Huawei ICT Competition 2020

Hands-on Lab Exam

Network Track

Issue: 1.0

HUAWEI

Contents

1 Background

A large company has a headquarters (HQ) and a branch (BR-1). The HQ network needs to provide both wired and wireless access for employees, and the wired and wireless services need to be isolated from each other.

To facilitate service development in the future, the company wants to deploy an IPv6 network for BR-1. However, the ISP has never deployed an IPv6 network before. Consequently, the HQ is used as a test node, where IPv6 transition technology is used to achieve connectivity between the HQ and BR-1 networks.

2 Exam Description

2.1 Total Score

The exam consists of three parts: routing and switching, security, and WLAN. The total score is 1000 points.

2.2 Device Introduction

2.2.1 Device List

- Two USG6000V firewalls (FW1 and FW2)
- Seven AR2220 routers (R1 to R6 and PC2)
- Four S5700 switches (SW1 to SW4)
- Two AC6005 devices (AC1 and AC2)

- One AP4050DN (AP1)
- One PC (PC1)
- One STA (STA1)

2.2.2 Exam Tools

Three computers, on which the eNSP, HedEx Lite, and HedEx product documentation is provided (AR + switch + firewall + AC)

3 Tasks

Figure 3-1 IP network topology

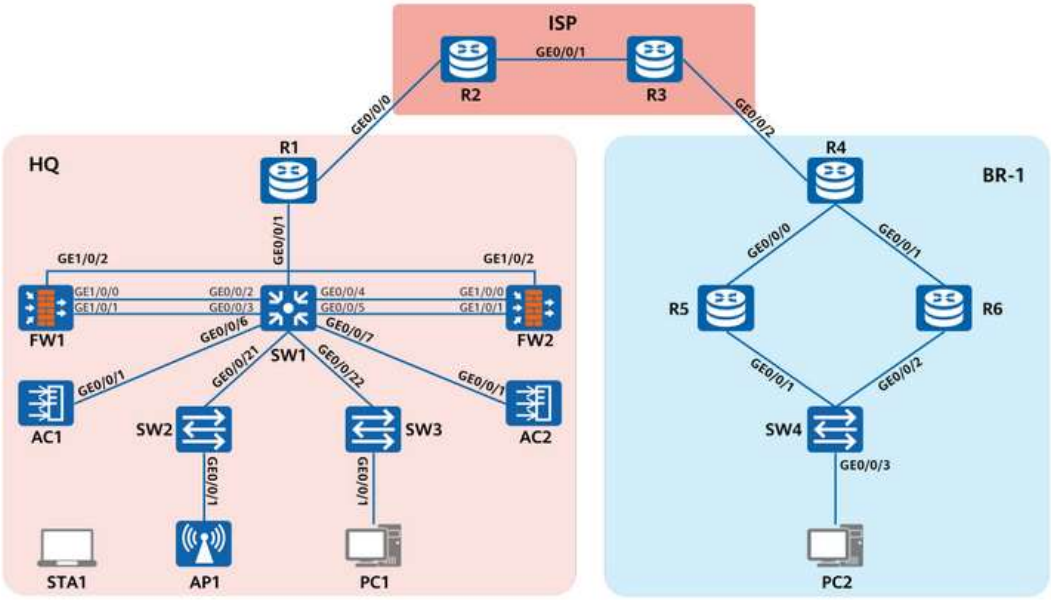


Table 3-1 Device login information

Device	User Name	Default Password	New Password
Firewall	admin	Admin@123	Huawei@ICT2020

Table 3-2 VLAN information

Device Name	Port	Link Type	VLAN Settings
SW1	Eth-Trunk1	Trunk	PVID: 1 Allow-pass: VLANs 110, 120, and 130
	Eth-Trunk2	Trunk	PVID: 1 Allow-pass: VLANs 110, 120, and 130
	G0/0/1	Access	PVID: 130
	G0/0/6	Trunk	PVID: 1 Allow-pass: VLAN 50
	G0/0/7	Trunk	PVID: 1 Allow-pass: VLAN 50
	G0/0/21	Trunk	PVID: 1 Allow-pass: VLANs 20 and 30
	G0/0/22	Trunk	PVID: 1 Allow-pass: VLAN 10
SW2	GE0/0/1	Access	PVID: 20
	G0/0/21	Trunk	PVID: 1 Allow-pass: VLANs 20 and 30
SW3	GE0/0/1	Access	PVID: 10
	G0/0/22	Trunk	PVID: 1 Allow-pass: VLAN 10
AC1	G0/0/1	Trunk	PVID: 1 Allow-pass: VLAN 50
AC2	G0/0/1	Trunk	PVID: 1 Allow-pass: VLAN 50
FW1	Eth-Trunk1	Trunk	PVID: 1 Allow-pass: VLANs 110, 120, and 130
FW2	Eth-Trunk1	Trunk	PVID: 1 Allow-pass: VLANs 110, 120, and 130

