN 10 VLAN 20 VLAN 30 VLAN 35
FW2	GigabitEthernet1/0/1.10 GigabitEthernet1/0/1.20		VLAN 10 VLAN 20

Device Name	Interface	Link Type	VLAN Parameter
	GigabitEthernet1/0/1.30		VLAN 30
DCGW2	Ethernet1/0/0.56 Ethernet1/0/1.10 Ethernet1/0/1.20 Ethernet1/0/1.30 Ethernet1/0/3.46		VLAN 56 VLAN 10 VLAN 20 VLAN 30 VLAN 46
AR1	GigabitEthernet0/0/2.310 GigabitEthernet0/0/2.320 GigabitEthernet0/0/2.330		VLAN 310 VLAN 320 VLAN 330
AR2	GigabitEthernet0/0/2.411 GigabitEthernet0/0/2.421 GigabitEthernet0/0/2.431		VLAN 411 VLAN 421 VLAN 431
AR3	GigabitEthernet0/0/0.118 GigabitEthernet0/0/0.128 GigabitEthernet0/0/0.138 GigabitEthernet0/0/2.2309 GigabitEthernet0/0/2.2310		VLAN 118 VLAN 128 VLAN 138 VLAN 2309 VLAN 2310
PE3	GigabitEthernet0/0/2.310 GigabitEthernet0/0/2.320 GigabitEthernet0/0/2.330 GigabitEthernet0/0/3.35		VLAN 310 VLAN 320 VLAN 330 VLAN 35
PE4	GigabitEthernet0/0/2.411 GigabitEthernet0/0/2.421 GigabitEthernet0/0/2.431 GigabitEthernet0/0/3.46		VLAN 411 VLAN 421 VLAN 431 VLAN 46
PE1	GigabitEthernet0/0/3.118 GigabitEthernet0/0/3.128 GigabitEthernet0/0/3.138		VLAN 118 VLAN 128 VLAN 138

4.1.2 IP Address Configuration

Configure IP addresses for the network interfaces according to Table 4-2.

Table 4-2 IP address data plan

Device Name	Interface	IPv4 Address	IPv6 Address	Description
PE1	Loopback 0	1.1.1.1/32	2000::1/128	
	GigabitEthernet0/0/0	100.1.2.1/30	2000:1:2::1/126	
	GigabitEthernet0/0/1	100.1.3.1/30	2000:1:3::1/126	
	GigabitEthernet0/0/2	100.1.25.1/30	2000:1:25::1/126	
	GigabitEthernet0/0/3.118	10.1.18.2/30	2000:1:18::2/126	The interface is bound to VPNA.
	GigabitEthernet0/0/3.128	100.1.18.2/30	N/A	Interface used for connecting PE1 to the IPv4 Internet.
	GigabitEthernet0/0/3.138	N/A	2001:1:18::2/126	Interface used for connecting PE1 to the IPv6 Internet.
PE2	Loopback 0	1.1.1.2/32	2000::2/128	
	GigabitEthernet0/0/0	100.1.2.2/30	2000:1:2::2/126	
	GigabitEthernet0/0/1	100.2.4.1/30	2000:2:4::1/126	
	GigabitEthernet0/0/2	100.2.21.1/30	N/A	
	GigabitEthernet0/0/3	100.2.25.2/30	2000:2:25::2/126	
	Loopback 8	8.8.8.8/32	8::8/128	Simulates the IPv4 and IPv6 Internet.
PE3	Loopback 0	1.1.1.3/32	2000::3/128	
	Ethernet0/0/0	100.3.25.1/30	2000:3:25::1/126	
	GigabitEthernet0/0/0	100.3.4.1/30	2000:3:4::1/126	
	GigabitEthernet0/0/1	100.1.3.2/30	2000:1:3::2/126	
	GigabitEthernet0/0/2.310	10.3.10.2/30	2000:3:10::2/1	The interface is bound

Device Name	Interface	IPv4 Address	IPv6 Address	Description
			26	to VPNA.
	GigabitEthernet0/0/2.320	100.3.10.2/30	N/A	Interface used for connecting PE3 to the IPv4 Internet.
	GigabitEthernet0/0/2.330	N/A	2001:3:10::2/126	Interface used for connecting PE3 to the IPv6 Internet.
	GigabitEthernet0/0/3	100.3.5.1/30	N/A	Interface used for connecting PE3 to the IPv4 Internet.
	GigabitEthernet0/0/3.35	10.3.5.1/30	N/A	The interface is bound to VPNA.
	Loopback34	1.1.1.34/32	N/A	Functions as the RP of the multicast service.
PE4	Loopback 0	1.1.1.4/32	2000::4/128	
	Ethernet0/0/1	100.4.25.2/30	2000:4:25::2/126	
	GigabitEthernet0/0/0	100.3.4.2/30	2000:3:4::2/126	
	GigabitEthernet0/0/1	100.2.4.2/30	2000:2:4::2/126	
	GigabitEthernet0/0/2.411	10.4.11.2/30	2000:4:11::2/126	The interface is bound to VPNA.
	GigabitEthernet0/0/2.421	100.4.11.2/30	N/A	Interface used for connecting PE4 to the IPv4 Internet.
	GigabitEthernet0/0/2.431	N/A	2001:4:11::2/126	Interface used for connecting PE4 to the IPv6 Internet.
	GigabitEthernet0/0/3	100.4.6.1/30	N/A	Interface used for connecting PE4 to the IPv4 Internet.
	GigabitEthernet0/0/3.46	10.4.6.1/30	N/A	The interface is bound to VPNA.
	Loopback34	1.1.1.34/32	N/A	Functions as the RP of

Device Name	Interface	IPv4 Address	IPv6 Address	Description
				the multicast service.
RR	Loopback 0	1.1.1.25/32	2000::25/128	
	GigabitEthernet0/0/2	100.1.25.2/30	2000:1:25::2/126	
	GigabitEthernet0/0/3	100.2.25.1/30	2000:2:25::1/126	
	Ethernet0/0/0	100.3.25.2/30	2000:3:25::2/126	
	Ethernet0/0/1	100.4.25.1/30	2000:4:25::1/126	
AR1	Loopback 0	1.1.1.10/30	2000::10/128	
	GigabitEthernet0/0/0	10.10.11.2/30	Automatic generation of a link-local addresses (LLA)	
	GigabitEthernet0/0/1	10.10.12.2/30	Automatic generation of an LLA	
	GigabitEthernet0/0/2.310	10.3.10.1/30	2000:3:10::1/126	Used for VPN services.
	GigabitEthernet0/0/2.320	100.3.10.1/30	N/A	Interface used for connecting AR1 to the IPv4 Internet.
	GigabitEthernet0/0/2.330	N/A	2001:3:10::1/126	Interface used for connecting AR1 to the IPv6 Internet.
	Loopback1011	1.1.10.11/32	N/A	Functions as the RP of the multicast service.
AR2	Loopback 0	1.1.1.11/30	2000::11/128	
	GigabitEthernet0/0/0	10.10.11.1/30	Automatic generation of an LLA	
	GigabitEthernet0/0/1	10.11.13.2/30	Automatic generation of	

Device Name	Interface	IPv4 Address	IPv6 Address	Description
			an LLA	
	GigabitEthernet0/0/2.411	10.4.11.1/30	2000:4:11::1/126	Used for VPN services.
	GigabitEthernet0/0/2.421	100.4.11.1/30	N/A	Interface used for connecting AR2 to the IPv4 Internet.
	GigabitEthernet0/0/2.431	N/A	2001:4:11::1/126	Interface used for connecting AR2 to the IPv6 Internet.
	Loopback1011	1.1.10.11/32	N/A	Functions as the RP of the multicast service.
LSW1	VLANIF2301	192.168.3.253/24 (VRRP)	192:168:3::1/64	Service network segment of the wired network.
	VLANIF2302	10.10.12.1/30	Automatic generation of an LLA	Interface used for connecting LSW1 to AR1.
	VLANIF2303	10.12.13.2/30	Automatic generation of an LLA	Interface used for connecting LSW1 to LSW2.
	VLANIF2305	172.16.2.251/24	N/A	Interface used for connecting LSW1 to ACs.
	VLANIF2306	172.16.3.253/24 (VRRP)	N/A	Management IP address segment of the AP at the HQ.
	VLANIF2307	192.168.4.253/24 (VRRP)	N/A	Service network segment of the HQ wireless network.
	VLANIF2308	192.168.5.253/24 (VRRP)	N/A	Service network segment of the HQ wireless network.
LSW2	VLANIF2301	192.168.3.252/24 (VRRP)	N/A	Service network segment of the wired network.
	VLANIF2303	10.12.13.1/30	Automatic generation of	Interface used for connecting LSW2 to

Device Name	Interface	IPv4 Address	IPv6 Address	Description
			an LLA	LSW1.
	VLANIF2304	10.11.13.1/30	Automatic generation of an LLA	Interface used for connecting LSW2 to AR2.
	VLANIF2305	172.16.2.250/24	N/A	Interface used for connecting LSW2 to ACs.
	VLANIF2306	172.16.3.252/24 (VRRP)	N/A	Management IP address segment of the AP at the HQ.
	VLANIF2307	192.168.4.252/24 (VRRP)	N/A	Service network segment of the HQ wireless network.
	VLANIF2308	192.168.5.252/24 (VRRP)	N/A	Service network segment of the HQ wireless network.
AC1	VLANIF 2305	172.16.2.253/24 (VRRP)	N/A	
AC2	VLANIF 2305	172.16.2.252/24 (VRRP)	N/A	
AR3	GigabitEthernet0/0/0.118	10.1.18.1/30	2000:1:18::1/126	Used for VPN services.
	GigabitEthernet0/0/0.128	100.1.18.1/30	N/A	Interface used for connecting AR3 to the IPv4 Internet.
	GigabitEthernet0/0/0.138	N/A	2001:1:18::1/126	Interface used for connecting AR3 to the IPv6 Internet.
	GigabitEthernet0/0/1	192.168.1.1/24	192:168:1::1/64	Service network segment of the wired network.
	GigabitEthernet0/0/2	172.16.4.254/24	N/A	Management IP address segment of the AP at branch 1.
	GigabitEthernet0/0/2.2309	192.168.6.254/24	N/A	Service network segment of the branch wireless network.

Device Name	Interface	IPv4 Address	IPv6 Address	Description
	GigabitEthernet0/0/2.2310	192.168.7.254/24	N/A	Service network segment of the branch wireless network.
	Loopback0	1.1.1.18/32	N/A	
AR4	GigabitEthernet0/0/1	192.168.2.1/24	N/A	Service network segment of the wired network.
	GigabitEthernet0/0/2	100.2.21.2/30	N/A	Interface used for connecting AR4 to the IPv4 Internet.
	Loopback0	1.1.1.21/32	N/A	
FW1	GigabitEthernet1/0/1	10.5.22.1/30	N/A	Interface used for connecting FW1 to DCGW1.
	GigabitEthernet1/0/1.10	10.110.110.1/30	N/A	Interface used for connecting FW1 to DCGW1 and added to the Web vSYS.
	GigabitEthernet1/0/1.20	10.120.120.1/30	N/A	Interface used for connecting FW1 to DCGW1 and added to the OA vSYS.
	GigabitEthernet1/0/1.30	10.130.130.1/30	N/A	Interface used for connecting FW1 to DCGW1 and added to the OA vSYS.
	GigabitEthernet1/0/6	10.22.23.1/30	N/A	Heartbeat interface used for connecting FW1 to FW2.
	Virtual-IF 0	172.16.0.1/24	N/A	Virtual interface used for communication between virtual systems.
	Virtual-IF 1	172.16.1.1/24	N/A	Virtual interface used for communication between virtual systems and added to the Web vSYS.

Device Name	Interface	IPv4 Address	IPv6 Address	Description
FW2	GigabitEthernet1/0/1	10.6.23.2/30	N/A	Interface used for connecting FW2 to DCGW2.
	GigabitEthernet1/0/1.10	10.210.210.2/30	N/A	Interface used for connecting FW2 to DCGW2 and added to the Web vSYS.
	GigabitEthernet1/0/1.20	10.220.220.2/30	N/A	Interface used for connecting FW2 to DCGW2 and added to the OA vSYS.
	GigabitEthernet1/0/1.30	10.230.230.2/30	N/A	Interface used for connecting FW2 to DCGW2 and added to the OA vSYS.
	GigabitEthernet1/0/6	10.22.23.2/30	N/A	Heartbeat interface used for connecting FW2 to FW1.
	Virtual-IF 0	172.16.0.1/24	N/A	Virtual interface used for communication between virtual systems.
	Virtual-IF 1	172.16.1.1/24	N/A	Virtual interface used for communication between virtual systems and added to the Web vSYS.
DCGW1	Ethernet1/0/0	10.5.6.1/30	N/A	Interface used for connecting DCGW1 to DCGW2.
	Ethernet1/0/0.56	10.6.5.1/30	N/A	Interface used for connecting DCGW1 to DCGW2 and bound to VPNA.
	Ethernet1/0/1	10.5.22.2/30	N/A	Interface used for connecting DCGW1 to FW1.
	Ethernet1/0/1.10	10.110.110.2/	N/A	Interface used for connecting DCGW1 to

Device Name	Interface	IPv4 Address	IPv6 Address	Description
		30		FW1 and bound to the DC VPN instance.
	Ethernet1/0/1.20	10.120.120.2/30	N/A	Interface used for connecting DCGW1 to FW1 and bound to the DC VPN instance.
	Ethernet1/0/1.30	10.130.130.2/30	N/A	Interface used for connecting DCGW1 to FW1 and bound to VPNA.
	Ethernet1/0/3	100.3.5.2/30	N/A	Interface used for connecting DCGW1 to the public network of PE3.
	Ethernet1/0/3.35	10.3.5.2/30	N/A	Interface used for connecting DCGW1 to PE3 and bound to VPNA.
	Ethernet1/0/4	10.5.7.1/30	N/A	Interface used for connecting DCGW1 to Spine1.
	LoopBack0	1.1.1.5/32	N/A	
	LoopBack1	10.10.10.10/32	N/A	
	Loopback56	1.1.1.56/32	N/A	Functions as the RP of the multicast service.
	Vbdif10	192.168.8.1/24	N/A	The interface is bound to the DC VPN instance.
DCGW2	Ethernet1/0/0	10.5.6.2/30	N/A	Interface used for connecting DCGW2 to DCGW1.
	Ethernet1/0/0.56	10.6.5.2/30	N/A	Interface used for connecting DCGW2 to DCGW1 and bound to VPNA.
	Ethernet1/0/1	10.6.23.1/30	N/A	Interface used for connecting DCGW2 to

