2022-2023 Huawei ICT Competition

Regional Stage

Issue: 1.0

HUAWEI

Huawei Technologies CO., LTD.

Contents

1 Background

The competition simulates the scenario where a large enterprise network connects to the data center through the WAN.

To meet network redundancy and load balancing requirements, MSTP is deployed on the enterprise network and firewalls are deployed in hot standby mode to transmit web services and Internet access services. In addition, WLAN devices need to be deployed on the enterprise network to provide Internet access for employees using wireless terminals.

When enterprise networks and data center networks are being built with abundant network resources, they are also facing severe security problems. To reduce security risks, next-generation firewalls (NGFWs) can be deployed at the egress of enterprise networks and data center networks to implement secure and efficient network management.

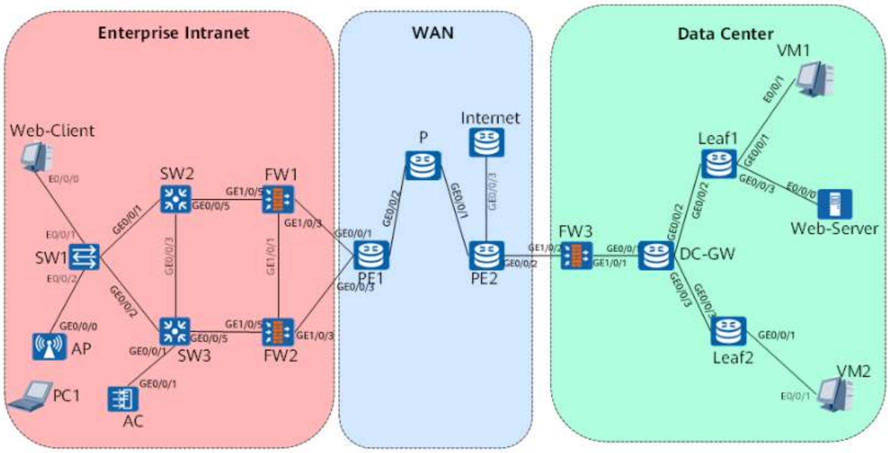
The private cloud of the enterprise is deployed in the equipment room of the HQ data center. Various service systems of the enterprise are deployed on its private cloud, and the web server (Web-Server) on which the enterprise's OA system resides is deployed in the HQ data center. Branches of the enterprise need to access Web-Server in the HQ data center through MPLS VPN. For security purposes, the private IP address of Web-Server is not advertised to the WAN. Instead, a public IP address, 100.1.1.1, is used for access to Web-Server. A web client (Web-Client) can access Web-Server only when the destination address of the traffic from Web-Client to Web-Server is translated into the private IP address of Web-Server on FW3 in the data center.

To implement mutual access between service VMs (VM1 and VM2) in different subnets in the HQ data center, GRE tunneling must be deployed in the data center to establish a Layer 3 channel between VM1 and VM2.

The WAN connects the enterprise intranet to the HQ data center. MPLS VPN is deployed on the WAN to deliver the Internet leased line function, thereby isolating services on the WAN.

2 Network Track Exam

Figure 2-1 IP network topology



The following devices are used in the lab environment:

- Two S5700 switches (SW2 and SW3)
- One S3700 switch (SW1)
- Three USG6000V firewalls (FW1 to FW3)
- Seven routers (PE1, PE2, P, Internet, DC-GW, Leaf1, and Leaf2)
- One AC6605 (AC)
- One AP6050 (AP)
- One WLAN terminal (PC)
- One web server (Web-Server)
- One web client (Web-Client)
- Two VMs (VM1 and VM2)

Table 2-1 Device login information

Device Name	Password
Firewall	huawei123

3.2 Exam Paper

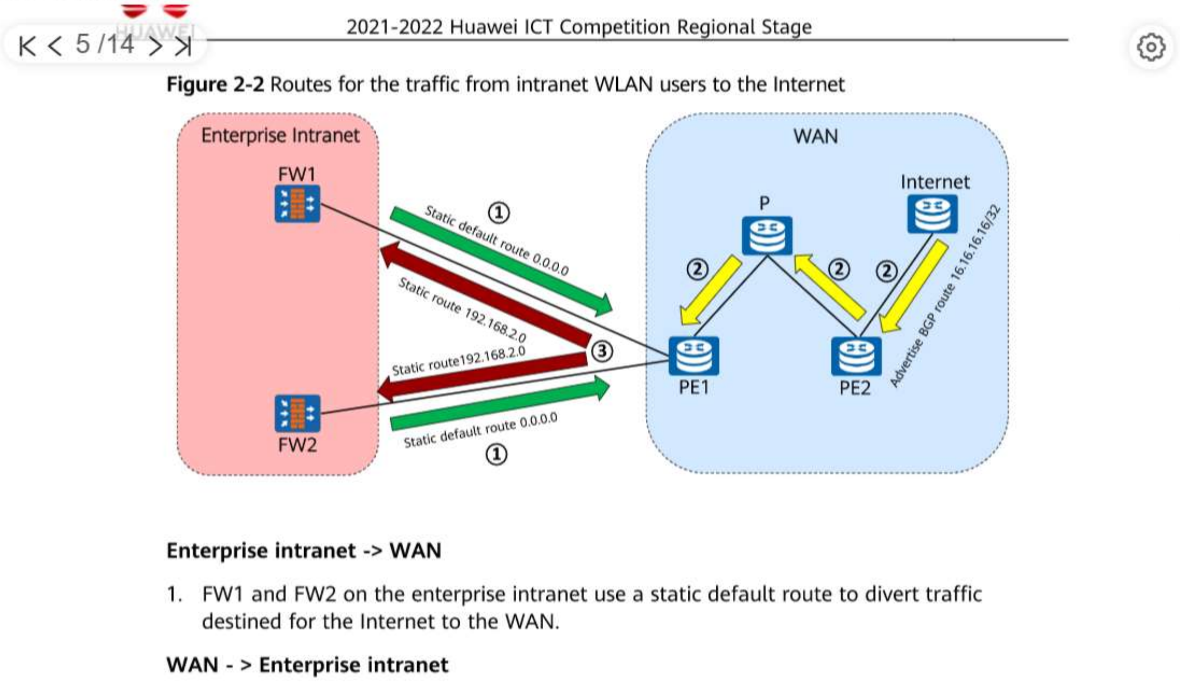


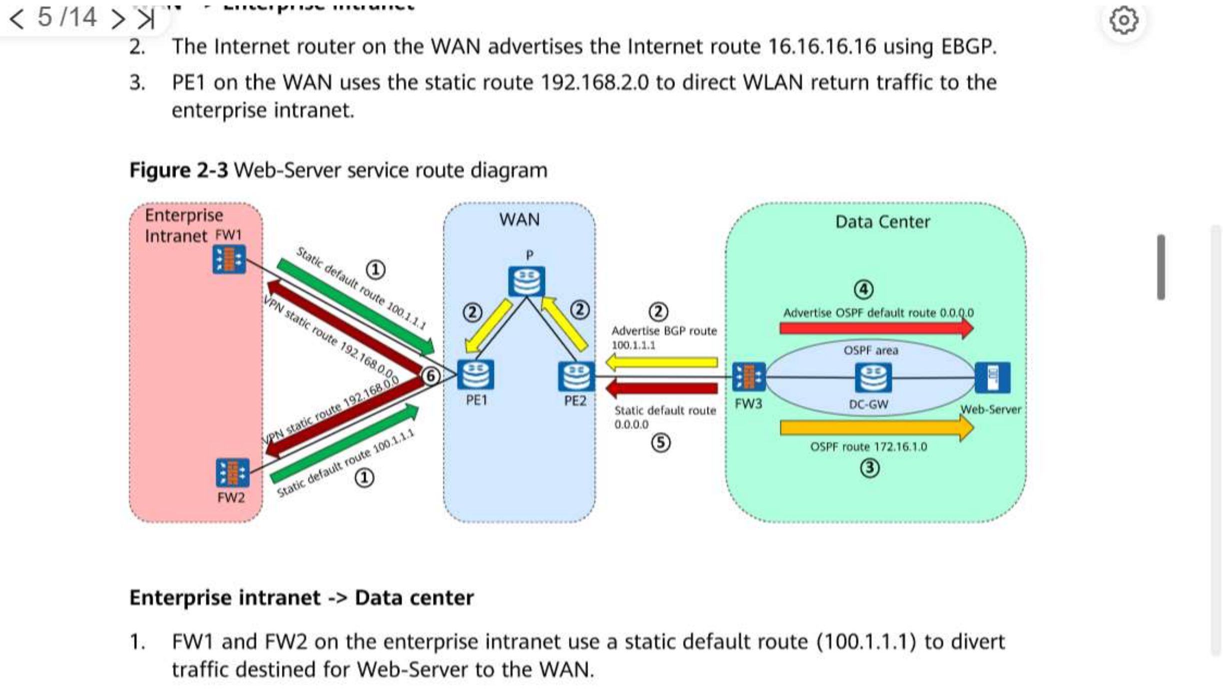
Figure 2-2 Routes for the traffic from intranet WLAN users to the Internet

Enterprise Intranet
FW1
FW2
WAN
P
Internet
PE1
PE2
① Static default route 0.0.0.0
Static route 192.168.2.0
③
Static route192.168.2.0
① Static default route 0.0.0.0
②
②
②
Advertise BGP route 16.16.16.16/32

Enterprise intranet -> WAN

1. FW1 and FW2 on the enterprise intranet use a static default route to divert traffic destined for the Internet to the WAN.