Table 3-3 IP address planning

Device Name	Port	IP Address
R1	Loopback0	1.1.1.1/32
	Loopback1	100.1.1.1/32
	Loopback2	2002:6401:101:101::1/64
	G0/0/0	100.1.12.1/30
	G0/0/1	192.168.130.1/24
	Tunnel0/0/0	2002:6401:101:1111::1/64
R2	Loopback0	2.2.2.2/32
	G0/0/0	100.1.12.2/30
	G0/0/1	100.1.23.1/30
R3	Loopback0	3.3.3.3/32
	Loopback1	114.114.114.114/32
	G0/0/1	100.1.23.2/30

	G0/0/2	100.1.34.1/30
R4	Loopback0	4.4.4.4/32
	Loopback1	100.4.4.4/32
	Loopback2	2002:6404:404:404::4/64
	G0/0/0	2002:6404:404:45::1/64
	G0/0/1	2002:6404:404:46::1/64
	G0/0/2	100.1.34.2/30
	Tunnel0/0/0	2002:6404:404:4444::4/64
R5	G0/0/0	2002:6404:404:45::2/64
	G0/0/1	2002:6404:404:56::1/64
R6	G0/0/1	2002:6404:404:46::2/64
	G0/0/2	2002:6404:404:56::2/64
SW1	VLANIF 10	192.168.10.254/24
	VLANIF 20	192.168.20.254/24
	VLANIF 30	192.168.30.254/24

Device Name	Port	IP Address
	VLANIF 50	192.168.50.1/24
	VLANIF 110	192.168.110.1/24
	VLANIF 120	192.168.120.1/24
FW1	G1/0/2	192.168.70.1/30
	VLANIF 110	192.168.110.2/24
	VLANIF 120	192.168.120.2/24
	VLANIF 130	192.168.130.2/24
FW2	G1/0/2	192.168.70.2/30
	VLANIF 110	192.168.110.3/24
	VLANIF 120	192.168.120.3/24
	VLANIF 130	192.168.130.3/24
AC1	Loopback0	11.11.11.11/32
	VLANIF 50	192.168.50.2/24
AC2	Loopback0	12.12.12.12/32
	VLANIF 50	192.168.50.3/24

3.1 Device Naming

Name the corresponding network devices according to the IP network topology in Figure 3-1.

3.2 HQ Network Configuration

3.2.1 Configuring Link Aggregation

1. Link aggregation in this exam is performed in manual mode.
2. Configure Eth-Trunk1 (G0/0/2 and G0/0/3) on SW1 and Eth-Trunk1 (G1/0/0 and G1/0/1) on FW1 for link aggregation.
3. Configure Eth-Trunk2 (G0/0/4 and G0/0/5) on SW1 and Eth-Trunk1 (G1/0/0 and G1/0/1) on FW2 for link aggregation.

3.2.2 Deploying VLANs

Configure VLANs on all switches, firewalls, and ACs according to Figure 3-1, Table 3-2, and Table 3-3. To ensure network connectivity, configure certain devices to allow traffic from corresponding VLANs to pass through according to Table 3-2.

NOTE

If traffic from other VLANs needs to be allowed to pass through in other modules, configure involved devices as required.

3.2.3 Configuring IP Addresses

Set interface IP addresses according to the IP network topology shown in Figure 3-1 and the IP address planning listed in Table 3-3.

3.2.4 Enabling HSB for Firewalls

FW1 and FW2 are connected to the aggregation switch in off-path mode to safeguard the HQ network. The company wants FW1 and FW2 to work in Active/Standby mode of hot standby (HSB). In normal situations, FW1 forwards traffic. If FW1 fails, FW2 takes over traffic forwarding to ensure service continuity.

3.2.4.1 Configuring a VRRP Group

1. Wired and wireless access traffic on the intranet and access traffic to the extranet need to pass through firewalls. As such, configure three VRRP groups on FW1 to connect to the wired network, wireless network, and router, respectively. Repeat this configuration on FW2.
2. Configure VRRP group 1 for VLAN 110 and set the virtual IP address of VLAN 110 to 192.168.110.4.
3. Configure VRRP group 2 for VLAN 120 and set the virtual IP address of VLAN 120 to 192.168.120.4.
4. Configure VRRP group 3 for VLAN 130 and set the virtual IP address of VLAN 130 to 192.168.130.4.

3.2.4.2 Configuring Heartbeat Links

Specify firewalls' GE1/0/2 in the DMZ as the heartbeat interface and enable HSB.

3.2.5 Configuring Network Isolation

3.2.5.1 Configuring Switch Isolation

1. Wired and wireless services must be isolated on SW1. To implement this, create two VPN instances, namely, **vpn-instance wired** and **vpn-instance wireless**, and set their RD values to 100:1 and 200:2, respectively.
2. On SW1, bind VLAN 10 and VLAN 110 with **vpn-instance wired**.
3. On SW1, bind VLANs 20, 30, 50, and 120 with **vpn-instance wireless**.