Device Name	Interface	IPv4 Address	IPv6 Address	Description
				FW2.
	Ethernet1/0/1.10	10.210.210.1/30	N/A	Interface used for connecting DCGW2 to FW2 and bound to the DC VPN instance.
	Ethernet1/0/1.20	10.220.220.2/30	N/A	Interface used for connecting DCGW2 to FW2 and bound to the DC VPN instance.
	Ethernet1/0/1.30	10.230.230.2/30	N/A	Interface used for connecting DCGW2 to FW2 and bound to VPNA.
	Ethernet1/0/3	100.4.6.2/30	N/A	Interface used for connecting DCGW2 to the public network of PE4.
	Ethernet1/0/3.46	10.4.6.2/30	N/A	Interface used for connecting DCGW2 to PE4 and is bound to VPNA.
	Ethernet1/0/4	10.6.8.1/30	N/A	Interface used for connecting DCGW2 to Spine2.
	LoopBack0	1.1.1.6/32	N/A	
	LoopBack1	10.10.10.10/32	N/A	VTEP
	Loopback56	1.1.1.56/32	N/A	Functions as the RP of the multicast service.
	Vbdif10	192.168.8.1/24	N/A	The interface is bound to the DC VPN instance.
Spine1	LoopBack0	1.1.1.7/32	N/A	
	VLANIF57	10.5.7.2/30	N/A	Interface used for connecting Spine1 to DCGW1.
	VLANIF78	10.7.8.1/30	N/A	Interface used for

Device Name	Interface	IPv4 Address	IPv6 Address	Description
				connecting Spine1 to Spine2.
	VLANIF79	10.7.9.1/30	N/A	Interface used for connecting Spine1 to Leaf1.
Spine2	LoopBack0	1.1.1.8/32	N/A	
	VLANIF68	10.6.8.2/30	N/A	Interface used for connecting Spine2 to DCGW2.
	VLANIF78	10.7.8.2/30	N/A	Interface used for connecting Spine2 to Spine1.
	VLANIF89	10.8.9.1/30	N/A	Interface used for connecting Spine2 to Leaf1.
Leaf1	GigabitEthernet1/0/0	100.2.10.1/24	N/A	Interface used for connecting Leaf1 to the multicast server.
	GigabitEthernet1/0/2	10.7.9.2/30	N/A	Interface used for connecting Leaf1 to Spine1.
	GigabitEthernet1/0/3	10.8.9.2/30	N/A	Interface used for connecting Leaf1 to Spine2.
	Loopback0	1.1.1.9/32	N/A	
PC1	Ethernet0/0/1	192.168.3.100/24	192:168:3::100/64	
PC2	Ethernet0/0/1	192.168.1.100/24	192:168:1::100/64	
PC3	Ethernet0/0/1	192.168.2.100/24	N/A	
OA Server	Ethernet0/0/1	192.168.8.100/24	N/A	
Web Server	Ethernet0/0/1	192.168.8.2/24	N/A	Public IP address: 100.1.10.1

Device Name	Interface	IPv4 Address	IPv6 Address	Description
Multicast Server	Ethernet0/0/1	100.2.10.2/24	N/A	

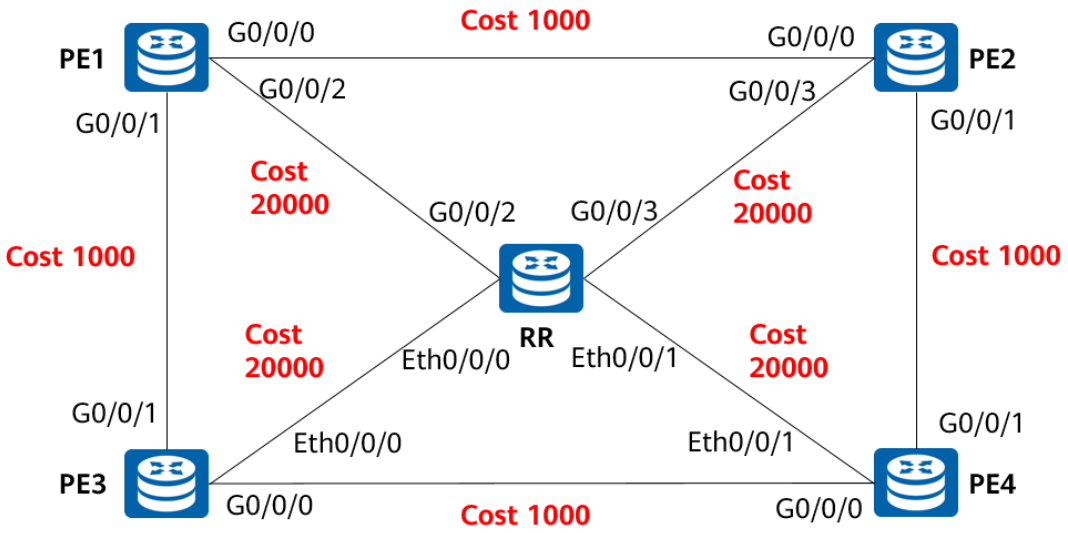
4.2 Task 2: Deploying IGP and BGP on the Carrier MAN

4.2.1 IGP Deployment

On the carrier's MAN, PE1, PE2, PE3, and PE4 are MAN access routers, responsible for providing access services for the enterprise HQ, enterprise branch 1, enterprise branch 2, and data center. Deploy IS-IS between PEs to implement interworking between addresses (IPv4/IPv6) of interconnected interfaces and between addresses (IPv4/IPv6) of loopback interfaces on nodes on the MAN. The configuration requirements are as follows:

1. Set the IS-IS process ID to 100, area ID to 86.0001, and IS-IS level to Level-2. Calculate the system IDs of IS-IS routers based on the IPv4 addresses of their loopback 0 interfaces. For example, if the IPv4 address of a loopback 0 interface is 1.1.1.1, the system ID will be 0010.0100.1001.
2. Configure the cost values of the links according to the data plan. The cost values of the interfaces at the two ends of a link are the same. For example, the cost value 1000 between PE1 and PE2 indicates that the cost values of the interfaces connecting PE1 and PE2 are both 1000.

Figure 4-1 IS-IS cost plan



3. To speed up IGP convergence, configure IS-IS routers on the MAN not to perform DIS election. Configure the intelligent timer for generating LSPs as follows: maximum delay (1s), initial delay (50 ms), and incremental delay (50 ms). Adjust the SPF calculation time

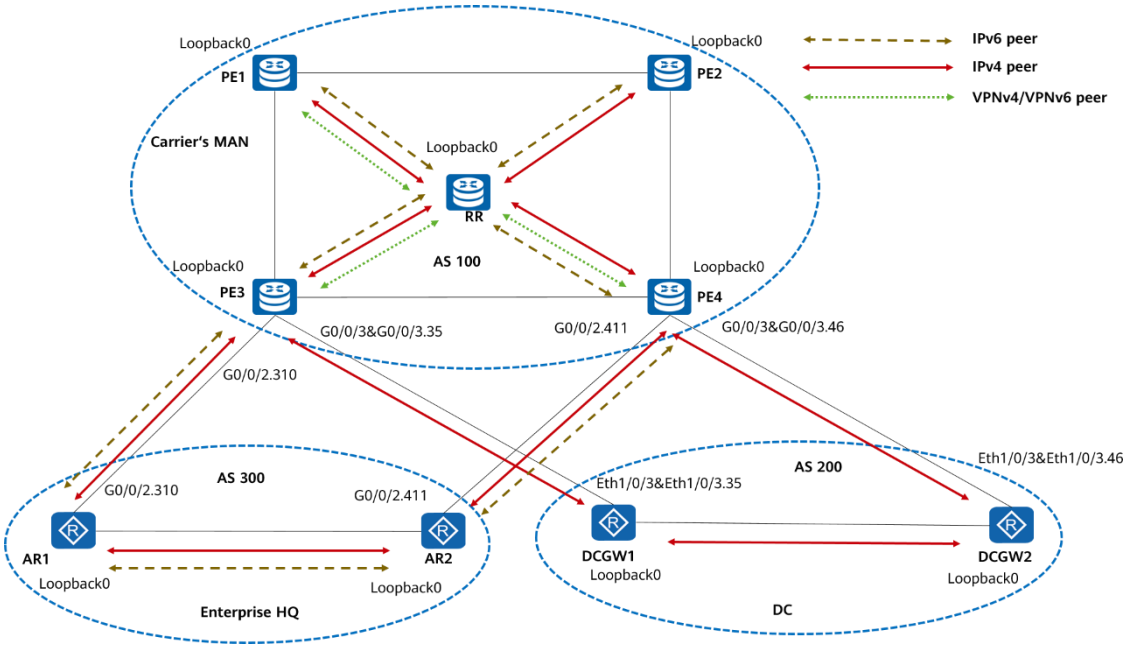
as follows: maximum delay (1s), initial delay (50 ms), and incremental delay (50 ms). Enable LSP fast flooding. Configure dynamic BFD for IS-IS. Enable BFD on all IS-IS interfaces and set the detection interval to 2000 ms (500 ms x 4). In this manner, IS-IS can detect neighbor state changes more quickly, ensuring fast network convergence.

4. To prevent malicious packets from attacking the network, configure IS-IS authentication for improved network security. Configure MD5 authentication for IS-IS Hello packets, and set the authentication password to **Huawei@123**.
5. Enable IS-IS dual-stack, ensure that IPv4 and IPv6 topologies are calculated independently, and set the same cost for IPv4 and IPv6 on each interface.

4.2.2 BGP Deployment

Deploy IBGP on the carrier's MAN to transmit service routes, including IPv4, IPv6, VPNv4, and VPNv6 routes. Deploy EBGP between the carrier's MAN and enterprise HQ, and between the carrier's MAN and data center, to transmit service routes, including IPv4 and IPv6 routes. The following figure shows the BGP peer relationships.

Figure 4-2 BGP peer relationships



The configuration requirements are as follows:

1. IBGP deployment on the carrier's MAN:
   (1) The AS number of the carrier's MAN is 100. Use the IP address of the loopback0 interface on each device as the router ID.
   (2) Configure the RR (as an IPv4 unicast RR on the MAN) to establish IPv4 unicast peer relationships with PE1, PE2, PE3, and PE4 using the IPv4 addresses of loopback 0 interfaces. Do not establish peer relationships between the PEs.

(3) Configure the RR (as a VPNv4 and VPNv6 RR on the MAN) to establish VPNv4 and VPNv6 peer relationships with PE1, PE3, and PE4 using the IPv4 addresses of loopback 0 interfaces. Do not establish peer relationships between the PEs.

(4) Configure the RR (as an IPv6 unicast RR on the MAN) to establish IPv6 unicast peer relationships with PE1, PE2, PE3, and PE4 using the IPv6 addresses of loopback 0 interfaces. Do not establish peer relationships between the PEs.

2. EBGP deployment between the carrier's MAN and data center:

(1) The AS number of the data center is 200. Use the IP address of the loopback0 interface on each device as the router ID.

(2) Establish public network IPv4 peer relationships and VPN instance IPv4 peer relationships between PE3 and DCGW1, and between PE4 and DCGW2, using the IPv4 addresses of their directly connected interfaces, as shown in the figure. For details about the VPN configuration requirements, see task 7.

(3) Enable GTSM on all EBGP IPv4 peers to limit the minimum number of hops.

(4) To divert traffic, establish an IPv4 peer relationship between DCGW1 and DCGW2 so that traffic can be transmitted over the link between the DCGWs if the uplink fails.

3. EBGP deployment between the carrier's MAN and the enterprise HQ:

(1) The AS number of the enterprise HQ is 300. Use the IP address of the loopback0 interface on each device as the router ID.

(2) Establish IPv4 and IPv6 peer relationships between PE3 and AR1 and between PE4 and AR2 in the BGP VPN instance (for detailed VPN configuration requirements, see task 7) using addresses of directly connected interfaces.

(3) Enable GTSM on all EBGP IPv4 peers to limit the minimum number of hops.

(4) To divert traffic, establish IPv4 and IPv6 peer relationships between AR1 and AR2 so that traffic can be transmitted over the link between the ARs if the uplink fails.

Table 4-3 BGP peer relationship list

Local Device	Local Interface	Remote Device	Remote Interface	Peer Relationship Type
RR	Loopback0	PE1	Loopback0	IPv4/IPv6/VPNv4/VPNv6
RR	Loopback0	PE3	Loopback0	IPv4/IPv6/VPNv4/VPNv6
RR	Loopback0	PE4	Loopback0	IPv4/IPv6/VPNv4/VPNv6
RR	Loopback0	PE2	Loopback0	IPv4/IPv6
PE3	G0/0/2.310	AR1	G0/0/2.310	IPv4/IPv6 (VPN instance)
PE4	G0/0/2.411	AR2	G0/0/2.411	IPv4/IPv6 (VPN instance)
PE3	G0/0/3	DCGW1	Eth1/0/3	IPv4
PE3	G0/0/3.35	DCGW1	Eth1/0/3.35	IPv4 (VPN instance)
PE4	G0/0/3	DCGW2	Eth1/0/3	IPv4

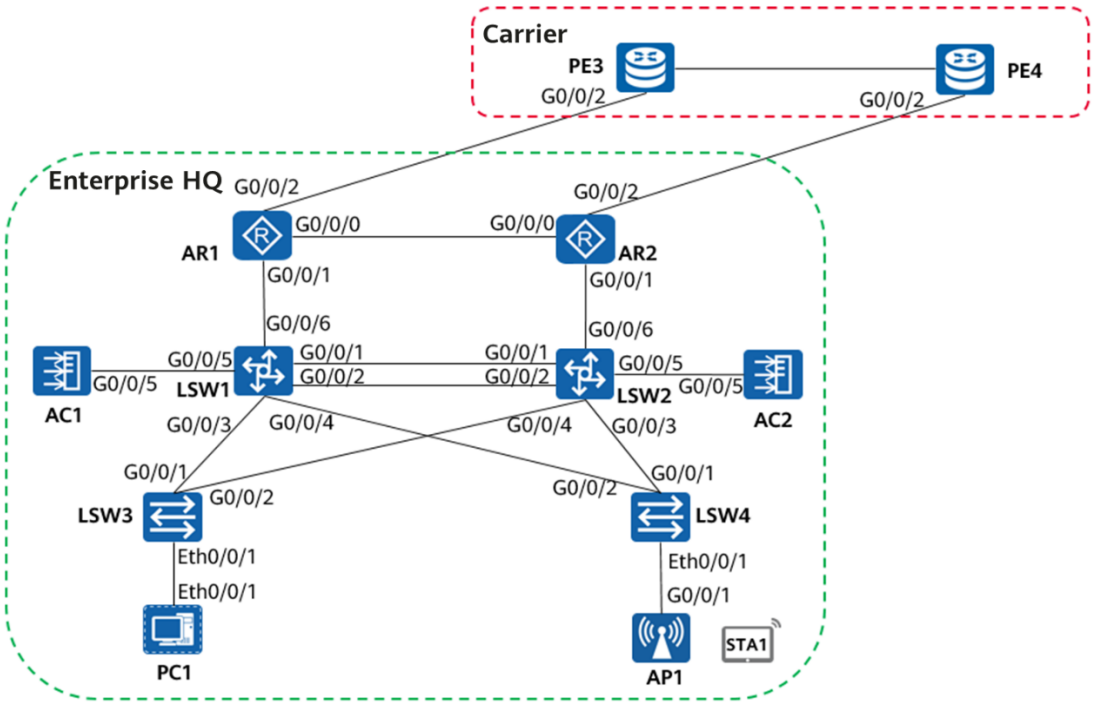
Local Device	Local Interface	Remote Device	Remote Interface	Peer Relationship Type
PE4	G0/0/3.46	DCGW2	Eth1/0/3.46	IPv4 (VPN Instance)
AR1	Loopback0	AR2	Loopback0	IPv4/IPv6
DCGW1	Loopback0	DCGW2	Loopback0	IPv4

4.3 Task 3: Network Deployment for the Enterprise HQ

4.3.1 Wired Network Deployment

LSW3 and LSW4 on the enterprise HQ network are access switches providing Layer 2 access. LSW1 and LSW2 are core switches and function as gateways for wired and wireless terminals at the HQ. LSW1 and LSW2 run OSPFv2 and OSPFv3 to exchange network segment routes of wired and wireless networks with the egress routers of the HQ AR1 and AR2, respectively.