WAN - > Enterprise intranet



2. The Internet router on the WAN advertises the Internet route 16.16.16.16 using EBGP.
3. PE1 on the WAN uses the static route 192.168.2.0 to direct WLAN return traffic to the enterprise intranet.

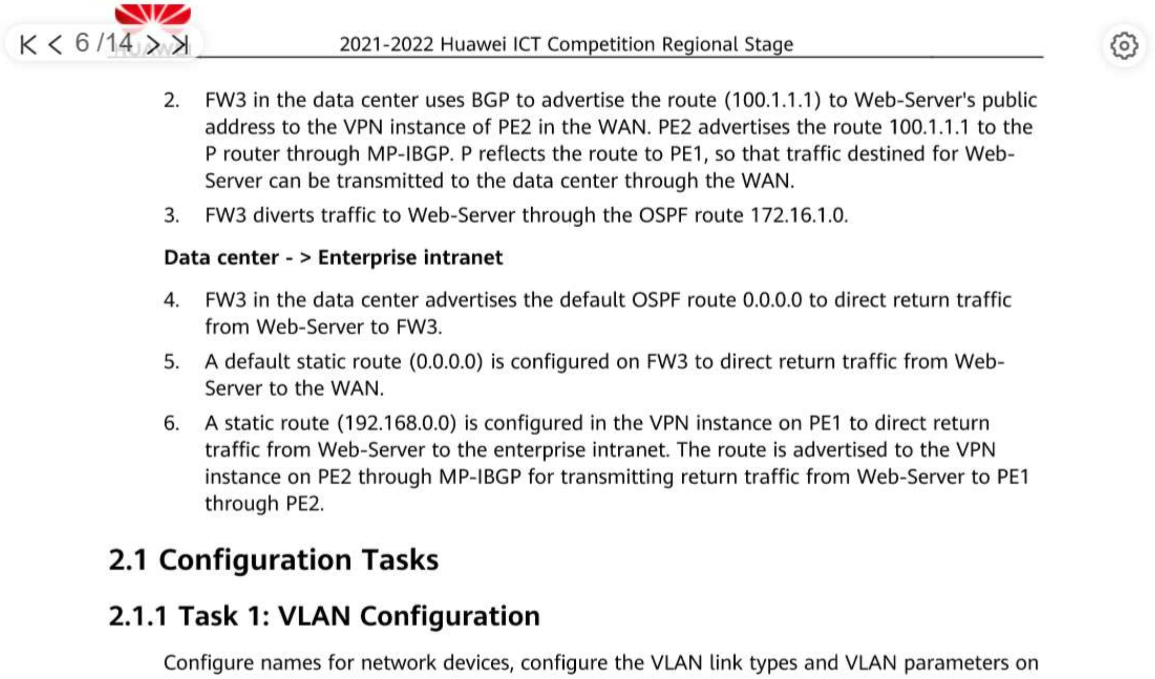
Figure 2-3 Web-Server service route diagram

Enterprise Intranet
FW1
FW2
① Static default route 100.1.1.1
VPN static route 192.168.0.0
⑥
VPN static route 192.168.0.0
① Static default route 100.1.1.1
WAN
P
②
②
PE1
PE2
② Advertise BGP route 100.1.1.1
Static default route 0.0.0.0 ⑤
Data Center
④ Advertise OSPF default route 0.0.0.0
OSPF area
FW3
DC-GW
Web-Server
OSPF route 172.16.1.0 ③

Enterprise intranet -> Data center

1. FW1 and FW2 on the enterprise intranet use a static default route (100.1.1.1) to divert traffic destined for Web-Server to the WAN.

3.2 Exam Paper



2. FW3 in the data center uses BGP to advertise the route (100.1.1.1) to Web-Server's public address to the VPN instance of PE2 in the WAN. PE2 advertises the route 100.1.1.1 to the P router through MP-IBGP. P reflects the route to PE1, so that traffic destined for Web-Server can be transmitted to the data center through the WAN.
3. FW3 diverts traffic to Web-Server through the OSPF route 172.16.1.0.

Data center - > Enterprise intranet

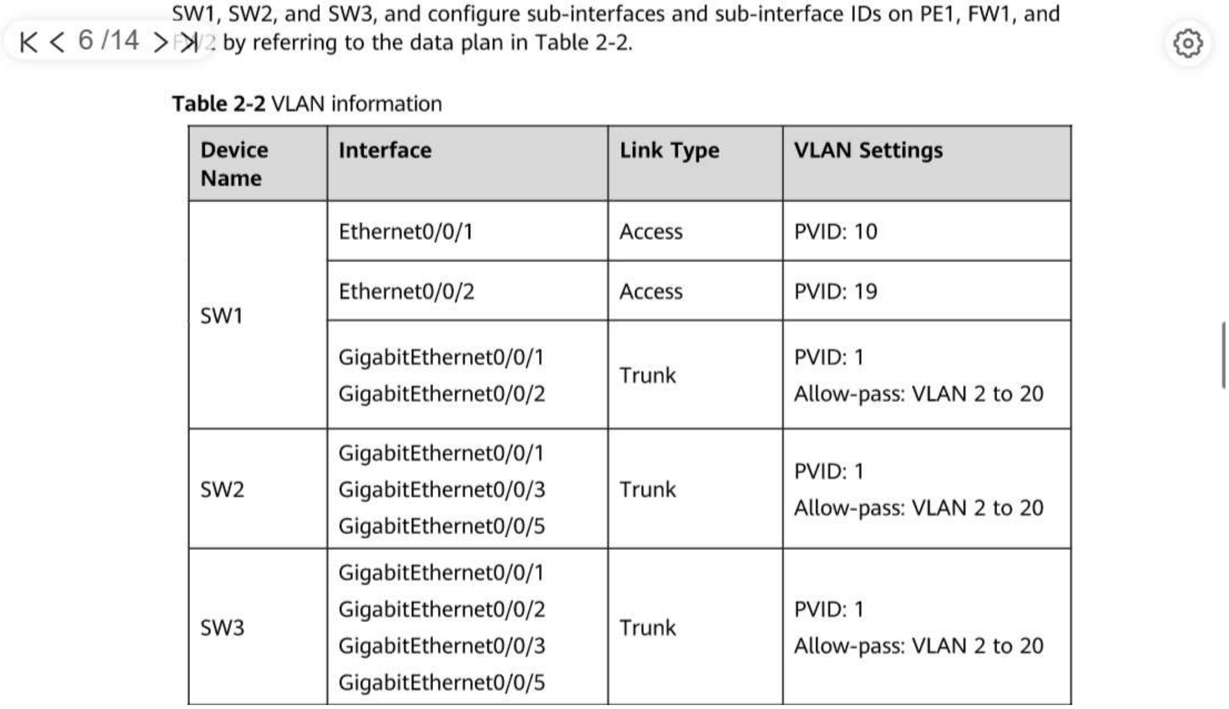
4. FW3 in the data center advertises the default OSPF route 0.0.0.0 to direct return traffic from Web-Server to FW3.
5. A default static route (0.0.0.0) is configured on FW3 to direct return traffic from Web-Server to the WAN.
6. A static route (192.168.0.0) is configured in the VPN instance on PE1 to direct return traffic from Web-Server to the enterprise intranet. The route is advertised to the VPN instance on PE2 through MP-IBGP for transmitting return traffic from Web-Server to PE1 through PE2.