Figure 4-3 Interfaces of the enterprise HQ



1. Configure the IP addresses and gateway addresses of the host at the HQ according to the following address data plan.

Table 4-4 Address data plan

Device Name	NIC IP Address	Gateway	Gateway IP Address
PC1	192.168.3.100/24	LSW1&LSW2 (VLANIF 2301)	192.168.3.254/24
	192:168:3::100/64	LSW1 (VLANIF 2301)	192:168:3::1/64

VLAN 2301 is the service VLAN of the wired network. Create VLANIF 2301 on LSW1 and LSW2 as the gateway. Deploy VRRP on LSW1 and LSW2, with the virtual router ID (VRID) of 1 and the virtual IP address (VIP) of 192.168.3.254. Configure LSW1 as the VRRP master and LSW2 as the VRRP backup. For IPv6 services, use the single-gateway mode and configure VLANIF 2301 of LSW1 as the gateway with the IP address of 192:168:3::1/64.

2. Configure link aggregation in LACP mode on LSW1 and LSW2, and set the Eth-Trunk ID to 1.
3. Deploy Rapid Spanning Tree Protocol (RSTP) on LSW1, LSW2, LSW3, and LSW4 to prevent loops. Configure LSW1 as the root switch of the STP network. When LSW1 fails, LSW2 can be upgraded to the root switch. Configure root protection on the ports of the corresponding devices.
4. Configure LSW1, LSW2, AR1, and AR2 to run OSPFv2 and OSPFv3 to exchange service network segment routes, with the OSPF process 1 and area 0 in use. Configure AR1 and AR2 to use OSPFv2 and OSPFv3 to deliver non-forcible default routes to direct upstream traffic out of the enterprise HQ.

4.3.2 Wireless Network Deployment

Deploy a WLAN for the enterprise HQ, and connect ACs to the Layer 3 network in off-path mode. Configure the switches on the enterprise intranet so that APs can communicate with the ACs and so that STAs connected to the APs can obtain network services after connecting to the WLAN. The configuration requirements are as follows:

1. Configure APs to automatically obtain management addresses on LSW1 and LSW2. Configure DHCP and VRRP on LSW1 and LSW2. Configure LSW1 as the active DHCP server and LSW2 as the standby DHCP server to assign IP addresses to APs. Ensure that APs register with the ACs at Layer 3 and join the AP group at the HQ.

Table 4-5 DHCP parameter plan for AP management addresses

Device Name	Management VLAN for APs	VLANIF IP Address	DHCP Address Pool	DHCP Gateway Address	AP Group
LSW1	VLAN 2306	172.16.3.253/24 (VRRP)	172.16.3.0/24	172.16.3.254/24	HQ
LSW2	VLAN 2306	172.16.3.252/24 (VRRP)	172.16.3.0/24	172.16.3.254/24	HQ

2. Configure STAs to automatically obtain service addresses on LSW1 and LSW2. Configure DHCP and VRRP on LSW1 and LSW2. Configure LSW1 as the active DHCP server and LSW2 as the standby DHCP server to assign IP addresses to STAs.

Table 4-6 DHCP parameter plan for STA service addresses

Device Name	Service VLAN	VLANIF IP Address	DHCP Address Pool	DHCP Gateway Address	SSID
LSW1	VLAN 2307	192.168.4.253/24 (VRRP)	192.168.4.0/24	192.168.4.254/24	Employee
	VLAN 2308	192.168.5.253/24 (VRRP)	192.168.5.0/24	192.168.5.254/24	Guest
LSW2	VLAN 2307	192.168.4.252/24 (VRRP)	192.168.4.0/24	192.168.4.254/24	Employee
	VLAN 2308	192.168.5.252/24 (VRRP)	192.168.5.0/24	192.168.5.254/24	Guest

3. Provide WLAN access for employees. Set the SSID of the WLAN to **Employee**, password to **Huawei@123**, security policy to WPA-WPA2+PSK+AES, and forwarding mode to direct forwarding.
4. Provide WLAN access for guests. Set the SSID of the WLAN to **Guest**, password to **Huawei@123**, security policy to WPA-WPA2+PSK+AES, and forwarding mode to direct forwarding.
5. Configure ACL filtering on LSW4 so that guests can access only Internet resources but cannot access the enterprise intranet.
6. Deploy VRRP hot standby (HSB) to implement AC HSB and improve data transmission reliability for STAs. Configure a VRRP group on AC1 and AC2. Configure a higher priority for AC1 so that AC1 functions as the master device, and configure a lower priority for AC2 so that AC2 functions as the backup device. Use the HSB function to back up service information on AC1 to AC2, ensuring that services can be switched to the backup device when the master device fails.
7. Configure the working channel and power of APs. For 2.4 GHz radios, set the channel to 1 and power to 25. For 5 GHz radios, set the channel to 149 and power to 25.
8. Configure the band steering function. Set the start threshold for the number of access users to 15, and the proportion threshold for 5 GHz users to 20%.
9. Configure the smart roaming function. Set the smart roaming triggering mode to **check-snr** and the SNR threshold to 15 dB.
10. Configure the user CAC function, set the thresholds for the number of new access users and roaming users both to 20, enable the function of denying access from weak-signal STAs, and set the signal threshold to 25 dB.
11. To prevent STAs from maliciously occupying network resources and reduce network congestion, limit the uplink and downlink rates of each STA on an AP both to 2 Mbit/s.
12. Configure port isolation on LSW4. Enable Layer 2 user isolation on the AC to prevent Layer 2 communication between user terminals associated with the same SSID and in the same VLAN.

Table 4-7 WLAN service data plan

Configuration Item	Setting
Management VLAN for APs	VLAN 2306
Service VLAN for STAs connected to the SSID **Employee**	VLAN 2307
Service VLAN for STAs connected to the SSID **Guest**	VLAN 2308
IP address pool for APs	172.16.3.0/24 (Gateway: 172.16.3.254)
IP address pool for STAs connected to the SSID **Employee**	192.168.4.0/24 (Gateway: 192.168.4.254)
IP address pool for STAs connected to the SSID **Guest**	192.168.5.0/24 (Gateway: 192.168.5.254)
IP address of AC1's and AC2's source interface	VRRP VIP: 172.16.2.254/24 (VLANIF IP address of AC1: 172.16.2.253/24, VLANIF IP address of AC2: 172.16.2.252/24)
HSB channel parameters on AC1	IP address: 172.16.2.253/24 of VLANIF 2305 (VRRP interface IP address) Port number: 10241
HSB channel parameters on AC2	IP address: 172.16.2.252/24 of VLANIF 2305 (VRRP interface IP address) Port number: 10241
HSB parameters consistent on AC1 and AC2	HSB service: 0 HSB group: 0
AP group	Name: HQ
	Referenced profiles: regulatory domain profile **default**, radio profiles **radio2g** and **radio5g**, and VAP profiles **HQ-Employee** and **HQ-Guest**
Regulatory domain profile	Name: default
	Country code: CN
2.4 GHz radio profile	Name: radio2g
	Referenced profiles: RRM profiles **wlan-5G**, **smart-roam**, and **user-cac**
5 GHz radio profile	Name: radio5g
	Referenced profile: RRM profile **smart-roam**

Configuration Item	Setting
RRM profiles	Name: wlan-5G
	Start threshold for the number of 5 GHz access users: 15 Proportion threshold for 5 GHz users: 20%
	Name: smart-roam
	Smart roaming triggering mode: check-snr SNR threshold for smart roaming: 15 dB
	Name: user-cac
	CAC threshold for new access users: 20 CAC threshold for roaming users: 20 RSSI threshold for rejecting access from weak-signal STAs: 25 dB
VAP profiles	Name: HQ-Employee
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 2307
	Referenced profiles: SSID profile **employee**, security profile **employee**, and traffic profile **wlan-traffic**
	Name: HQ-Guest
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 2308
	Referenced profiles: SSID profile **guest**, security profile **guest**, and traffic profile **wlan-traffic**
SSID profiles	Name: employee
	SSID name: Employee
	Name: guest
	SSID name: Guest
Security profiles	Name: employee
	Security policy: WPA-WPA2+PSK+AES
	Password: Huawei@123
	Name: guest
	Security policy: WPA-WPA2+PSK+AES

Configuration Item	Setting
	Password: Huawei@123
Traffic profile	Name: wlan-traffic
	STA uplink rate limit: 2 Mbit/s
	STA downlink rate limit: 2 Mbit/s
	User isolation mode: Layer 2 isolation and Layer 3 communication

4.3.3 Internet Access of the HQ

The enterprise HQ needs to access the IPv4 and IPv6 Internet. For IPv4 Internet access, configure NAT on ARs to translate uses private IP addresses on the HQ intranet into public addresses. For IPv6 Internet access, configure routes as required.

1. Create Loopback8 on PE2 to simulate the IPv4 Internet (8.8.8.8/32) and IPv6 Internet (8::8/128).
2. On AR1, configure a default route to PE3 to access the IPv4 and IPv6 Internet. On AR2, configure a default route destined to PE4 to access the IPv4 and IPv6 Internet.

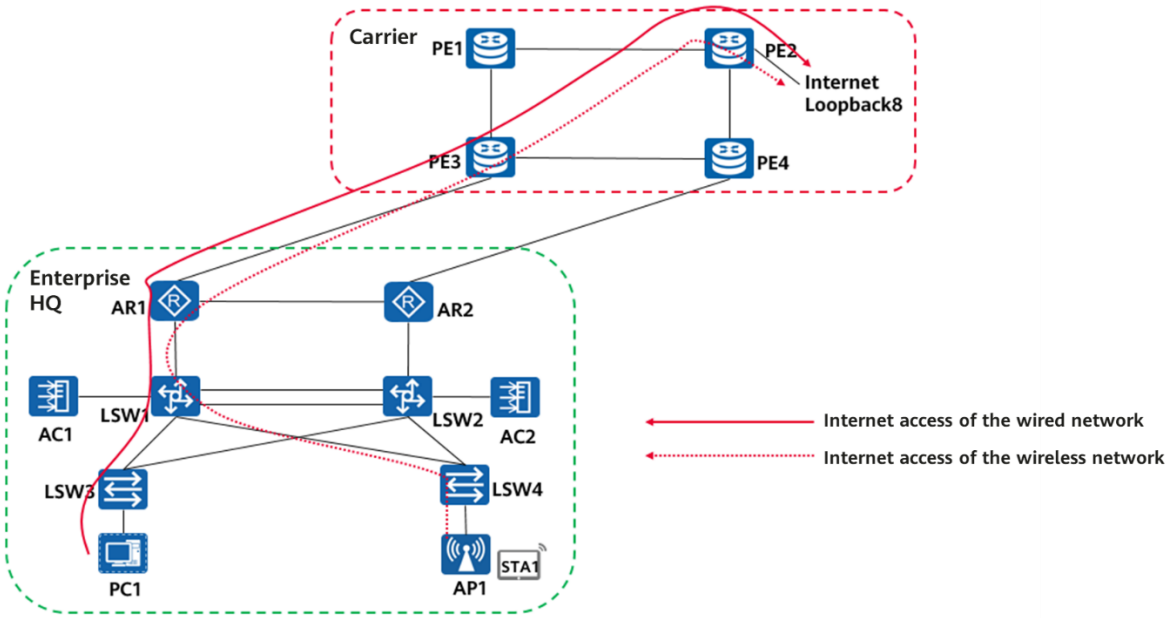
Table 4-8 AR-PE interconnection description

Local Interface	Peer Interface	Description
AR1 G0/0/2.310	PE3 G0/0/2.310	Used for MPLS VPN access (in task 7)
AR1 G0/0/2.320	PE3 G0/0/2.320	Default route of AR1 to PE3, used for IPv4 Internet access
AR1 G0/0/2.330	PE3 G0/0/2.330	Default route of AR1 to PE3, used for IPv6 Internet access
AR2 G0/0/2.411	PE4 G0/0/2.411	Used for MPLS VPN access (in task 7)
AR2 G0/0/2.421	PE4 G0/0/2.421	Default route of AR2 to PE4, used for IPv4 Internet access
AR2 G0/0/2.431	PE4 G0/0/2.431	Default route of AR2 to PE4, used for IPv6 Internet access

3. For intranet IPv4 access to the Internet, configure ACLs on AR1 and AR2 to filter service network segments for wired and wireless services (with SSIDs of Employee and Guest). Ensure that NAT can be performed only on network segments in the whitelist. Configure the public address pools 2.2.2.0/24 and 3.3.3.0/24 on AR1 and AR2, respectively.

4. For intranet IPv6 access to the Internet, NAT is not required. Configure IPv6 routes to access the Internet.

Figure 4-4 Accessing the Internet from the enterprise HQ



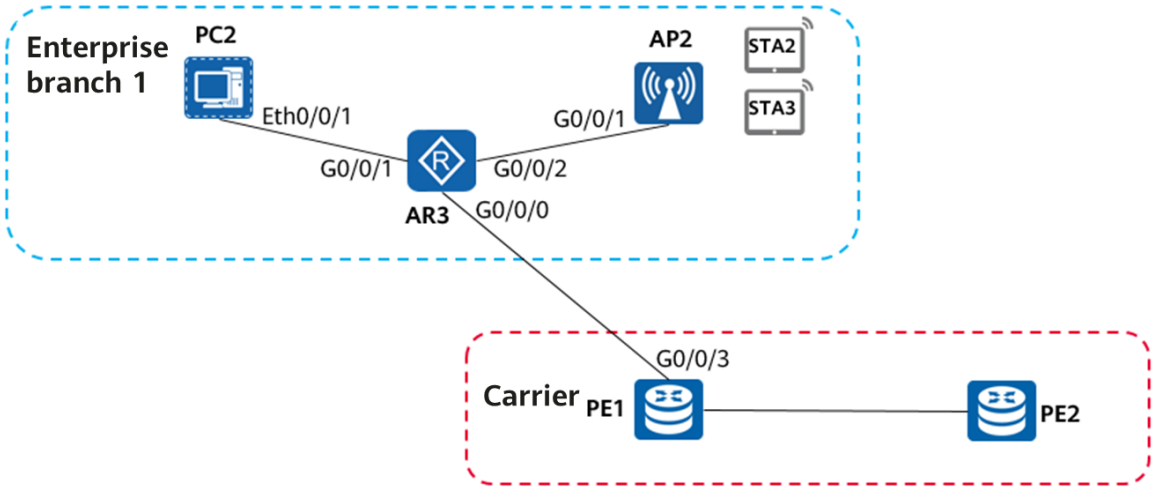
5. After the preceding configurations are complete, terminals at the HQ can ping the simulated IPv4 and IPv6 Internet addresses on PE2.

4.4 Task 4: Network Deployment for Enterprise Branch 1

4.4.1 Wired Network Deployment

AR3 is the egress gateway at enterprise branch 1 and connects to PE1. PC2 is a dual-stack PC and is directly connected to AR3.

Figure 4-5 Interfaces of enterprise branch 1



1. Configure the IP addresses and gateway addresses of the host at enterprise branch 1 according to the following address data plan.

Table 4-9 Address data plan

Device Name	NIC IP Address	Gateway	Gateway IP Address
PC2	192.168.1.100/24	AR3 (G0/0/1)	192.168.1.1/24
	192:168:1::100/64	AR3 (G0/0/1)	192:168:1::1/64

4.4.2 Wireless Network Deployment

Deploy a WLAN for enterprise branch 1. After the configuration for MPLS VPN communication between enterprise branch 1 and the HQ is complete (in task 7), APs at the branch can communicate with the ACs at the HQ. Add the APs to the branch AP group **Branch-1**. Ensure that STAs associated the APs can obtain network services after connecting to the WLAN. The configuration requirements are as follows:

1. Configure AR3 as a DHCP server to assign IP addresses to APs so that APs register with the ACs at the HQ at Layer 3 and join the branch AP group.

Table 4-10 DHCP parameter plan for AP management addresses

Device Name	Interface	IP Address	DHCP Address Pool	DHCP Gateway Address	AP group
AR3	GigabitEthernet0/0/2	172.16.4.254/24	172.16.4.0/24	172.16.4.254/24	Branch-1

2. Configure AR3 as a DHCP server to assign IP addresses to STAs.

Table 4-11 DHCP parameter plan for STA service addresses

Device Name	Interface	IP Address	DHCP Address Pool	DHCP Gateway Address	SSID
AR3	GigabitEthernet0/0/2.2309	192.168.6.254/24	192.168.6.0/24	192.168.6.254/24	Guest
	GigabitEthernet0/0/2.2310	192.168.7.254/24	192.168.7.0/24	192.168.7.254/24	Employee

3. Provide WLAN access for employees. Set the SSID of the WLAN to **Employee**, password to **Huawei@123**, security policy to WPA-WPA2+PSK+AES, and forwarding mode to direct forwarding.
4. Provide WLAN access for guests. Set the SSID of the WLAN to **Guest**, password to **Huawei@123**, security policy to WPA-WPA2+PSK+AES, and forwarding mode to direct forwarding.
5. Configure ACL filtering on AR3 so that guests can access only Internet resources but cannot access the enterprise intranet.
6. Configure the working channel and power of APs. For 2.4 GHz radios, set the channel to 1 and power to 25. For 5 GHz radios, set the channel to 149 and power to 25.
7. The network administrator detects that STA3 is a rogue STA. Add its MAC address to the STA blacklist to forbid it from accessing the WLAN. STAs whose MAC addresses are not blacklisted can access the WLAN.
8. Configure the band steering function. Set the start threshold for the number of access users to 15, and the proportion threshold for 5 GHz users to 20%.
9. Configure the smart roaming function. Set the smart roaming triggering mode to **check-snr** and the SNR threshold to 15 dB.
10. Configure the user CAC function, set the thresholds for the number of new access users and roaming users both to 20, enable the function of denying access from weak-signal STAs, and set the signal threshold to 25 dB.
11. To prevent STAs from maliciously occupying network resources and reduce network congestion, limit the uplink and downlink rates of each STA on an AP both to 2 Mbit/s.

Table 4-12 WLAN service data plan

Configuration Item	Setting
Service VLAN for STAs connected to the SSID **Employee**	VLAN 2310
Service VLAN for STAs connected to the SSID **Guest**	VLAN 2309

Configuration Item	Setting
IP address pool for APs	172.16.4.0/24 (Gateway: 172.16.4.254)
IP address pool for STAs connected to the SSID **Employee**	192.168.7.0/24 (Gateway: 192.168.7.254)
IP address pool for STAs connected to the SSID **Guest**	192.168.6.0/24 (Gateway: 192.168.6.254)
AP group	Name: Branch-1
	Referenced profiles: regulatory domain profile **default**, radio profiles **radio2g** and **radio5g**, and VAP profiles **Branch-Employee** and **Branch-Guest**
Regulatory domain profile	Name: default
	Country code: CN
2.4 GHz radio profile	Name: radio2g
	Referenced profiles: RRM profiles **wlan-5G**, **smart-roam**, and **user-cac**
5 GHz radio profile	Name: radio5g
	Referenced profile: RRM profile **smart-roam**
RRM profiles	Name: wlan-5G
	Start threshold for the number of 5 GHz access users: 15 Proportion threshold for 5 GHz users: 20%
	Name: smart-roam
	Smart roaming triggering mode: check-snr SNR threshold for smart roaming: 15 dB
	Name: user-cac
	CAC threshold for new access users: 20 CAC threshold for roaming users: 20 RSSI threshold for rejecting access from weak-signal STAs: 25 dB
VAP profiles	Name: Branch-Employee
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 2310
	Referenced profiles: SSID profile **employee**, security

Configuration Item	Setting
	profile **employee**, traffic profile **wlan-traffic**, and STA blacklist profile **sta-blacklist**
	Name: Branch-Guest
	Forwarding mode: direct forwarding
	Service VLAN: VLAN 2309
	Referenced profiles: SSID profile **guest**, security profile **guest**, traffic profile **wlan-traffic**, and STA blacklist profile **sta-blacklist**
STA blacklist profile	Name: sta-blacklist
	Blacklisted STA: STA3 (5489-98E2-5F9B)

4.4.3 Internet Access of Enterprise Branch 1

Enterprise branch 1 needs to access the IPv4 and IPv6 Internet. For IPv4 Internet access, configure NAT on AR3 to translate uses private IP addresses on the network at enterprise branch 1 into public addresses. For IPv6 Internet access, configure routes as required.

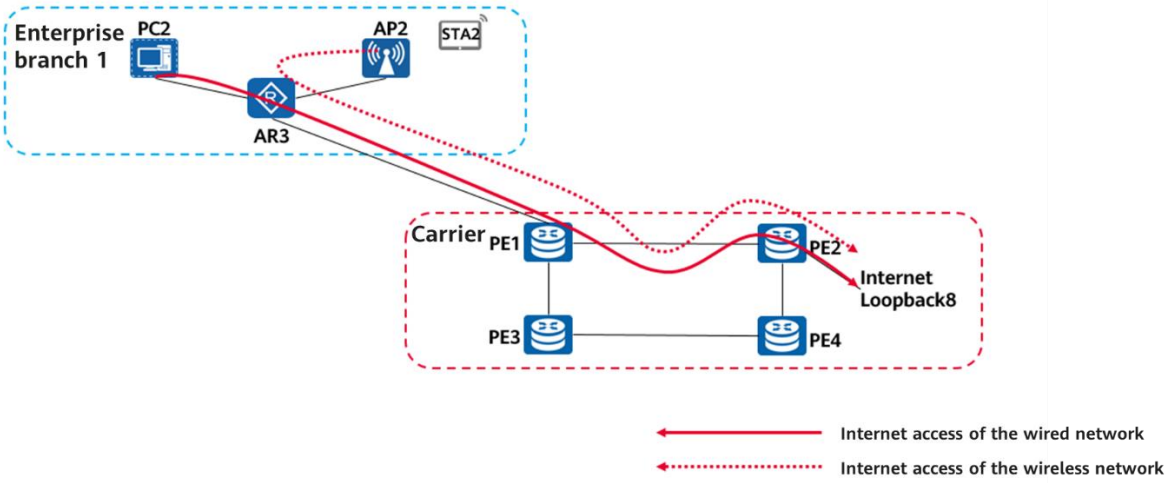
1. On the egress router of enterprise branch 1 AR3, configure a default route to the Internet for accessing the IPv4 and IPv6 Internet.

Table 4-13 AR3-PE1 interconnection description

Local Interface	Peer Interface	Remarks
AR3 G0/0/0.118	PE1 G0/0/3.118	Used for MPLS VPN access (in task 7)
AR3 G0/0/0.128	PE1 G0/0/3.128	Default route of AR3 to PE1, used for IPv4 Internet access
AR3 G0/0/0.138	PE1 G0/0/3.138	Default route of AR3 to PE1, used for IPv6 Internet access

2. For intranet IPv4 access to the Internet, configure ACLs on AR3 to filter service network segments for wired and wireless services (with SSIDs of **Employee** and **Guest**). Ensure that NAT can be performed only on network segments in the whitelist. Configure the public address pool 4.4.4.0/24 on AR3.
3. For intranet IPv6 access to the Internet, NAT is not required. Configure IPv6 routes to access the Internet.

Figure 4-6 Accessing the Internet from enterprise branch 1



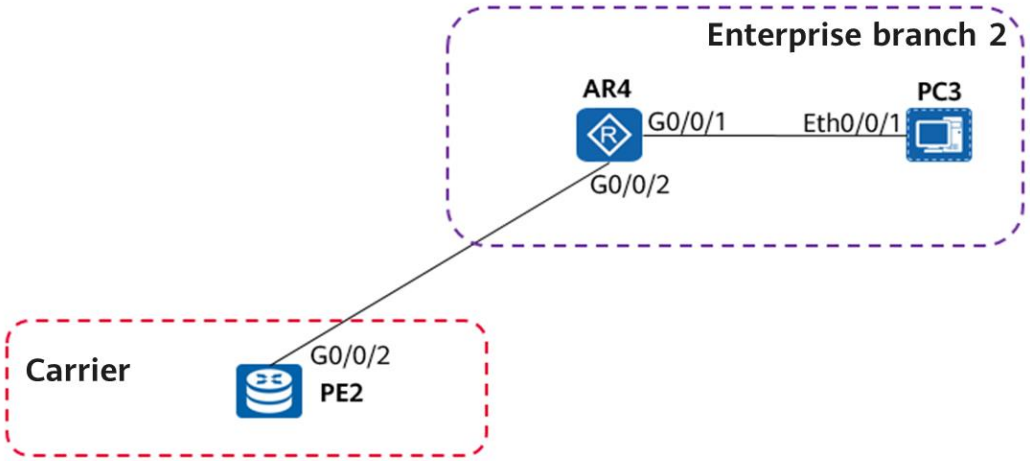
4. After the configuration is complete, terminals on the wired and wireless networks of enterprise branch 1 can ping the simulated IPv4 and IPv6 Internet addresses on PE2.

4.5 Task 5: Network Deployment for Enterprise Branch 2

4.5.1 Wired Network Deployment

AR4 is the egress gateway at enterprise branch 2 and connects to PE2. PC3 is a dual-stack PC and is directly connected to AR4.

Figure 4-7 Interfaces of enterprise branch 2



1. Configure the IP addresses and gateway addresses of the host at enterprise branch 2 according to the following address data plan.

Table 4-14 Address data plan

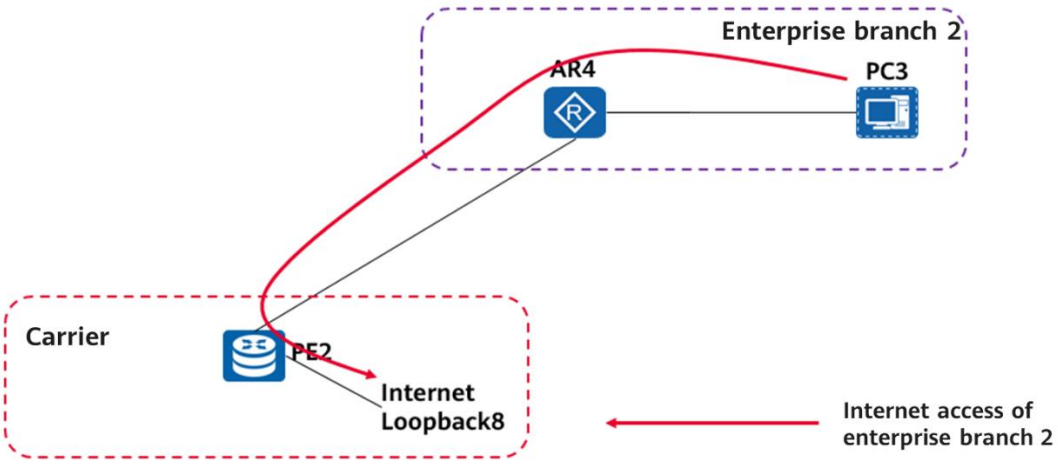
Device Name	NIC IP Address	Gateway	Gateway IP Address
PC3	192.168.2.100/24	AR4 (G0/0/1)	192.168.2.1/24

4.5.2 Internet Access of Enterprise Branch 2

Enterprise branch 2 needs to access the IPv4 and IPv6 Internet. For IPv4 Internet access, configure NAT on AR4 to translate uses private IP addresses on the network at enterprise branch 2 into public addresses. For IPv6 Internet access, configure routes as required.