2.1 Configuration Tasks

2.1.1 Task 1: VLAN Configuration

Configure names for network devices, configure the VLAN link types and VLAN parameters on

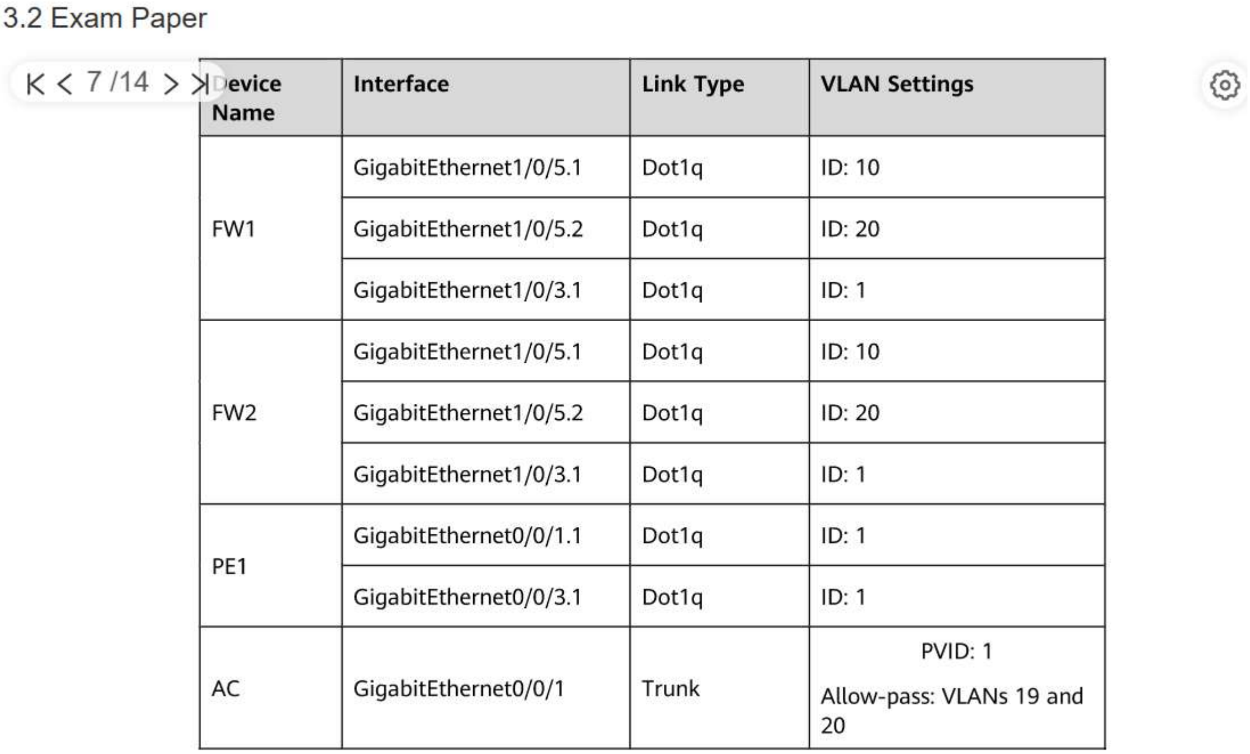
3.2 Exam Paper



SW1, SW2, and SW3, and configure sub-interfaces and sub-interface IDs on PE1, FW1, and FW2 by referring to the data plan in Table 2-2.

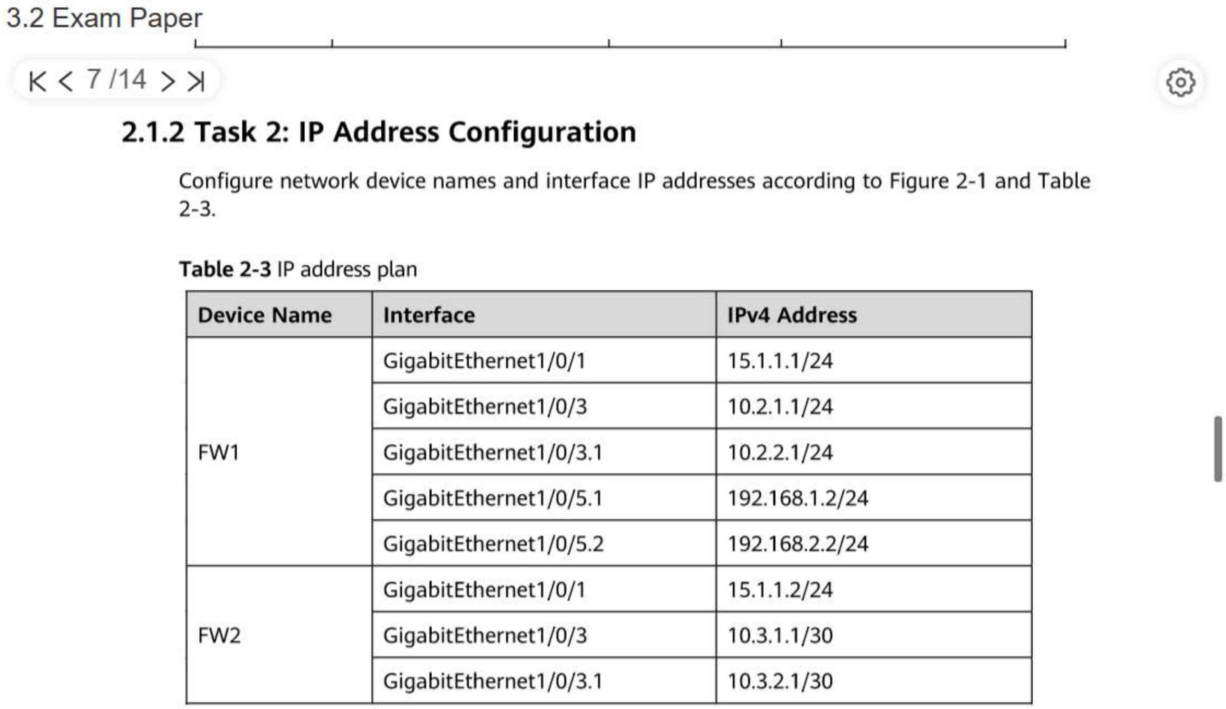
Table 2-2 VLAN information

Device Name	Interface	Link Type	VLAN Settings
SW1	Ethernet0/0/1	Access	PVID: 10
	Ethernet0/0/2	Access	PVID: 19
	GigabitEthernet0/0/1 GigabitEthernet0/0/2	Trunk	PVID: 1 Allow-pass: VLAN 2 to 20
SW2	GigabitEthernet0/0/1 GigabitEthernet0/0/3 GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2 to 20
SW3	GigabitEthernet0/0/1 GigabitEthernet0/0/2 GigabitEthernet0/0/3 GigabitEthernet0/0/5	Trunk	PVID: 1 Allow-pass: VLAN 2 to 20



3.2 Exam Paper

Device Name	Interface	Link Type	VLAN Settings
FW1	GigabitEthernet1/0/5.1	Dot1q	ID: 10
	GigabitEthernet1/0/5.2	Dot1q	ID: 20
	GigabitEthernet1/0/3.1	Dot1q	ID: 1
FW2	GigabitEthernet1/0/5.1	Dot1q	ID: 10
	GigabitEthernet1/0/5.2	Dot1q	ID: 20
	GigabitEthernet1/0/3.1	Dot1q	ID: 1
PE1	GigabitEthernet0/0/1.1	Dot1q	ID: 1
	GigabitEthernet0/0/3.1	Dot1q	ID: 1
AC	GigabitEthernet0/0/1	Trunk	PVID: 1 Allow-pass: VLANs 19 and 20