1. For intranet IPv4 access to the Internet, configure ACLs on AR4 to filter the intranet wired service network segment. Ensure that NAT can be performed only on network segments in the whitelist. Configure NAT in Easy IP mode on AR3.
2. For intranet IPv6 access to the Internet, NAT is not required. Configure IPv6 routes to access the Internet.

Figure 4-8 Accessing the Internet from enterprise branch 2



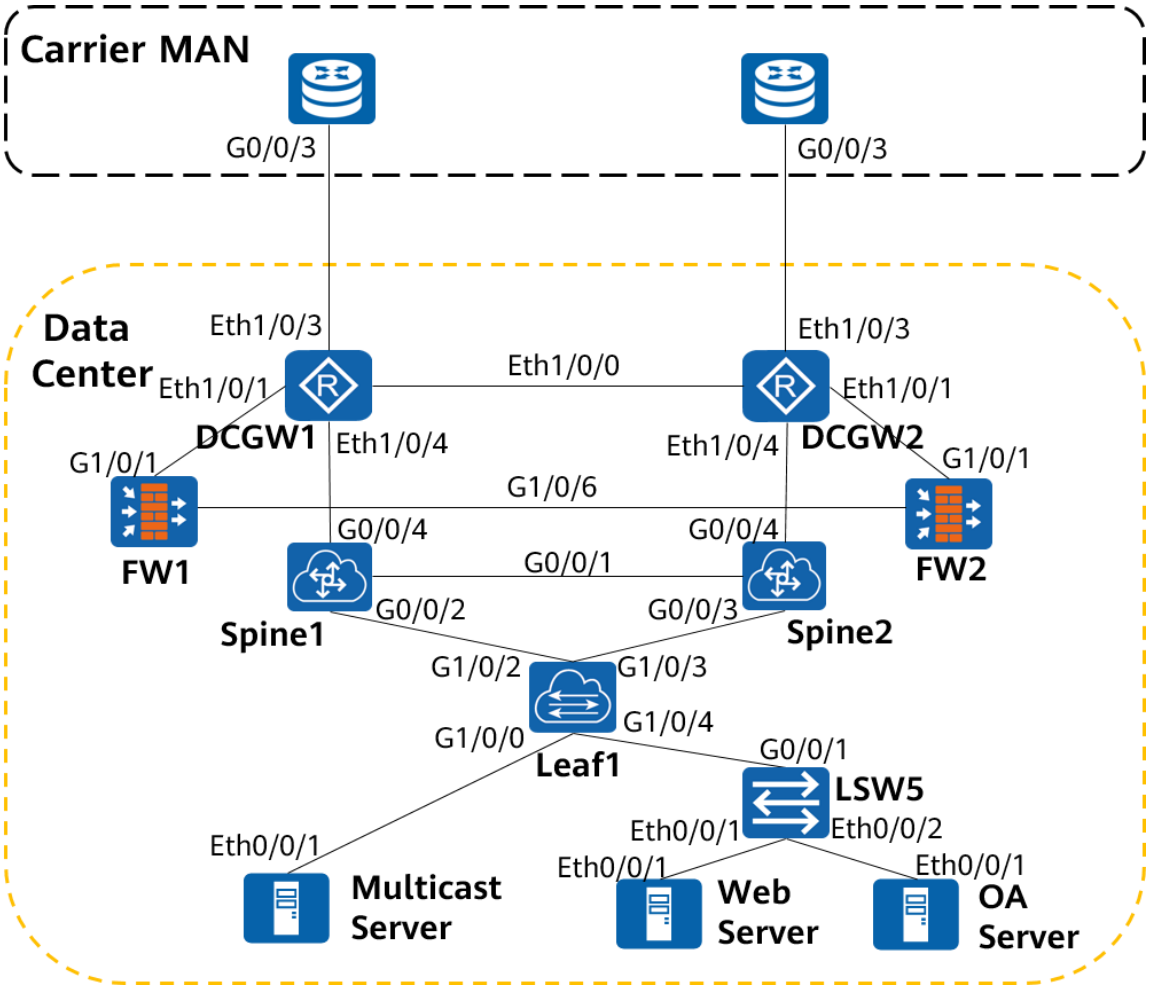
4.6 Task 6: Data Center Network Deployment

4.6.1 Underlay Network Deployment

Figure 4-9 shows the network topology of a carrier's data center. The OA Server, Web Server, and Multicast Server are service servers hosted by an enterprise in the DC. After the data center network is configured, these service servers can meet the enterprise's requirements for daily office work and external communication.

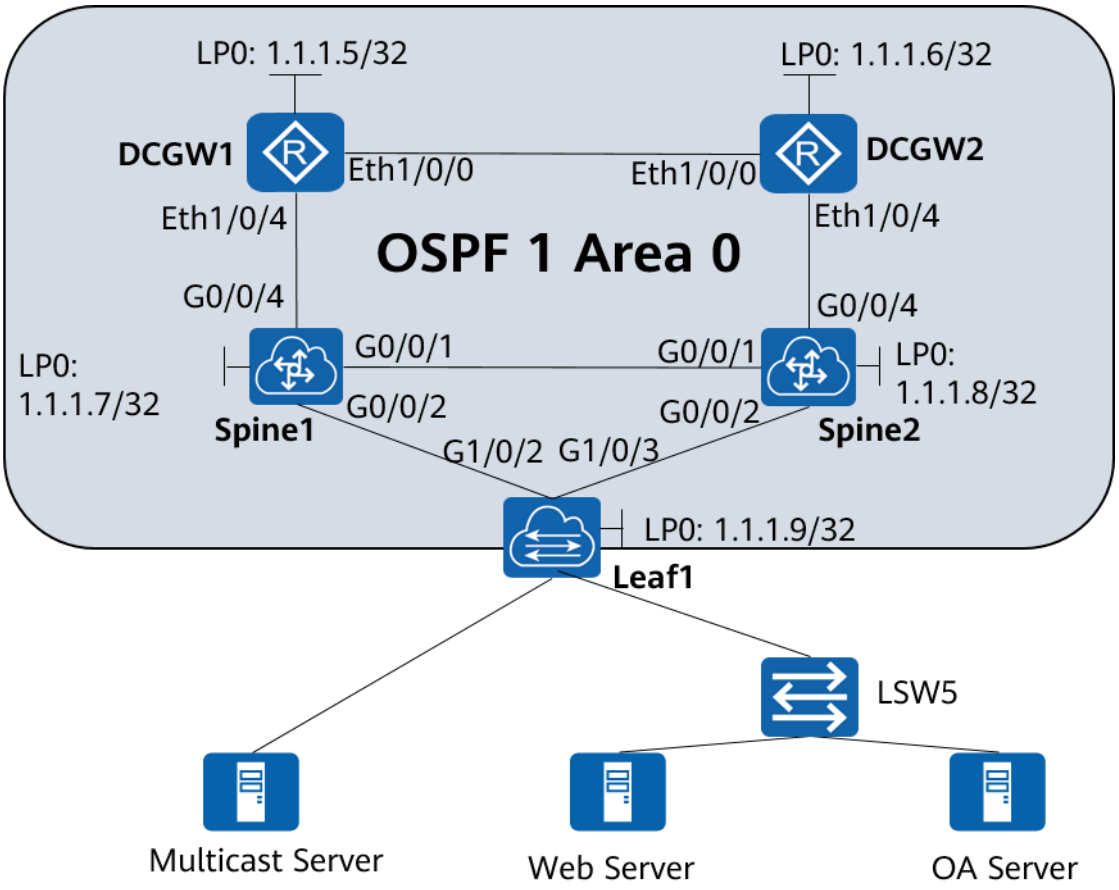
The carrier's DC uses OSPF for Layer 3 interconnection on the underlay network.

Figure 4-9 Data center topology



1. Deploy OSPF between DCGW1, DCGW2, Spine1, Spine2, and Leaf1 to transmit network segment routes and loopback interface routes between devices. Set the OSPF process ID to 1, area ID to 0, and network segment advertisement mode to Network. Enable interface authentication, set the authentication mode to MD5, and set the authentication password to **Admin@123**.

Figure 4-10 OSPF interfaces



2. To speed up IGP convergence, configure OSPF devices not to elect a DR. In addition, configure BFD for OSPF and set the detection interval to 500 ms x 3 to further speed up network convergence.

4.6.2 Overlay Network Deployment

The enterprise hosts the Web Server and OA Server in the carrier's DC. The two servers implement VLAN access through LSW5. The gateways of the Web Server and OA Server are both configured on DCGWs. A VXLAN tunnel is deployed between the Leaf1 and DCGWs to ensure that the Web Server and OA Server can communicate with the DCGWs. All traffic for accessing the Web Server and OA Server must be transmitted through the VXLAN tunnel. To improve gateway reliability, deploy DCGWs in active-active mode. The detailed planning is as follows:

1. Dynamically establish a VXLAN tunnel between Leaf1 and DCGWs through EVPN. DCGW1 and DCGW2 are active-active gateways for the Web Server and OA Server. Use active-active VTEPs to establish a VXLAN tunnel with Leaf1. Deploy a bypass VXLAN tunnel between DCGW1 and DCGW2 to transmit traffic temporarily.

Table 4-15 VTEP plan

VXLAN Tunnel	Configuration Item	Setting
VXLAN tunnel between Leaf1 and DCGWs	Local VTEP address	Leaf1: 1.1.1.9
	Peer VTEP (active-active) address	DCGW1 & DCGW2: 10.10.10.10
Bypass VXLAN tunnel	Local VTEP address	DCGW1: 1.1.1.5
	Peer VTEP address	DCGW2: 1.1.1.6

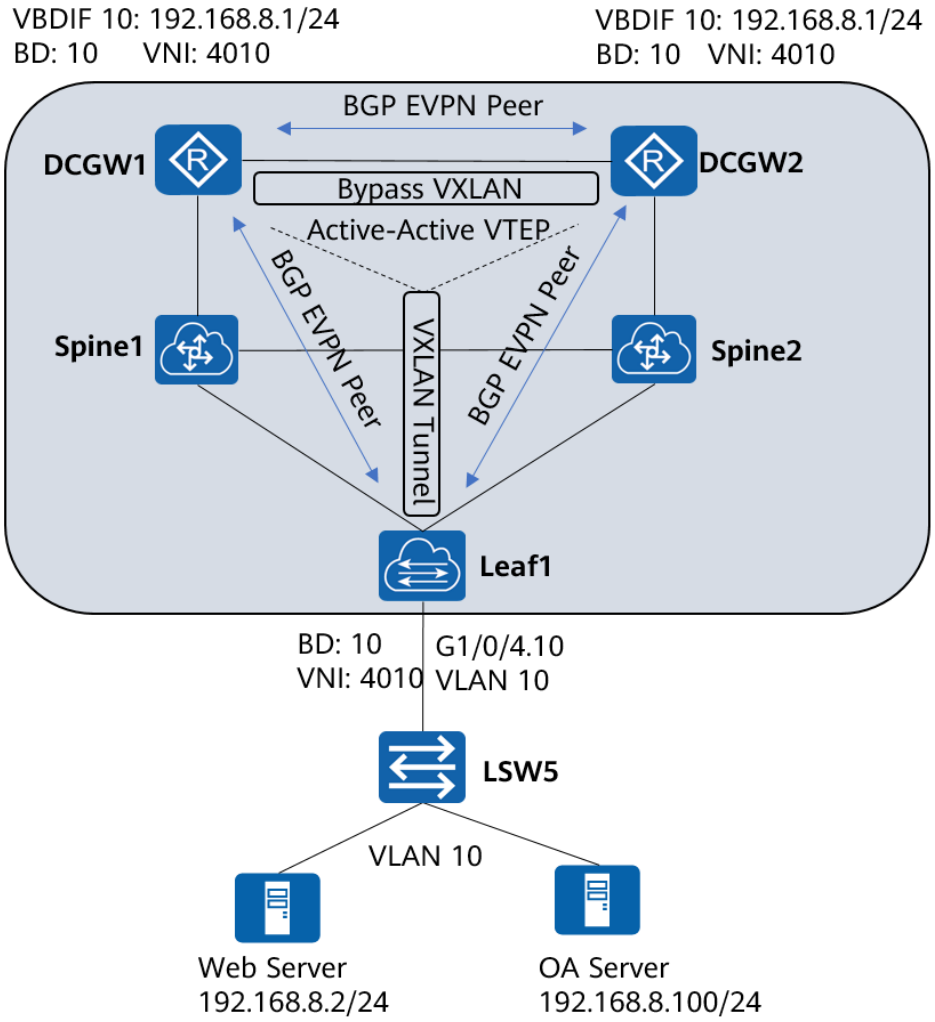
2. Configure a sub-interface on Leaf1 for VXLAN access. Configure DCGW1 and DCGW2 as active-active service gateways for the Web Server and OA Server. Synchronize ARP entries of the OA Server and Web Server between DCGWs to ensure that external traffic to these servers can be properly forwarded.