3.2 Exam Paper

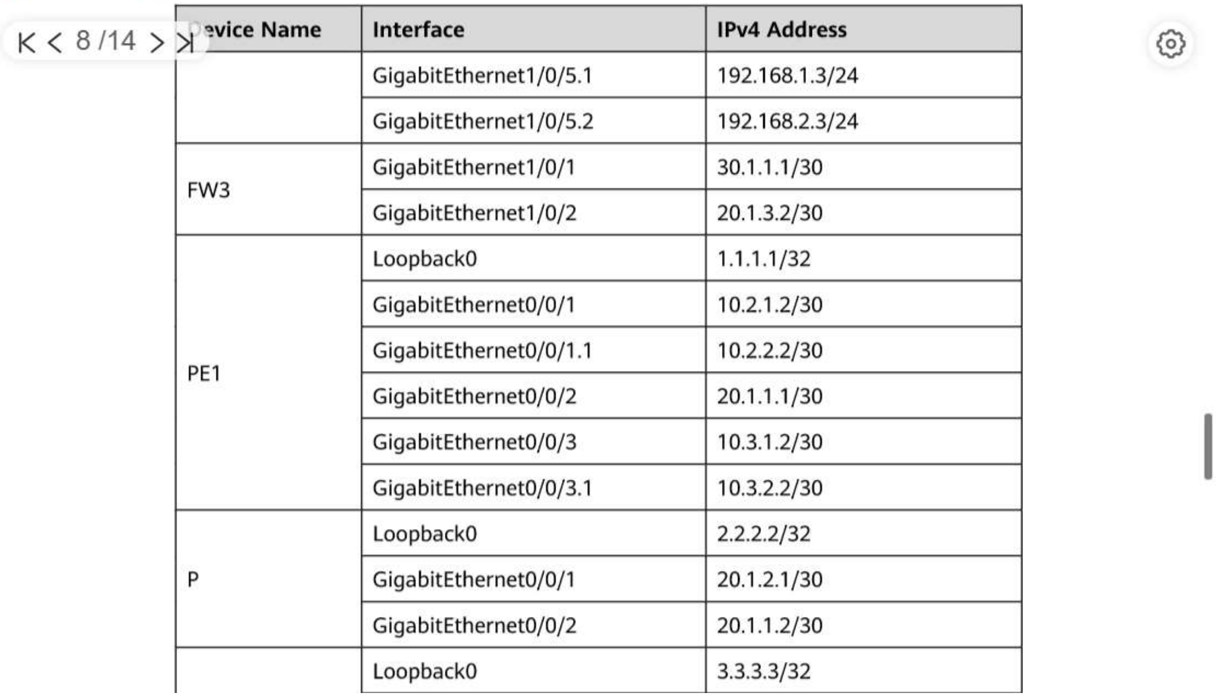
2.1.2 Task 2: IP Address Configuration

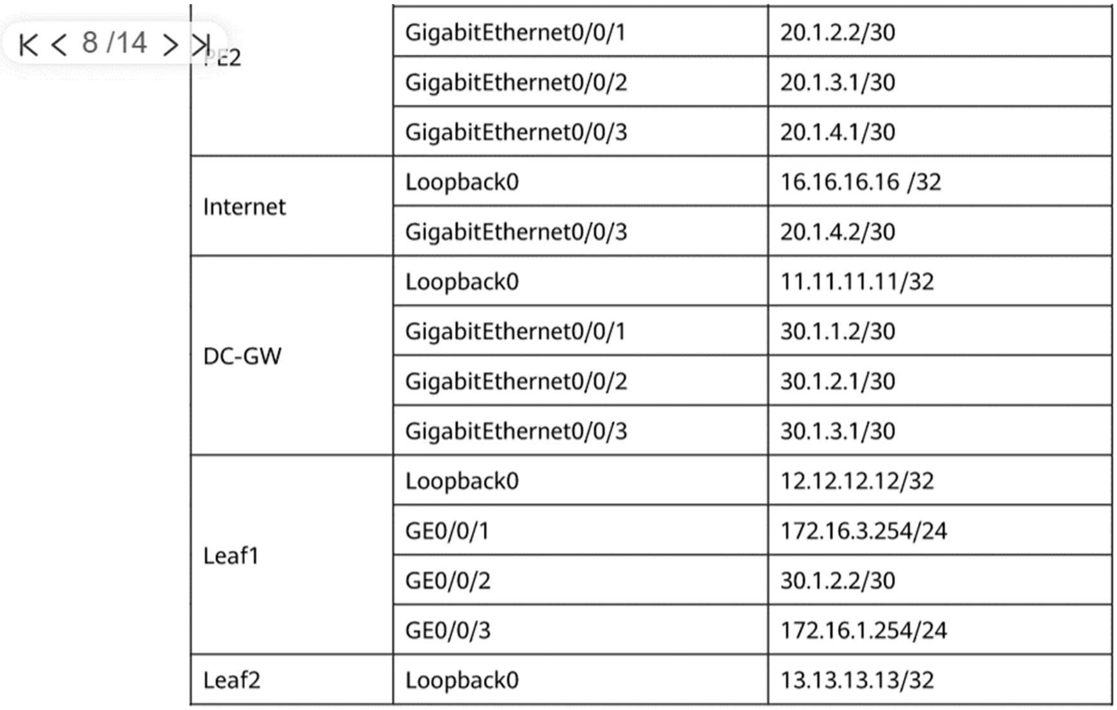
Configure network device names and interface IP addresses according to Figure 2-1 and Table 2-3.

Table 2-3 IP address plan

Device Name	Interface	IPv4 Address
FW1	GigabitEthernet1/0/1	15.1.1.1/24
	GigabitEthernet1/0/3	10.2.1.1/24
	GigabitEthernet1/0/3.1	10.2.2.1/24
	GigabitEthernet1/0/5.1	192.168.1.2/24
	GigabitEthernet1/0/5.2	192.168.2.2/24
FW2	GigabitEthernet1/0/1	15.1.1.2/24
	GigabitEthernet1/0/3	10.3.1.1/30
	GigabitEthernet1/0/3.1	10.3.2.1/30