Table 4-16 Information for server access to the VXLAN

Configuration Module	Configuration Item	Setting
Server access to the VXLAN	Leaf1 access interface	G1/0/4.10
	VLAN to which the interface of Leaf1 is added	10
	BD	10
	VNI	4010
	OA Server IP address	192.168.8.100/24
	Web Server IP address	192.168.8.2/24
	OA & Web Server gateway	192.168.8.1

3. Bind the service server gateway created on DCGW1 and DCGW2 to VPNs. For details, see task 9.

Figure 4-11 VXLAN overlay network deployment of the DC



4.6.3 External Network Deployment

The DC accesses the external network through the DCGW1 and DCGW2. The DCGWs establish BGP peer relationships with PEs on the carrier's metropolitan area network (MAN) to transmit routes. The detailed planning is as follows:

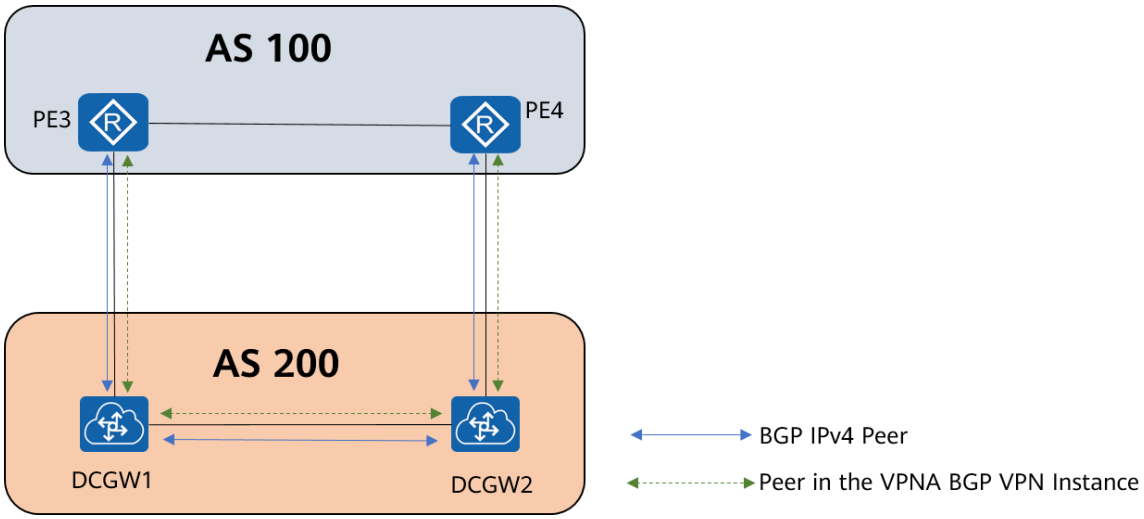
1. Establish BGP IPv4 unicast peer relationships between DCGW1 and PE3 and between DCGW2 and PE4 through main interfaces. Establish peer relationships between DCGW1 and PE3 and between DCGW2 and PE4 in the **VPNA** BGP VPN instance through sub-interfaces, and implement inter-AS interconnection in Option A mode. For details about the **VPNA** instance, see task 7.
2. Establish a BGP IPv4 unicast peer relationship between DCGW1 and DCGW2 through main interfaces, and establish a peer relationship in the **VPNA** BGP VPN instance through sub-interfaces.

3. Use BGP IPv4 unicast peers to transmit service routes of the Web Server, and use peers in the **VPNA** BGP VPN instance to transmit service routes of the OA Server.

Table 4-17 Plan of the parameters for the DC to connect to the external network

BGP Peer	Device	AS	BGP Peer Update Source	
			IPv4 Unicast	VPN Instance VPNA
DCGW1-DCGW2	DCGW1	200	Loopback 0	ETH1/0/0.56
	DCGW2	200	Loopback 0	ETH1/0/0.56
DCGW1-PE3	DCGW1	200	ETH1/0/3	ETH1/0/3.35
	PE3	100	G0/0/3	G0/0/3.35
DCGW2-PE4	DCGW2	200	ETH1/0/3	ETH1/0/3.46
	PE4	100	G0/0/3	G0/0/3.46

Figure 4-12 External network deployment of the DC



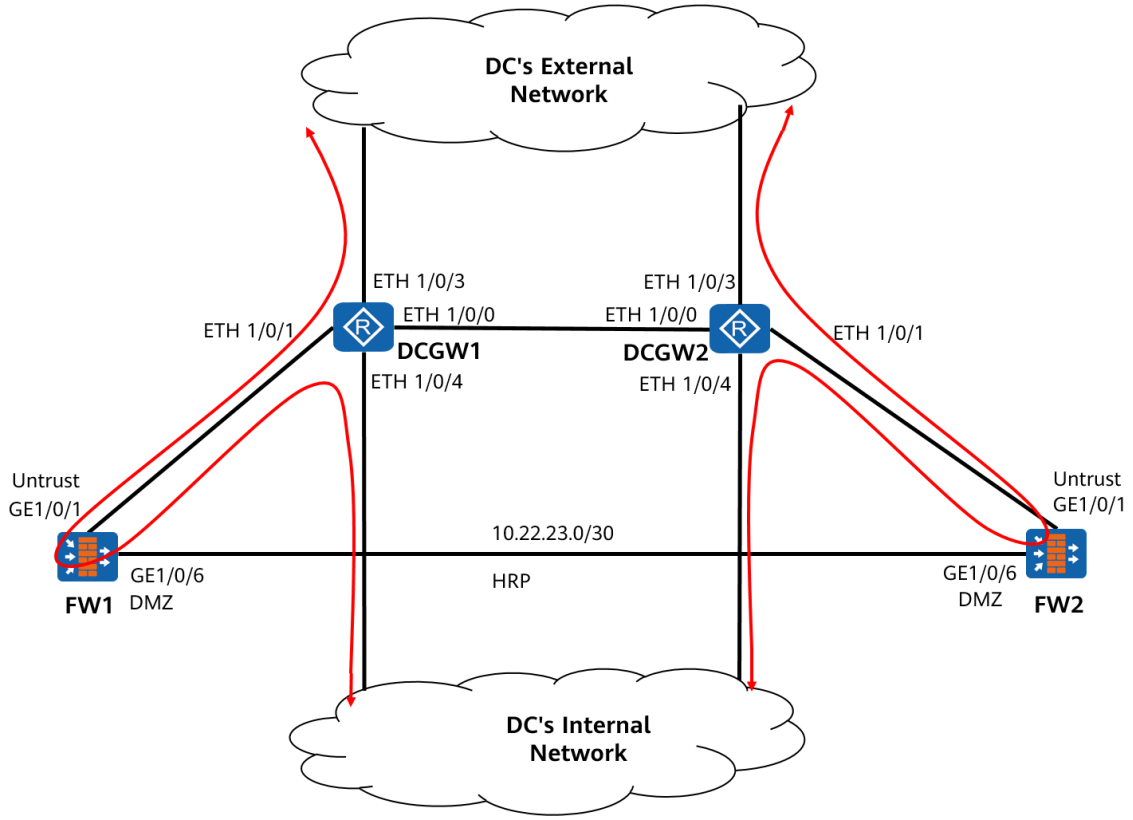
4.6.4 Hot Standby Firewall Deployment

FW1 and FW2 working in hot standby mode are connected to the DCGWs in off-path mode to ensure data center network security. The two firewalls work in load balancing mode. Under normal circumstances, both FW1 and FW2 forward traffic. If one firewall fails, the other firewall forwards all service traffic to ensure service continuity. The detailed planning is as follows:

1. On FW1 and FW2, deploy a VGMP group to monitor the service main interface G1/0/1, specify G1/0/6 as the heartbeat interface, and enable hot standby.

2. Configure the firewalls to work in load balancing mode. In this mode, both firewalls forward traffic. Deploy the quick session backup function on the firewalls.

Figure 4-13 Hot standby firewall deployment in the DC



4.6.5 Virtual System Deployment on Firewalls

To manage the OA and web service flows on firewalls, create virtual systems in the firewall hot standby system. The detailed planning is as follows:

1. Enable the virtual system function in the firewall hot standby system and create VSYSs **Web** and **OA**.
2. Allocate resource classes to the created VSYSs and create administrator accounts for the VSYSs.

Table 4-18 Virtual system plan (1)

Virtual System	OA	Web
Resource Allocation	Resources are shared with the public firewall.	Name: r1
		Guaranteed number of sessions: 100
		Maximum number of sessions: 200
		Number of users: 10
		Number of policies: 100
		Assured bandwidth in the outbound direction: 2 Mbit/s
Administrator Account Prefix	Admin1	Admin2
Administrator Account Password	Huawei@123	Huawei@123

Table 4-19 Virtual system plan (2)

Device	**Interface**	**Virtual System**	**Security Zone**
FW1	GigabitEthernet 1/0/1	Public	Untrust
	Virtual-IF 0		Trust
	GigabitEthernet 1/0/1.20	OA	Trust
	GigabitEthernet 1/0/1.30		Untrust
	GigabitEthernet 1/0/1.10	Web	Trust
	Virtual-IF 1		Untrust
FW2	GigabitEthernet 1/0/1	Public	Untrust
	Virtual-IF 0		Trust
	GigabitEthernet 1/0/1.20	OA	Trust
	GigabitEthernet 1/0/1.30		Untrust
	GigabitEthernet 1/0/1.10	Web	Trust
	Virtual-IF 1		Untrust

4.6.6 IPS Deployment on Firewalls

To protect the Web Server from attacks from the Internet, enable the blacklist and intrusion prevention system (IPS) functions on firewalls. The configuration requirements are as follows:

1. As the host at 200.200.200.200 on the Internet initiates attacks, configure the blacklist function on the public firewall to block this IP address.
2. Configure the IPS function on the enterprise egress firewall, set the attack object to the intranet server, and apply the IPS profile to the interzone security policy. The data planning is as follows (no verification is required after the configuration is complete).

Table 4-20 IPS profile data plan

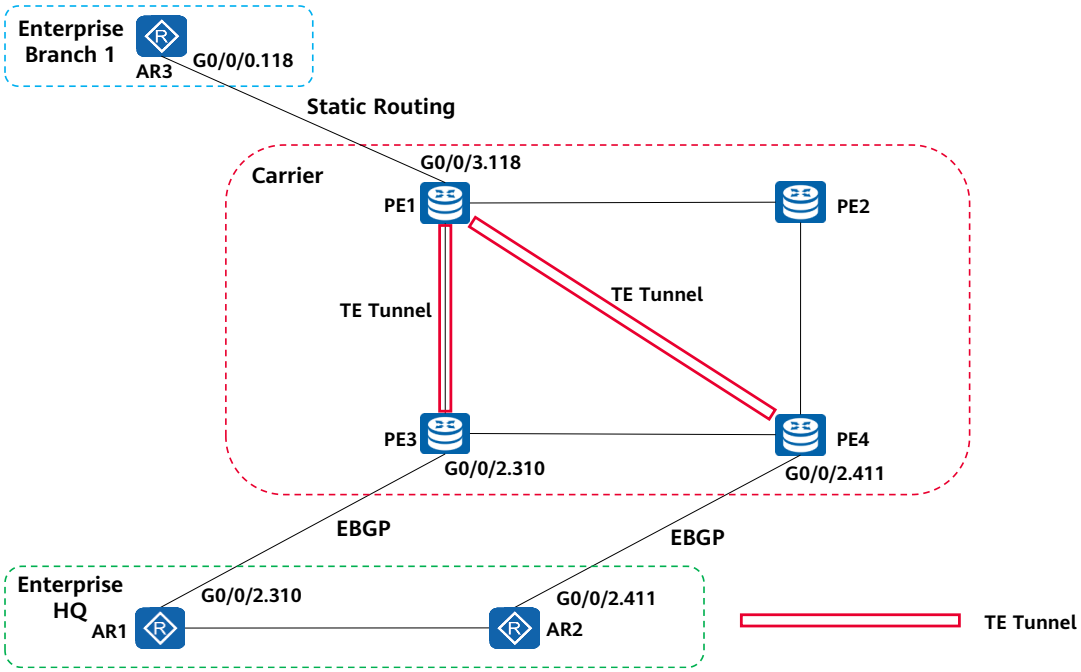
Configuration Item	Setting
IPS profile name	Profile_ips_server
Signature filter	filter_web
Object	Server
Severity	High
Protocol	HTTP

4.7 Task 7: Communication Between the Enterprise HQ and Enterprise Branch 1 Through MPLS VPN

4.7.1 MPLS VPN Deployment

The enterprise HQ and enterprise branch 1 communicate with each other at Layer 3 through the carrier's MPLS BGP L3VPN private line network, which includes the wired service network segment and wireless employee network segment between the HQ and branch 1. The wired service network segment also requires IPv4/IPv6 dual-stack communication.

Figure 4-14 VPN communication between the enterprise HQ and branch 1



The configuration requirements are as follows:

1. Connect AR1 and AR2 at the HQ to PE3 and PE4, respectively, and connect AR3 to PE1. Configure PEs to exchange VPNv4 and VPNv6 service routes through RRs. The following table lists the configuration requirements for VPN instance names, RDs, RTs, and service interfaces.

Table 4-21 VPN configuration requirements

Configuration Item	Setting
VPN instance name	VPNA
RD	This item needs to be planned as required.
RT	This item needs to be planned as required.
PE service access interface	PE1: G0/0/3.118
	PE3: G0/0/2.310
	PE4: G0/0/2.411
CE service access interface	AR3: G0/0/0.118
	AR1: G0/0/2.310
	AR2: G0/0/2.411
Transport tunnel	Primary RSVP-TE tunnel and backup LDP tunnel

Configuration Item	Setting
Protocol running between PEs and CEs	Between PE1 and AR3: specific static routes
	Between PE3 and AR1 and between PE4 and AR2: EBGP

2. Run MPLS RSVP-TE between PEs to provide the primary tunnels for carrying L3VPN IPv4 and IPv6 services. The TE tunnel configuration requirements are as follows:

Table 4-22 TE configuration requirements

Configuration Item	Setting
Information advertisement	IS-IS TE
Path computation	CSPF
Path establishment	RSVP-TE
Traffic forwarding mode	Tunnel policy
Tunnel interface	Tunnel from PE1 to PE3: Tunnel0/0/13
	Tunnel from PE1 to PE4: Tunnel0/0/14
	Tunnel from PE3 to PE1: Tunnel0/0/31
	Tunnel from PE4 to PE1: Tunnel0/0/41
Tunnel interface address	IP address of Loopback0
Explicit path	Loose explicit path, which is used to restrict physical interfaces that are used
Tunnel protection	TE hot-standby

To improve TE tunnel reliability, deploy TE hot-standby for hot standby protection. The following table lists the constraints on the primary and backup LSPs of TE hot-standby.

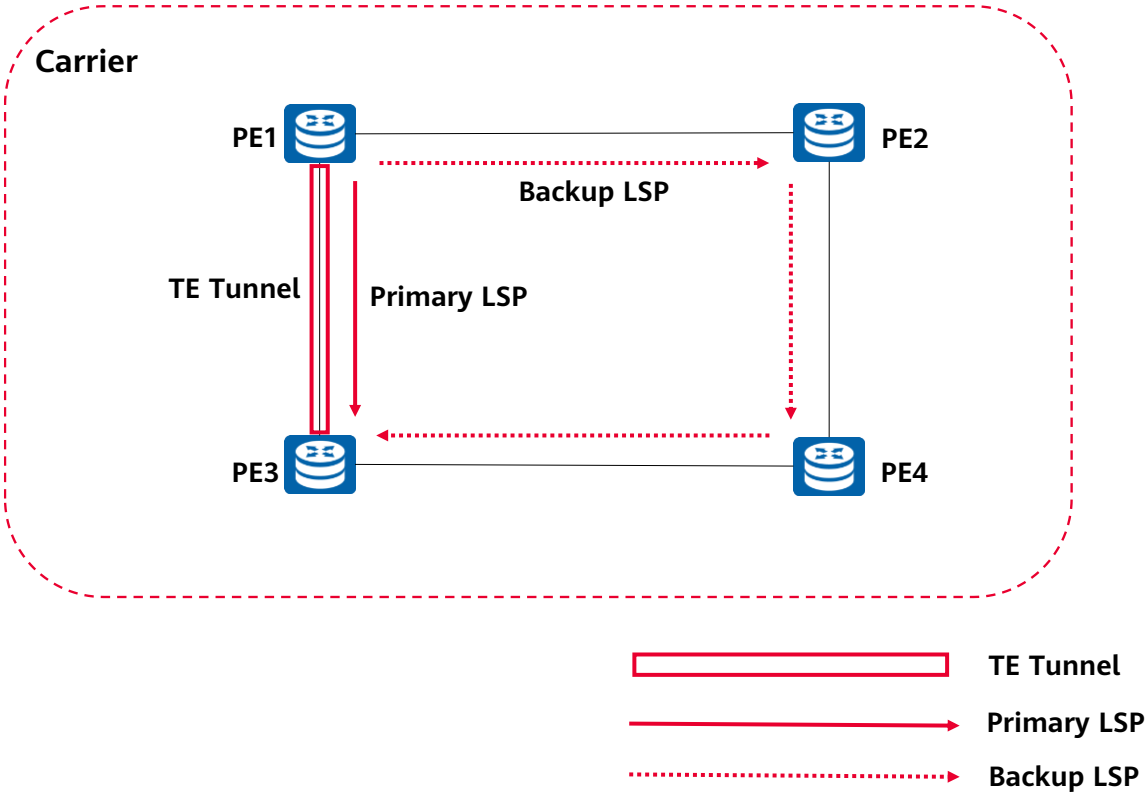
Table 4-23 TE tunnel information

Tunnel Interface	Source	Destination	Primary LSP Name	Primary LSP	Backup LSP Name	Backup LSP
Tunnel0/0/13	PE1	PE3	to-PE3-main	PE1-PE3	to-PE3-backup	PE1-PE2-PE4-PE3
Tunnel0/0/14	PE1	PE4	to-PE4-main	PE1-PE2-PE4	to-PE4-backup	PE1-PE3-PE4

Tunnel Interface	Source	Destination	Primary LSP Name	Primary LSP	Backup LSP Name	Backup LSP
Tunnel0/0/31	PE3	PE1	to-PE1-main	PE3-PE1	to-PE1-backup	PE3-PE4-PE2-PE1
Tunnel0/0/41	PE4	PE1	to-PE1-main	PE4-PE2-PE1	to-PE1-backup	PE4-PE3-PE1

The following takes the tunnel from PE1 to PE3 as an example. The following figure shows information about the primary and backup LSPs.

Figure 4-15 Primary and backup LSPs of the tunnel from PE1 to PE3



3. To speed up fault detection on the primary LSP, configure static BFD for TE-LSP and set the BFD detection interval to 1500 ms (500 ms x 3) on related devices. When BFD detects a fault, TE hot-standby is triggered to perform a primary/backup switchover. When the primary LSP recovers, traffic can be switched back to the primary LSP from the backup LSP. To prevent frequent switchovers caused by an unstable primary LSP, set the switchback delay to 20 seconds.
4. To ensure tunnel reliability, deploy LDP to provide backup tunnels in addition to MPLS TE tunnels. When an MPLS TE tunnel fails, service traffic can be automatically switched to the backup LDP tunnel.

5. Run EBGP between the enterprise HQ and the carrier network to transmit routes, and set the AS number of the enterprise HQ network to AS300 and the AS number of the carrier network to AS100. Run EBGP between AR1 and PE3, and between AR2 and PE4, and advertise the IPv4 and IPv6 service network segments of the HQ to the PEs using the **network** command.
6. Configure static routes between branch 1 and the carrier network to implement route interworking. On AR3, configure a specific static route to the HQ network segment. On PE1, configure a specific static route to branch 1.
7. Configure PE3 and PE4 to add the MED attribute to VPNv4 and VPNv6 routes to be transmitted to PE1 through the RR, and ensure that PE1 preferentially selects the routes advertised by PE3 and that these routes take over the routes advertised by PE4. Configure PE3 and PE4 to use the IP prefix list to filter out specific routes to the HQ. Set the MED value of the routes on PE3 to 100, and that of the routes on PE4 to 150.
8. To implement fast convergence at the VPN service layer, configure VPN FRR on PE1. This ensures that when PE3 fails, PE1 can quickly switch traffic to the backup next hop PE4, without having to wait for a long time for route convergence. In addition, set a proper next-hop weight to avoid traffic loss when traffic is switched to PE4 after PE3 fails.
9. Configure BFD for TE tunnel and set the detection period to 2400 ms (800 ms x 3). When the BFD status is down, VPN FRR can be triggered immediately.

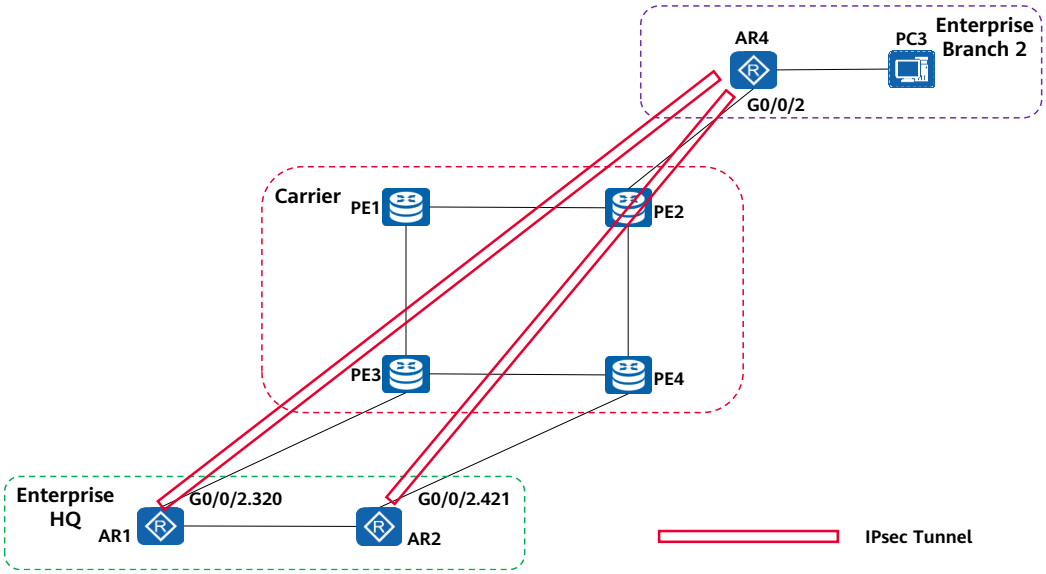
4.8 Task 8: Enterprise Branch 2 Accessing Enterprise Internal Resources Through IPsec

4.8.1 IPsec Deployment

The egress router AR4 of enterprise branch 2 is connected to the Internet through PE2 of the carrier network. An IPsec tunnel is deployed between branch 2 and the enterprise HQ across the Internet to implement secure and reliable access to the enterprise's IPv4 intranet. After the data traffic of branch 2 reaches the HQ through the IPsec tunnel, branch 2 can access internal resources at the HQ and branch 1 as well as access the OA server in the DC.

Note: To enable branch 2 to access the OA server in the DC, you need to perform Task 9. After task 9 is complete, branch 2 can access the OA server in the DC.

Figure 4-16 Establishing IPsec tunnels between branch 2 and the HQ



Deploy IPsec tunnels between AR4 and AR1, and between AR4 and AR2. The configuration requirements are as follows:

1. Configure an advanced ACL numbered 3102 on AR4 and define the data flows to be protected in the ACL to allow branch 2 to securely and reliably access the HQ, branch 1, and OA server in the DC. Configure ACL 3102 on AR1 and AR2 to allow branch 2 to access enterprise intranet resources.
2. Create ISAKMP IPsec policies on AR1 and AR2 and create an ISAKMP IPsec policy group on AR4 to ensure that the priority of the IPsec policy for the IPsec tunnel from AR4 to AR1 is higher than the priority of the IPsec policy for the IPsec tunnel from AR4 to AR2. After the IPsec policies are configured, apply them to the corresponding interfaces (as shown in the following table) of AR1, AR2, and AR4 to enable IPsec protection on the interfaces.

Table 4-24 IPsec policies

Device	IPsec Policy Name	Interface to Which an IPsec Policy Is Applied
AR4	policy1	G0/0/2
AR1	policy1	G0/0/2.320
AR2	policy1	G0/0/2.421

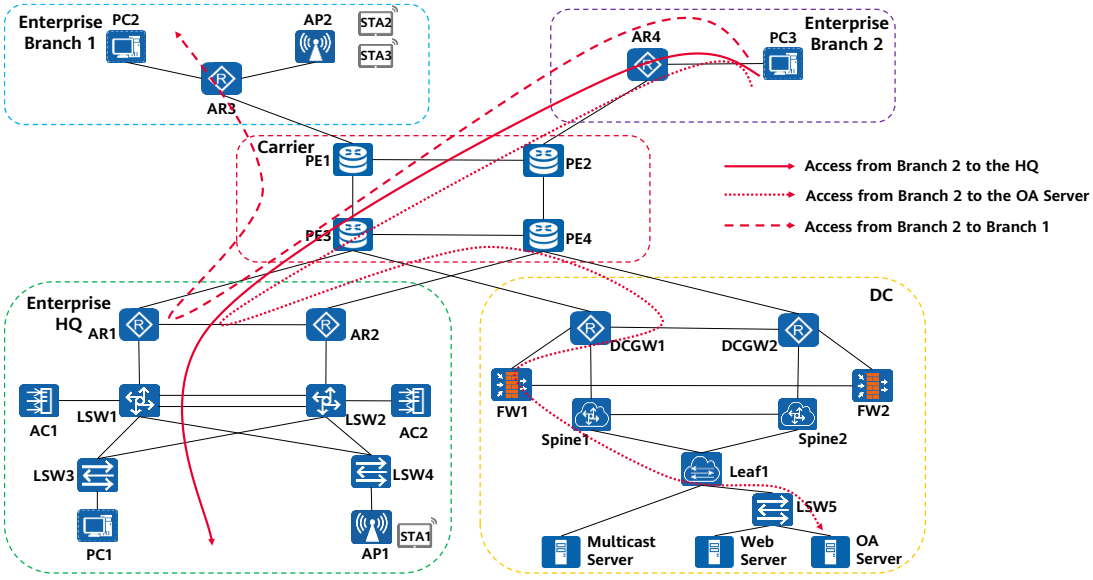
3. The following table lists the IPsec tunnel configuration requirements.

Table 4-25 IPsec configuration requirements

Configuration	Configuration Item	Setting
IKE configuration	IKE authentication method	pre-share
	IKE authentication algorithm	sha1
	IKE encryption algorithm	aes-cbc-128
	IKE key exchange mode	DH Group14
	PRF algorithm	hmac-sha1
	IKE pre-shared key	Huawei@123
	IKE version	V1
IPsec configuration	IPsec proposal name	pro1
	IPsec encapsulation mode	Tunnel mode
	IPsec security protocol	ESP
	ESP authentication algorithm	sha2-256
	ESP authentication algorithm	aes-192

4. After the preceding configurations are complete, enterprise branch 2 can access the HQ, branch 1, and the OA server in the DC. (Access to the OA server in the DC is allowed after Task 9 is complete.) The following figure shows the traffic diagram.

Figure 4-17 Access from branch 2 to intranet resources



4.9 Task 9: Enabling Intranet Users to Access the OA Server and Internet Users to Access the Web Server

The OA Server at the DC can be accessed only from the enterprise intranet. The enterprise HQ and branch 1 access the OA Server through the carrier's MPLS VPN. Branch 2 first accesses the HQ through the IPsec tunnel established over the Internet, and then accesses the OA Server.

The Web Server at the DC is used for the enterprise's external communication. Internet users can directly access the Web Server through the Internet. Intranet users can access the Web Server through both the Internet and intranet.

The following figures show the traffic accessing the OA Server and Web Server.