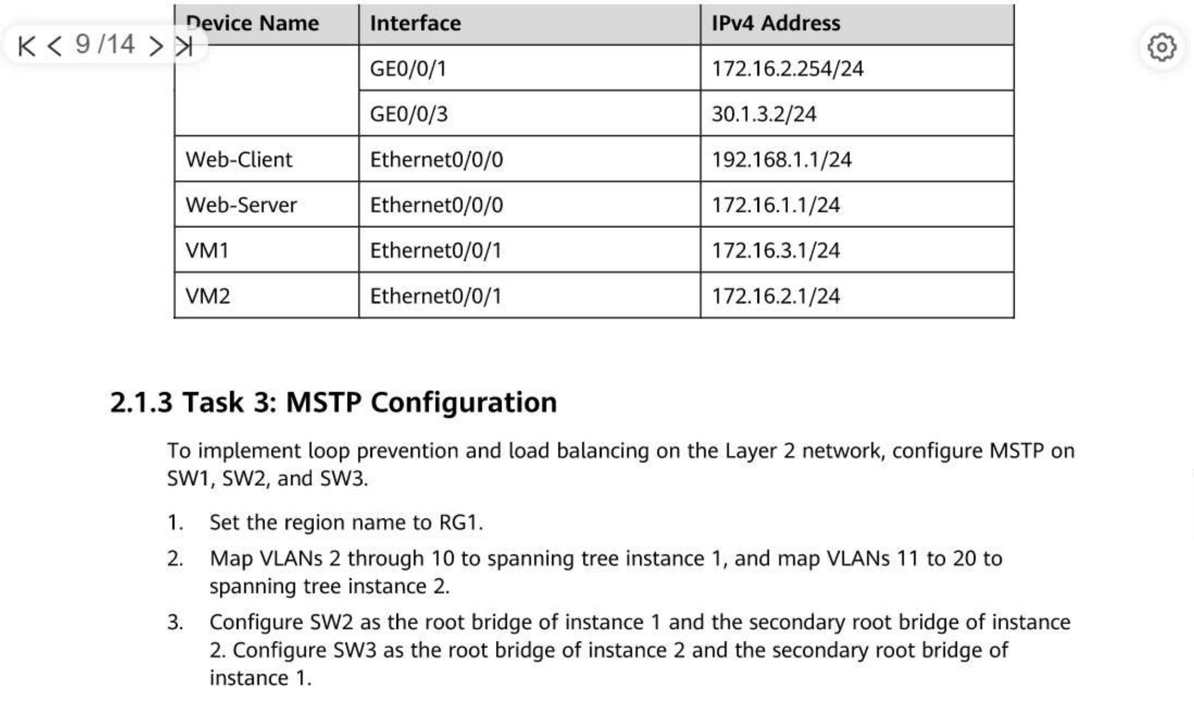
3.2 Exam Paper





Device Name	Interface	IPv4 Address
	GigabitEthernet1/0/5.1	192.168.1.3/24
	GigabitEthernet1/0/5.2	192.168.2.3/24
FW3	GigabitEthernet1/0/1	30.1.1.1/30
	GigabitEthernet1/0/2	20.1.3.2/30
PE1	Loopback0	1.1.1.1/32
	GigabitEthernet0/0/1	10.2.1.2/30
	GigabitEthernet0/0/1.1	10.2.2.2/30
	GigabitEthernet0/0/2	20.1.1.1/30
	GigabitEthernet0/0/3	10.3.1.2/30
	GigabitEthernet0/0/3.1	10.3.2.2/30
P	Loopback0	2.2.2.2/32
	GigabitEthernet0/0/1	20.1.2.1/30
	GigabitEthernet0/0/2	20.1.1.2/30
PE2	Loopback0	3.3.3.3/32
	GigabitEthernet0/0/1	20.1.2.2/30
	GigabitEthernet0/0/2	20.1.3.1/30
	GigabitEthernet0/0/3	20.1.4.1/30
Internet	Loopback0	16.16.16.16 /32
	GigabitEthernet0/0/3	20.1.4.2/30
DC-GW	Loopback0	11.11.11.11/32
	GigabitEthernet0/0/1	30.1.1.2/30
	GigabitEthernet0/0/2	30.1.2.1/30
	GigabitEthernet0/0/3	30.1.3.1/30
Leaf1	Loopback0	12.12.12.12/32
	GE0/0/1	172.16.3.254/24
	GE0/0/2	30.1.2.2/30
	GE0/0/3	172.16.1.254/24
Leaf2	Loopback0	13.13.13.13/32

3.2 Exam Paper



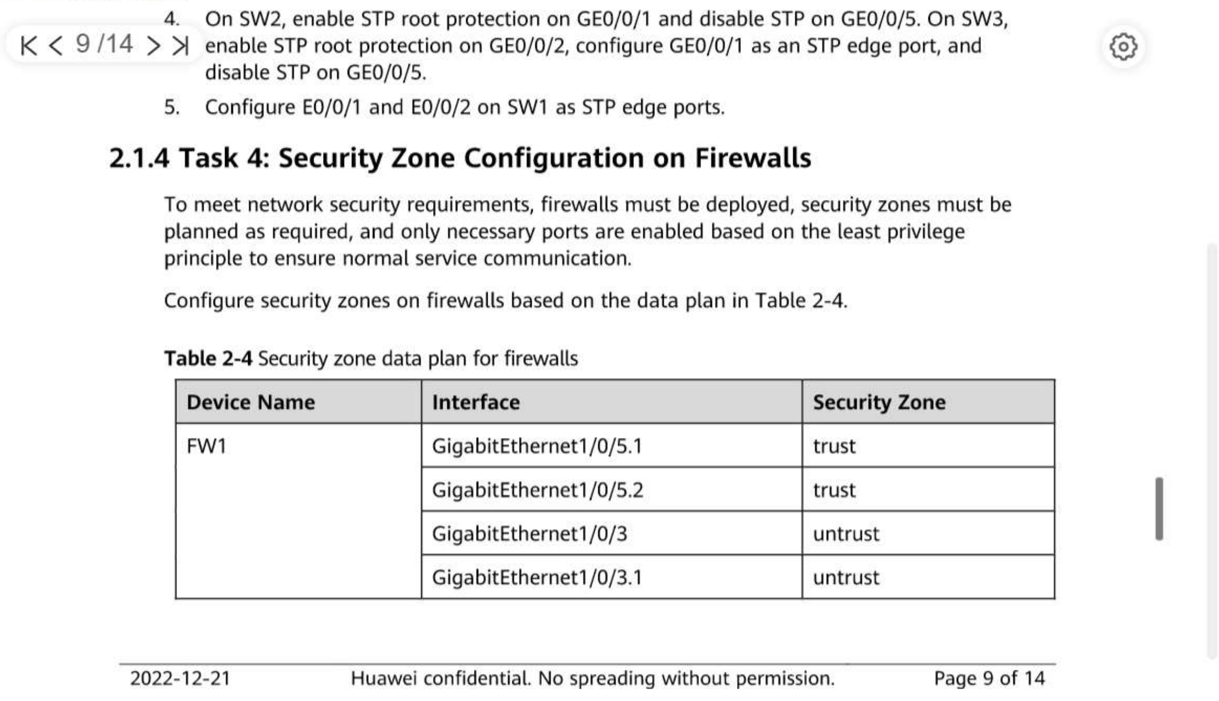
Device Name	Interface	IPv4 Address
	GE0/0/1	172.16.2.254/24
	GE0/0/3	30.1.3.2/24
Web-Client	Ethernet0/0/0	192.168.1.1/24
Web-Server	Ethernet0/0/0	172.16.1.1/24
VM1	Ethernet0/0/1	172.16.3.1/24
VM2	Ethernet0/0/1	172.16.2.1/24

2.1.3 Task 3: MSTP Configuration

To implement loop prevention and load balancing on the Layer 2 network, configure MSTP on SW1, SW2, and SW3.

1. Set the region name to RG1.
2. Map VLANs 2 through 10 to spanning tree instance 1, and map VLANs 11 to 20 to spanning tree instance 2.
3. Configure SW2 as the root bridge of instance 1 and the secondary root bridge of instance 2. Configure SW3 as the root bridge of instance 2 and the secondary root bridge of instance 1.

3.2 Exam Paper



4. On SW2, enable STP root protection on GE0/0/1 and disable STP on GE0/0/5. On SW3, enable STP root protection on GE0/0/2, configure GE0/0/1 as an STP edge port, and disable STP on GE0/0/5.
5. Configure E0/0/1 and E0/0/2 on SW1 as STP edge ports.

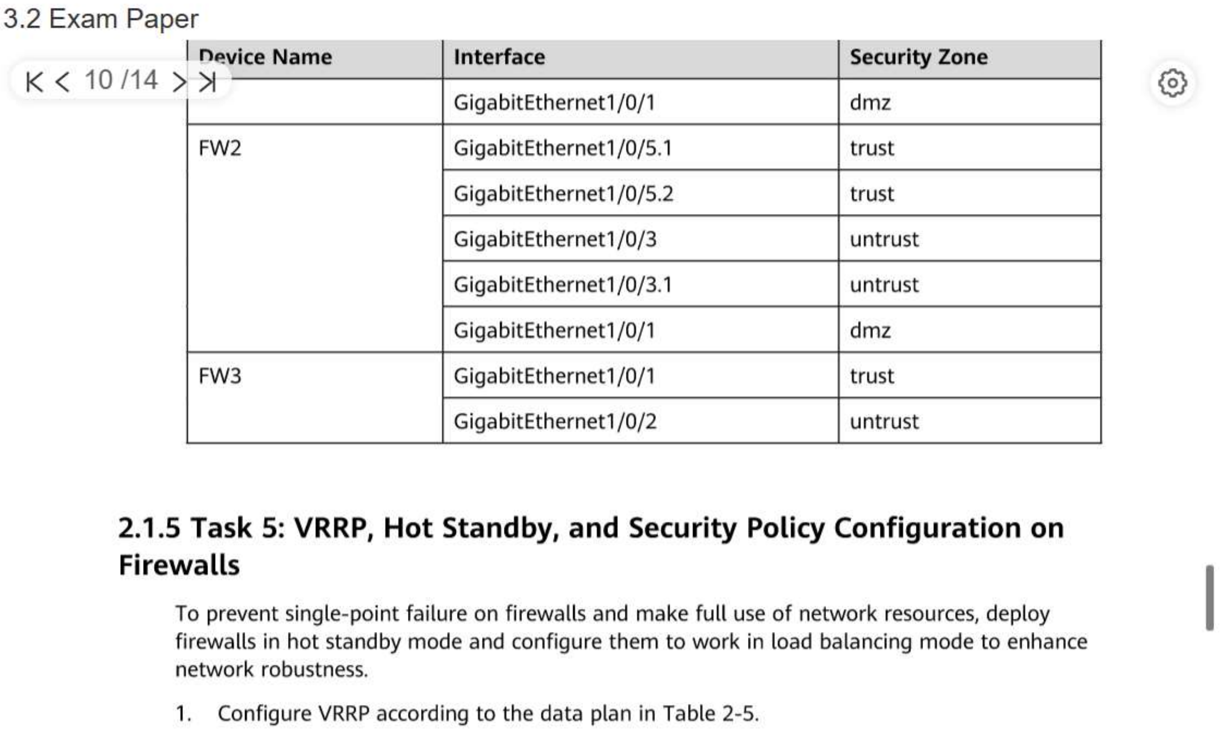
2.1.4 Task 4: Security Zone Configuration on Firewalls

To meet network security requirements, firewalls must be deployed, security zones must be planned as required, and only necessary ports are enabled based on the least privilege principle to ensure normal service communication.

Configure security zones on firewalls based on the data plan in Table 2-4.

Table 2-4 Security zone data plan for firewalls

Device Name	Interface	Security Zone
FW1	GigabitEthernet1/0/5.1	trust
	GigabitEthernet1/0/5.2	trust
	GigabitEthernet1/0/3	untrust
	GigabitEthernet1/0/3.1	untrust



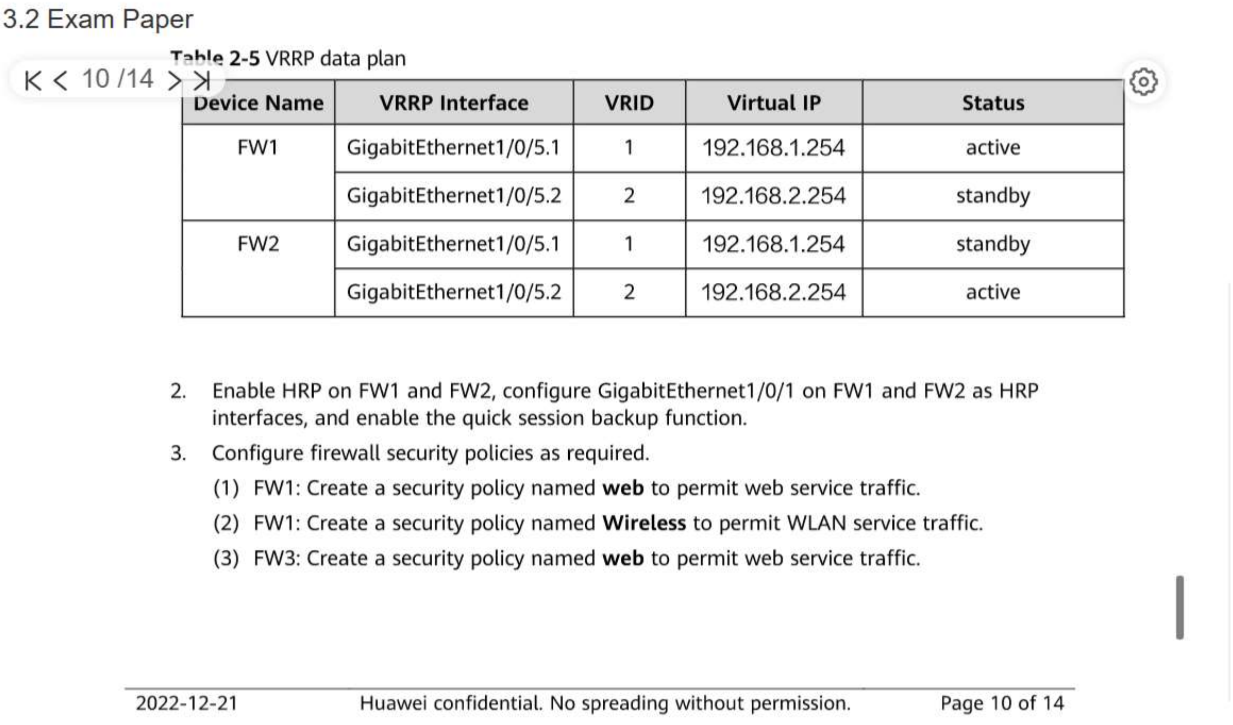
3.2 Exam Paper

Device Name	Interface	Security Zone
	GigabitEthernet1/0/1	dmz
FW2	GigabitEthernet1/0/5.1	trust
	GigabitEthernet1/0/5.2	trust
	GigabitEthernet1/0/3	untrust
	GigabitEthernet1/0/3.1	untrust
	GigabitEthernet1/0/1	dmz
FW3	GigabitEthernet1/0/1	trust
	GigabitEthernet1/0/2	untrust

2.1.5 Task 5: VRRP, Hot Standby, and Security Policy Configuration on Firewalls

To prevent single-point failure on firewalls and make full use of network resources, deploy firewalls in hot standby mode and configure them to work in load balancing mode to enhance network robustness.

1. Configure VRRP according to the data plan in Table 2-5.



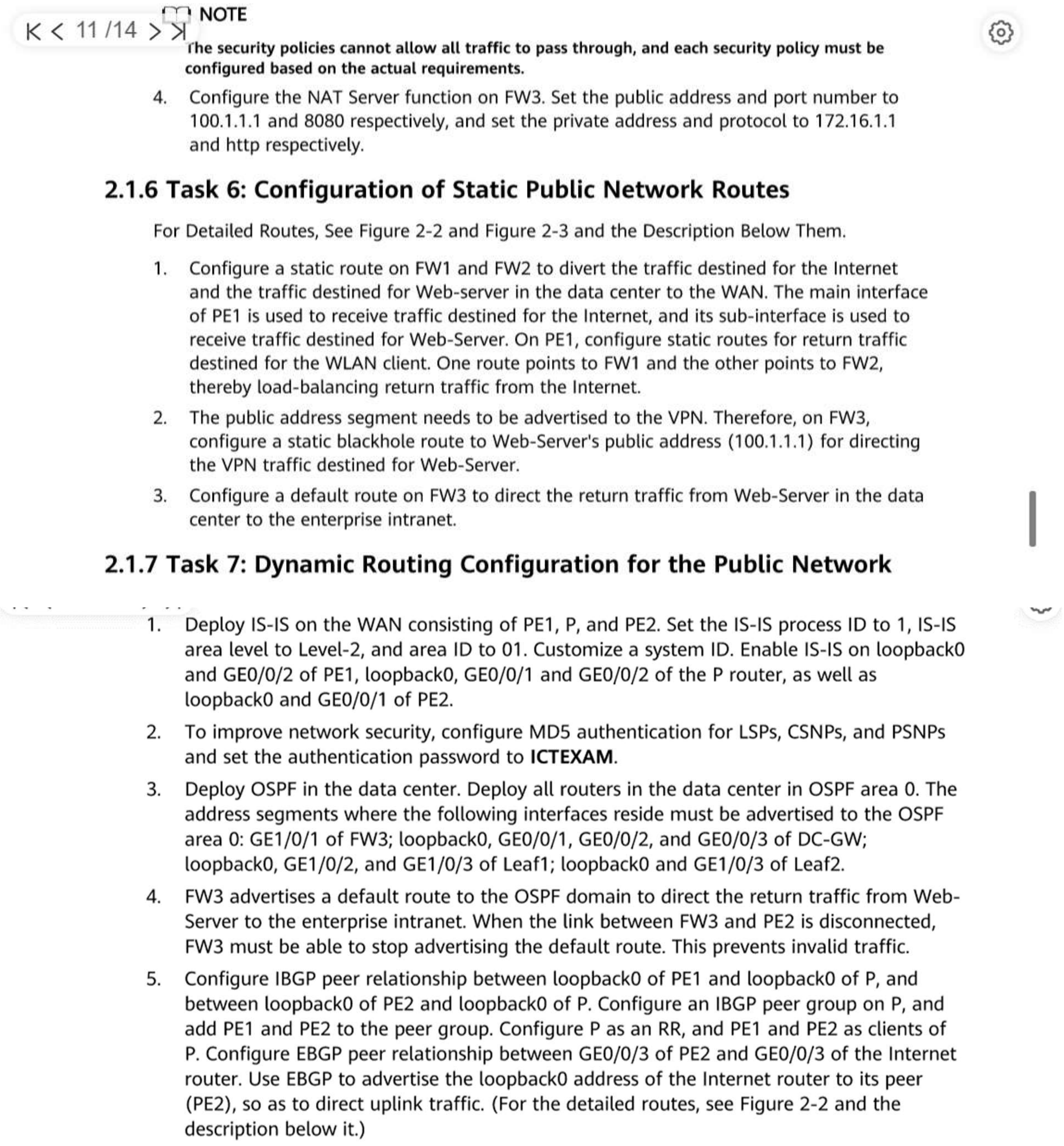
3.2 Exam Paper

Table 2-5 VRRP data plan

Device Name	VRRP Interface	VRID	Virtual IP	Status
FW1	GigabitEthernet1/0/5.1	1	192.168.1.254	active
	GigabitEthernet1/0/5.2	2	192.168.2.254	standby
FW2	GigabitEthernet1/0/5.1	1	192.168.1.254	standby
	GigabitEthernet1/0/5.2	2	192.168.2.254	active

2. Enable HRP on FW1 and FW2, configure GigabitEthernet1/0/1 on FW1 and FW2 as HRP interfaces, and enable the quick session backup function.
3. Configure firewall security policies as required.
   (1) FW1: Create a security policy named **web** to permit web service traffic.
   (2) FW1: Create a security policy named **Wireless** to permit WLAN service traffic.
   (3) FW3: Create a security policy named **web** to permit web service traffic.