Figure 4-18 Accessing the OA Server from the enterprise intranet

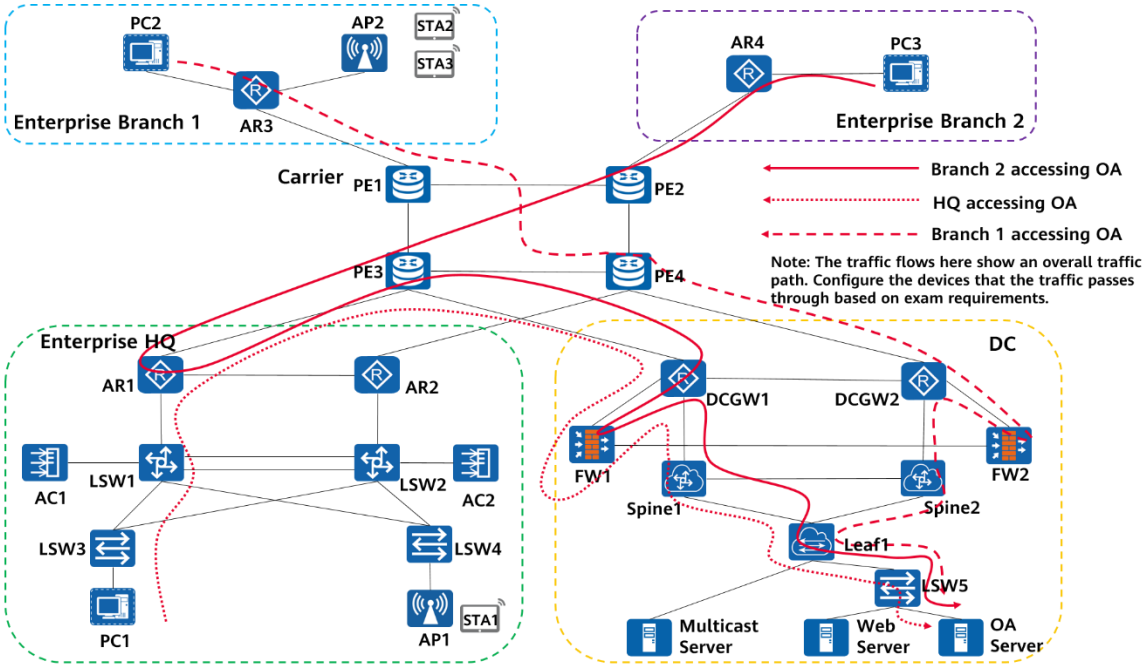
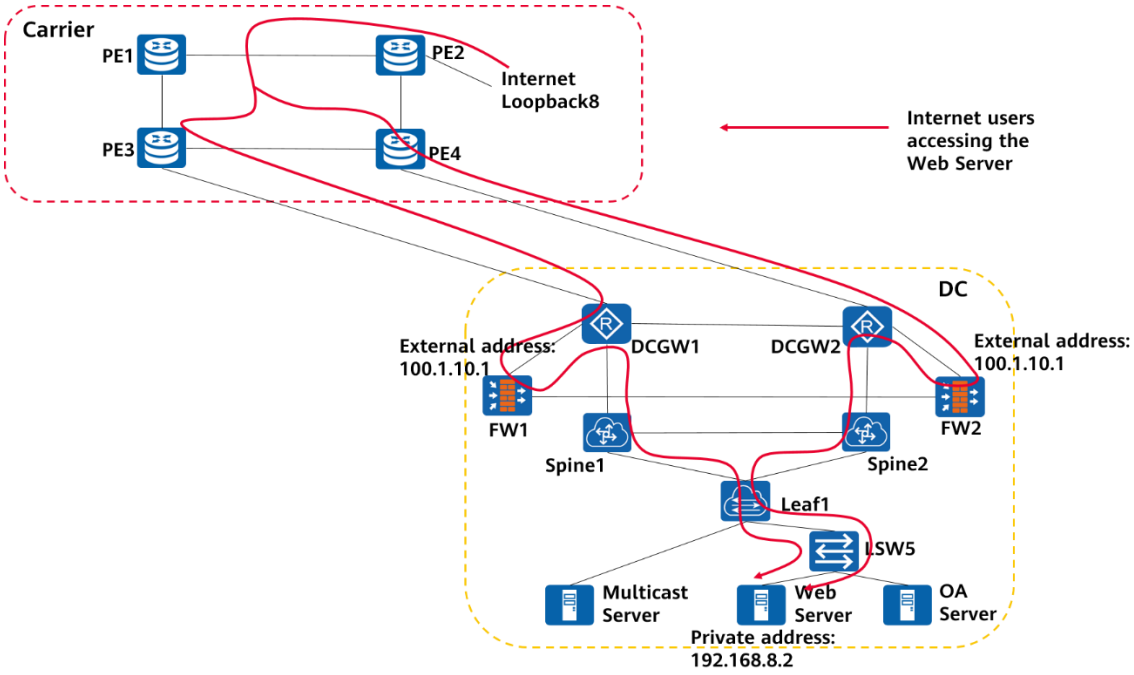


Figure 4-19 Internet users accessing the Web Server



4.9.1 NAT Deployment on the Firewalls at the DC

To ensure that the Web Server at the DC can be accessed from the Internet, NAT Server must be deployed in the public system. The requirements are as follows:

Table 4-26 NAT Server data plan for firewalls at the DC

Server	Configuration Item	Setting
Web Server	NAT Server	Web
	Public IP address	100.1.10.1
	Private IP address	192.168.8.2
	Translation mode	NAT server

4.9.2 DC Service Traffic Planning

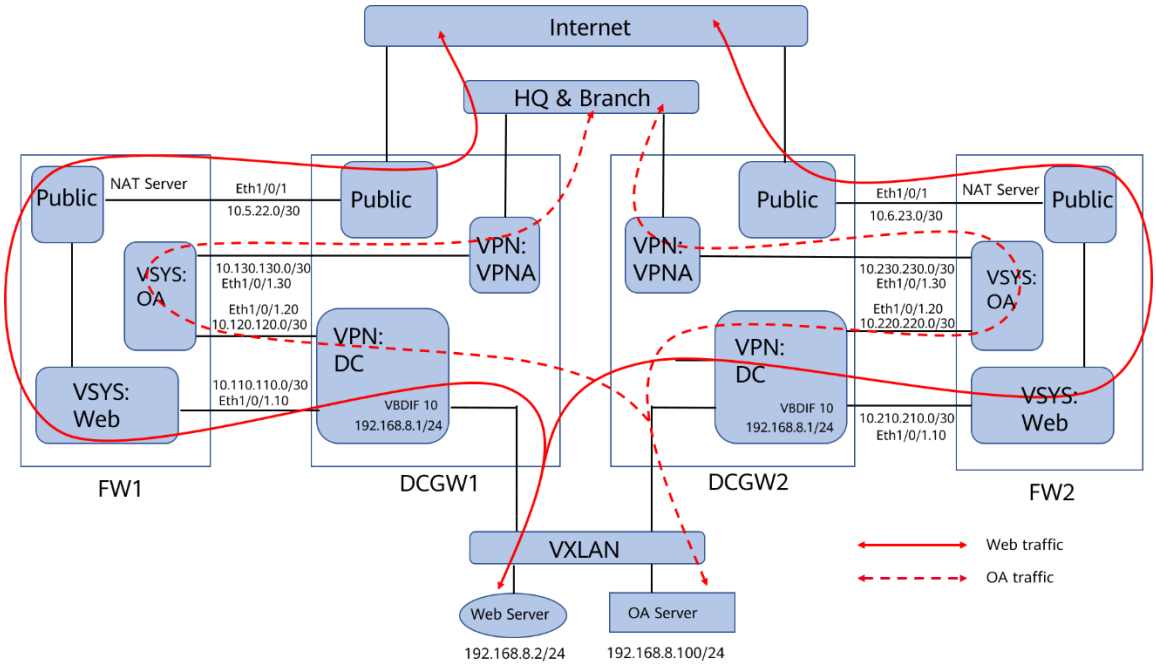
When traffic from the enterprise intranet to the OA Server and traffic from Internet users to the Web Server pass through the DCGWs, the DCGWs need to divert the traffic to the firewalls that are deployed in off-path mode for security detection. The traffic diversion mode is static routing. The specific requirements are as follows:

1. Deploy virtual systems on the firewalls that work in hot standby mode, and configure Virtual-if interfaces to implement traffic interworking between the Web vSYS and the public system.
2. Web service traffic: As shown in Figure 4-20, when an Internet user accesses the Web Server using a public IP address, the DCGWs forward the traffic to the firewalls' public systems through static routes. After translation by NAT Server, the traffic is diverted to the Web vSYSs for forwarding. The Web vSYSs forward the traffic to the DC VPNs on the DCGWs through static routes. The VBDIF 10 interfaces of the DCGWs are advertised in the DC VPNs and forward the traffic to the Web Server.
3. OA service traffic: As shown in Figure 4-20, when the enterprise HQ and branches access the OA Server through the carrier's MPLS VPN, the DCGWs forward the traffic to the firewalls' OA vSYSs through static routes in VPNA. The OA vSYSs filter the traffic based on security policies and forward the traffic to the DC VPNs on the DCGWs through static routes. The VBDIF 10 interfaces of the DCGWs are advertised in the DC VPNs and forward the traffic to the OA Server.
4. Deploy a traffic-filter on the interface connecting LSW5 to the Web Server to prevent Internet users from directly accessing the OA Server through the Web Server.
5. Deploy a security policy in each OA vSYS to allow only the traffic from the 192.168.0.0/16 network segment to access the OA Server.

Table 4-27 VPN data plan for DCGWs at the DC

VPN	RD	Import RT	Export RT
VPNA	1:2	1:2	
DC	1:3	1:3	

Figure 4-20 Internal traffic at the DC



4.10 Task 10: Multicast Service

4.10.1 Multicast Service Deployment

To satisfy an enterprise's video conferencing and online training needs, the enterprise has a multicast server hosted in the carrier's DC, with the multicast server directly connected to Leaf1. Wired terminals in the enterprise HQ, branch 1, and branch 2 join multicast groups to obtain multicast streams.

Note: Multicast services are directly carried over the Internet. IP reachability is established to ensure normal use of multicast services. Multicast traffic does not enter the MPLS VPN or IPsec tunnel.

The specific configuration requirements are as follows:

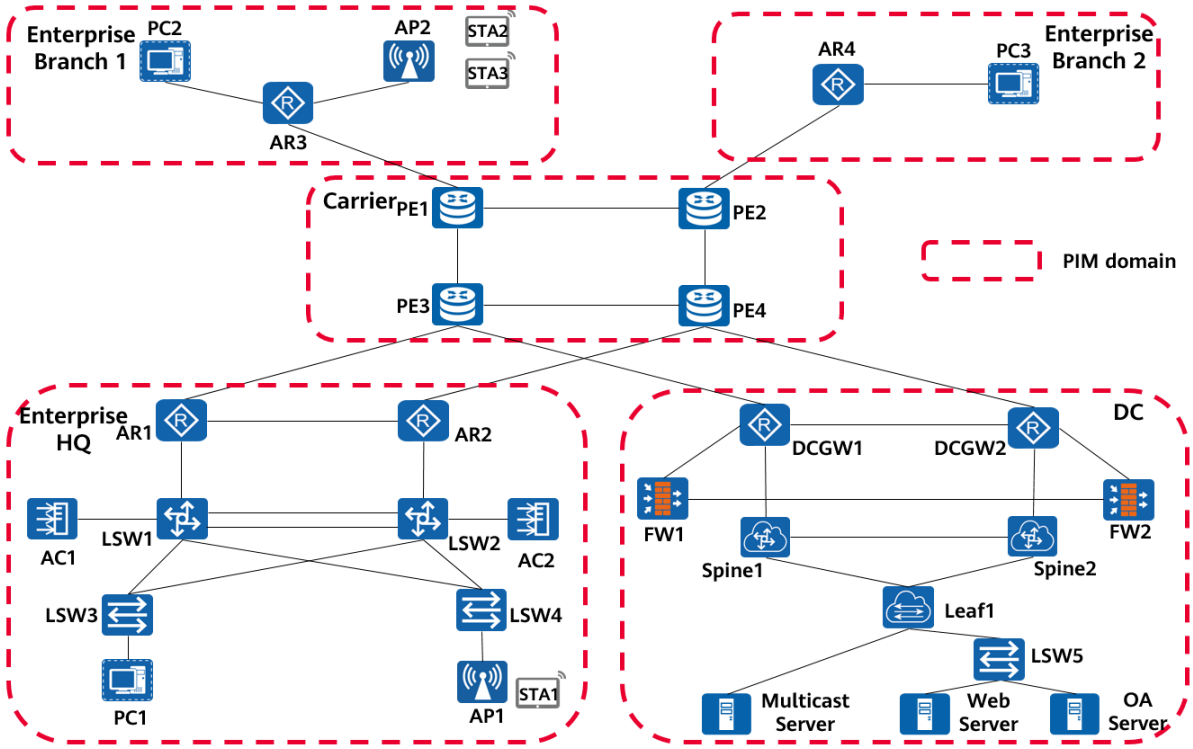
Table 4-28 Multicast parameters

Configuration Item	Setting
Multicast routing protocol	PIM-SM
IGMP	IGMPv2
Multicast source	Multicast Server
Multicast source IP address	100.2.10.2/24
Multicast source gateway	100.2.10.1

Configuration Item	Setting
Multicast group	225.0.0.5
Multicast receivers	PC1 (HQ), PC2 (branch 1), and PC3 (branch 2)

1. Enable multicast routing on network-wide devices and deploy PIM-SM as the multicast routing protocol to set up a multicast distribution tree. Divide the entire network into several PIM domains and configure a BSR boundary on the edge device of each PIM domain, so as to prevent each PIM domain from sending BSR messages to and receiving BSR messages from other PIM domains.

Figure 4-21 PIM domain division



2. Deploy the multicast server, and configure the multicast server gateway on Leaf1. Multicast traffic is carried over the underlay OSPF network without entering the VXLAN network or passing through firewalls. Configure the DCGWs to advertise the network segment where the multicast server resides to the carrier's MAN.
3. Deploy dynamic RP election in each PIM-SM domain. In the DC, enterprise HQ, and carrier MAN, deploy PIM Anycast-RP to ensure RP reliability and load balancing of multicast traffic.

Table 4-29 RP configuration requirements

Multicast Domain	RP	Anycast-RP (Yes/No)	C-BSR/C-RP	RP Address
DC	DCGW1/DCGW2	Yes	Loopback56	1.1.1.56
HQ	AR1/AR2	Yes	Loopback1011	1.1.10.11
Branch 1	AR3	No	Loopback0	1.1.1.18
Branch 2	AR4	No	Loopback0	1.1.1.21
Carrier	PE3/PE4	Yes	Loopback34	1.1.1.34

4. To implement information sharing between PIM-SM domains, set up MSDP peer relationships between PIM-SM domains. MSDP peers exchange SA messages to transmit multicast source and group information. Set up MSDP peer relationships between related devices using physical interfaces.
5. To prevent MSDP RPF check failures, configure static RPF peers on related devices. To prevent MSDP SA messages from being flooded among MSDP peers, configure mesh groups on related devices.
6. On DCGW1 and DCGW2, specify group 225.0.0.5 as the multicast group that the RP serves.
7. Configure an IGMP group policy on devices in each PIM-SM domain to set the range of multicast groups that hosts can join to 225.0.0.0-225.0.0.255.
8. To speed up network convergence, configure IGMP prompt leave, so that an interface can delete the corresponding IGMP entry as soon as it receives a Leave message, without sending a last-member Query message.
9. On related devices in the HQ, branch 1, and branch 2, configure a static multicast group with the group address 225.0.0.5.
10. To forward and control multicast data at the data link layer, enable IGMP snooping on related devices in the enterprise HQ.
11. After the preceding configurations are complete, wired terminals in the enterprise HQ, branch 1, and branch 2 should be able to receive data flows from the multicast server in the DC, as shown in the following figure.

Note: In this exam, the multicast server does not send multicast video traffic. Traffic distribution in the figure below is for reference only.

Figure 4-22 Multicast traffic distribution