3.2 Exam Paper



NOTE

The security policies cannot allow all traffic to pass through, and each security policy must be configured based on the actual requirements.

4. Configure the NAT Server function on FW3. Set the public address and port number to 100.1.1.1 and 8080 respectively, and set the private address and protocol to 172.16.1.1 and http respectively.

2.1.6 Task 6: Configuration of Static Public Network Routes

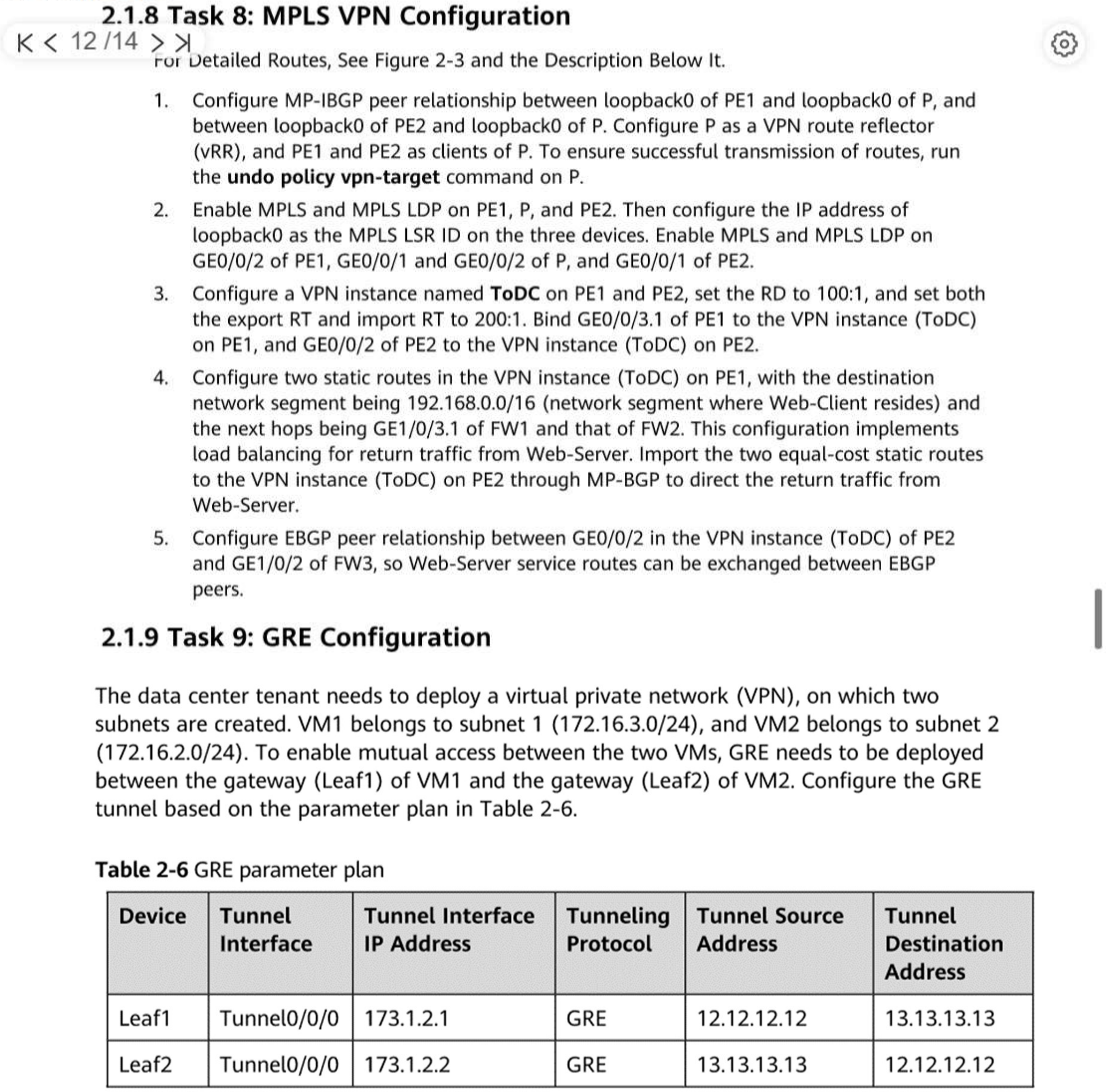
For Detailed Routes, See Figure 2-2 and Figure 2-3 and the Description Below Them.

1. Configure a static route on FW1 and FW2 to divert the traffic destined for the Internet and the traffic destined for Web-server in the data center to the WAN. The main interface of PE1 is used to receive traffic destined for the Internet, and its sub-interface is used to receive traffic destined for Web-Server. On PE1, configure static routes for return traffic destined for the WLAN client. One route points to FW1 and the other points to FW2, thereby load-balancing return traffic from the Internet.
2. The public address segment needs to be advertised to the VPN. Therefore, on FW3, configure a static blackhole route to Web-Server's public address (100.1.1.1) for directing the VPN traffic destined for Web-Server.
3. Configure a default route on FW3 to direct the return traffic from Web-Server in the data center to the enterprise intranet.

2.1.7 Task 7: Dynamic Routing Configuration for the Public Network

1. Deploy IS-IS on the WAN consisting of PE1, P, and PE2. Set the IS-IS process ID to 1, IS-IS area level to Level-2, and area ID to 01. Customize a system ID. Enable IS-IS on loopback0 and GE0/0/2 of PE1, loopback0, GE0/0/1 and GE0/0/2 of the P router, as well as loopback0 and GE0/0/1 of PE2.
2. To improve network security, configure MD5 authentication for LSPs, CSNPs, and PSNPs and set the authentication password to **ICTEXAM**.
3. Deploy OSPF in the data center. Deploy all routers in the data center in OSPF area 0. The address segments where the following interfaces reside must be advertised to the OSPF area 0: GE1/0/1 of FW3; loopback0, GE0/0/1, GE0/0/2, and GE0/0/3 of DC-GW; loopback0, GE1/0/2, and GE1/0/3 of Leaf1; loopback0 and GE1/0/3 of Leaf2.
4. FW3 advertises a default route to the OSPF domain to direct the return traffic from Web-Server to the enterprise intranet. When the link between FW3 and PE2 is disconnected, FW3 must be able to stop advertising the default route. This prevents invalid traffic.
5. Configure IBGP peer relationship between loopback0 of PE1 and loopback0 of P, and between loopback0 of PE2 and loopback0 of P. Configure an IBGP peer group on P, and add PE1 and PE2 to the peer group. Configure P as an RR, and PE1 and PE2 as clients of P. Configure EBGP peer relationship between GE0/0/3 of PE2 and GE0/0/3 of the Internet router. Use EBGP to advertise the loopback0 address of the Internet router to its peer (PE2), so as to direct uplink traffic. (For the detailed routes, see Figure 2-2 and the description below it.)

3.2 Exam Paper



2.1.8 Task 8: MPLS VPN Configuration

For Detailed Routes, See Figure 2-3 and the Description Below It.

1. Configure MP-IBGP peer relationship between loopback0 of PE1 and loopback0 of P, and between loopback0 of PE2 and loopback0 of P. Configure P as a VPN route reflector (vRR), and PE1 and PE2 as clients of P. To ensure successful transmission of routes, run the **undo policy vpn-target** command on P.
2. Enable MPLS and MPLS LDP on PE1, P, and PE2. Then configure the IP address of loopback0 as the MPLS LSR ID on the three devices. Enable MPLS and MPLS LDP on GE0/0/2 of PE1, GE0/0/1 and GE0/0/2 of P, and GE0/0/1 of PE2.
3. Configure a VPN instance named **ToDC** on PE1 and PE2, set the RD to 100:1, and set both the export RT and import RT to 200:1. Bind GE0/0/3.1 of PE1 to the VPN instance (ToDC) on PE1, and GE0/0/2 of PE2 to the VPN instance (ToDC) on PE2.
4. Configure two static routes in the VPN instance (ToDC) on PE1, with the destination network segment being 192.168.0.0/16 (network segment where Web-Client resides) and the next hops being GE1/0/3.1 of FW1 and that of FW2. This configuration implements load balancing for return traffic from Web-Server. Import the two equal-cost static routes to the VPN instance (ToDC) on PE2 through MP-BGP to direct the return traffic from Web-Server.
5. Configure EBGP peer relationship between GE0/0/2 in the VPN instance (ToDC) of PE2 and GE1/0/2 of FW3, so Web-Server service routes can be exchanged between EBGP peers.

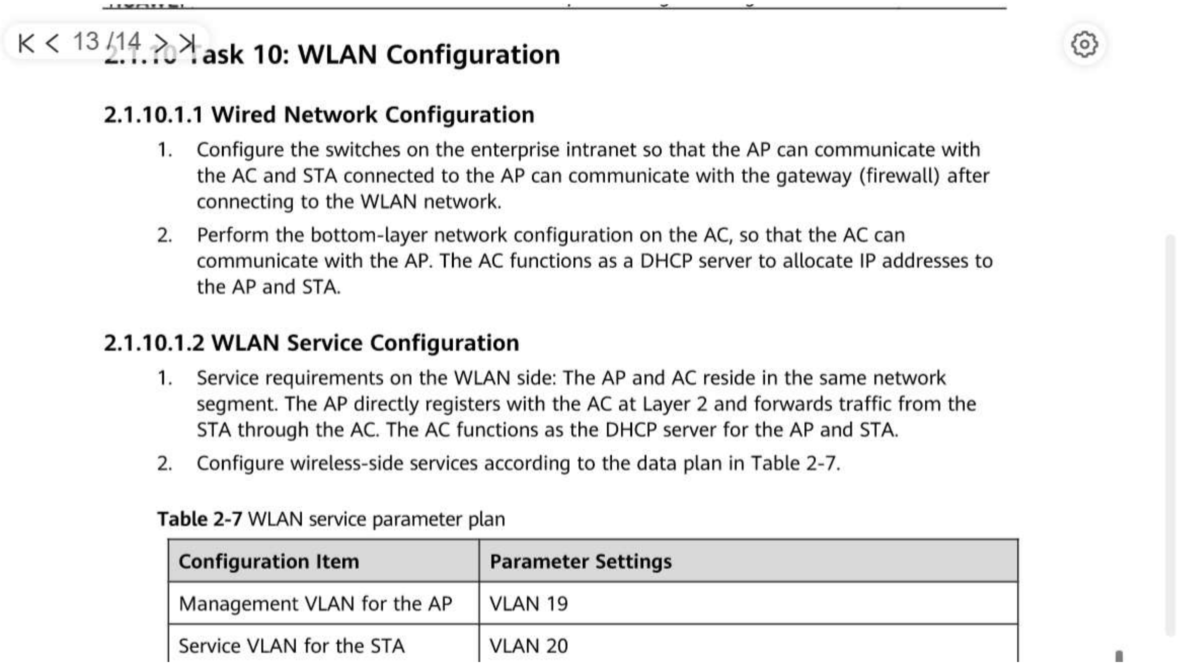
2.1.9 Task 9: GRE Configuration

The data center tenant needs to deploy a virtual private network (VPN), on which two subnets are created. VM1 belongs to subnet 1 (172.16.3.0/24), and VM2 belongs to subnet 2 (172.16.2.0/24). To enable mutual access between the two VMs, GRE needs to be deployed between the gateway (Leaf1) of VM1 and the gateway (Leaf2) of VM2. Configure the GRE tunnel based on the parameter plan in Table 2-6.

Table 2-6 GRE parameter plan

Device	Tunnel Interface	Tunnel Interface IP Address	Tunneling Protocol	Tunnel Source Address	Tunnel Destination Address
Leaf1	Tunnel0/0/0	173.1.2.1	GRE	12.12.12.12	13.13.13.13
Leaf2	Tunnel0/0/0	173.1.2.2	GRE	13.13.13.13	12.12.12.12

3.2 Exam Paper



2.1.10 Task 10: WLAN Configuration

2.1.10.1.1 Wired Network Configuration

1. Configure the switches on the enterprise intranet so that the AP can communicate with the AC and STA connected to the AP can communicate with the gateway (firewall) after connecting to the WLAN network.
2. Perform the bottom-layer network configuration on the AC, so that the AC can communicate with the AP. The AC functions as a DHCP server to allocate IP addresses to the AP and STA.

2.1.10.1.2 WLAN Service Configuration

1. Service requirements on the WLAN side: The AP and AC reside in the same network segment. The AP directly registers with the AC at Layer 2 and forwards traffic from the STA through the AC. The AC functions as the DHCP server for the AP and STA.
2. Configure wireless-side services according to the data plan in Table 2-7.

3.2 Exam Paper

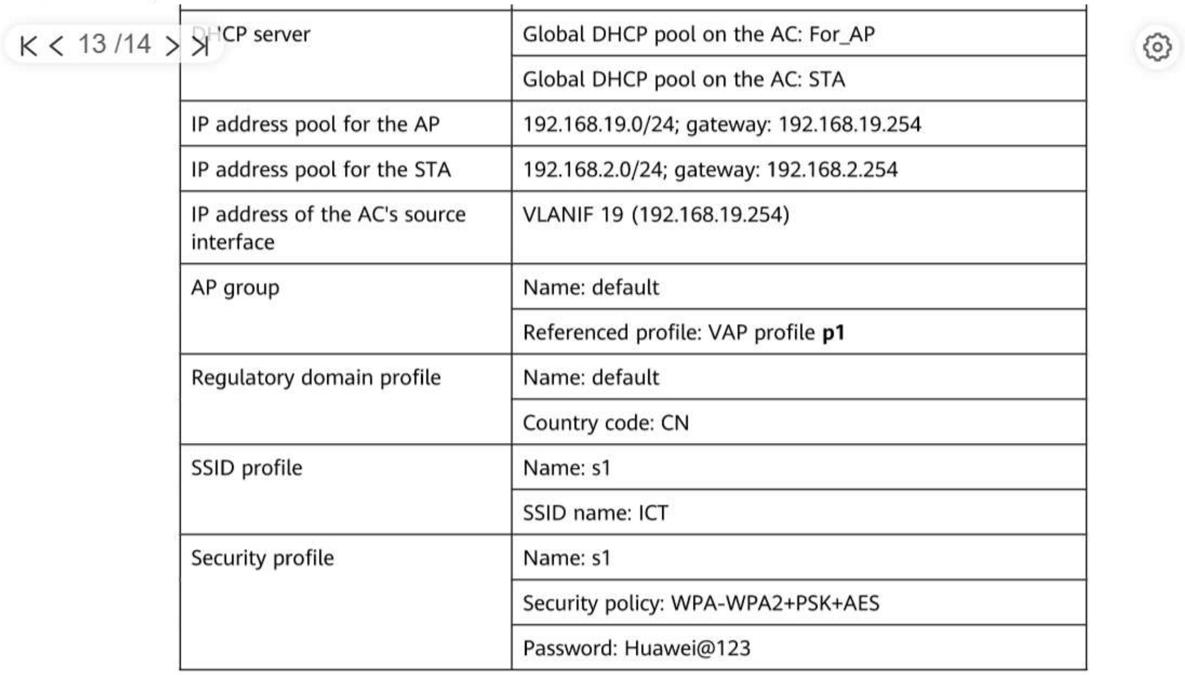


Table 2-7 WLAN service parameter plan

Configuration Item	Parameter Settings
Management VLAN for the AP	VLAN 19
Service VLAN for the STA	VLAN 20
DHCP server	Global DHCP pool on the AC: For_AP
	Global DHCP pool on the AC: STA
IP address pool for the AP	192.168.19.0/24; gateway: 192.168.19.254
IP address pool for the STA	192.168.2.0/24; gateway: 192.168.2.254
IP address of the AC's source interface	VLANIF 19 (192.168.19.254)
AP group	Name: default
	Referenced profile: VAP profile **p1**
Regulatory domain profile	Name: default
	Country code: CN
SSID profile	Name: s1
	SSID name: ICT
Security profile	Name: s1
	Security policy: WPA-WPA2+PSK+AES
	Password: Huawei@123

Configuration Item	Parameter Settings
VAP profile	Name: p1
	Forwarding mode: tunnel forwarding
	Service VLAN: VLAN 20
	Referenced profiles: SSID profile **s1** and security profile **s1**