3.2.5.2 Configuring Virtual Systems on Firewalls

1. Create two virtual systems (one named **wired** and the other named **wireless**) on firewalls to connect to wired and wireless services on SW1, respectively.

   NOTE

   You must create the virtual system named wired before creating the virtual system named wireless.

2. Assign VLAN 110 to the virtual system **wired** and VLAN 120 to the virtual system **wireless**.

   NOTE

   After VLAN 110 and VLAN 120 are assigned to the corresponding virtual systems, all configurations on the VLANIF interfaces are lost.

3.2.6 Enabling DHCP on the Wired Side

On SW1, create a DHCP service based on a global address pool. Set the name of the address pool to **wired**, gateway address to 192.168.10.254, network segment to 192.168.10.0/24, and DNS server IP address to 114.114.114.114. PC1 needs to dynamically obtain an IP address from the DHCP server.

NOTE

To assign IP addresses to VPN users from an address pool, run the vpn-instance X command in the address pool view to bind the address pool to a VPN instance.

3.2.7 Configuring Security Zones on Firewalls

3.2.7.1 Configuring a Security Zone

1. In the virtual system **public**, assign Virtual-if 0 connected to the virtual system to the Trust zone, VLANIF 130 to the Untrust zone, and G1/0/2 to the DMZ.
2. In the virtual system **wired**, assign virtual interface Virtual-if 1 connected to the virtual system to the Untrust zone and VLANIF 110 to the Trust zone.
3. In the virtual system **wireless**, assign virtual interface Virtual-if 2 connected to the virtual system to the Untrust zone and VLANIF 120 to the Trust zone.

3.2.7.2 Configuring a Security Policy

1. The virtual system **public** allows only one security policy.
2. Configure security policies in virtual systems **wired** and **wireless** to meet service requirements. The security policies must be specific to network segments, security zones, and protocol services.

3.2.8 Configuring a WLAN

3.2.8.1 Enabling DHCP on the Wireless Side

Configure SW1 as a DHCP server, configure a global address pool named **AP**, and enable SW1 to assign IP addresses to APs in VLAN 20.

Configure SW1 as a DHCP server, configure a global address pool named **Laptop**, and enable SW1 to assign IP addresses to STAs in VLAN 30.

Table 3-4 WLAN data planning

Configuration Item	Data
Management VLAN for APs	VLAN 20
Service VLAN for STAs	VLAN 30
DHCP server	SW1 functions as a DHCP server to assign IP addresses to APs and STAs. APs' gateway address: 192.168.20.254/24 STAs' gateway address: 192.168.30.254/24
AC's source interface	Loopback0
Management IP address of AC1	11.11.11.11/32
Management IP address of AC2	12.12.12.12/32
Active AC	Priority of AC1: 0
Standby AC	Priority of AC2: 1
IP addresses of the primary/secondary channel of AC1 Port number	IP addresses: 192.168.50.2/24 Port number: 10241
IP address of the primary/secondary channel of AC2 Port number	IP address: 192.168.50.3/24 Port number: 10241
AP group	Name: **Huawei** Referenced profiles: VAP profile **Huawei** and regulatory domain profile **Huawei**
Regulatory domain profile	Name: **Huawei** Country code: CN
VAP profile	Name: **Huawei**

Configuration Item	Data
	Referenced profiles: SSID profile **Huawei** and security profile **Huawei** Forwarding mode: tunnel forwarding

3.2.8.2 Enabling HSB for ACs

The company wants to improve network reliability to guarantee normal service operation. To meet the company's requirements, configure Dual-link HSB on the WLAN.

1. Enable AC1 and AC2 to work in Active/Standby mode. AC1 function as the active device and AC2 functions as the standby device.
2. All information on AC1 is backed up to AC2 in real time. If AC1 fails, AC2 immediately becomes the active device and starts to provide the WLAN service, ensuring service continuity.

3.2.8.3 Configuration and Delivery

1. Enable an SSID named **Huawei-ICT**.
2. Set the authentication mode to WPA2-PSK, encryption mode to aes-tkip, password to **Huawei@ICT2020**, and service data forwarding mode to tunnel forwarding.

3.2.9 Ensuring Network Connectivity

3.2.9.1 Configuring NAT

You need to configure NAT on firewalls so that both wired and wireless users can access the Internet. To differentiate wired and wireless services, deploy NAT in virtual systems **wired** and **wireless**, and assign 20 public IP addresses obtained from the ISP to the wired and wireless services.

1. Assign public IP addresses to the virtual systems. The IP address segment for virtual systems **wired** and **wireless** are 200.1.1.1-200.1.1.10 and 200.1.2.1–200.1.2.10, respectively.
2. In the virtual system **wired**, configure NAT No-Pat using an address pool named **wired** and with an IP address range 200.1.1.1–200.1.1.10.
3. In the virtual system **wireless**, configure NAPT using an address pool named **wireless** and with an IP address range 200.1.2.1–200.1.2.10.

3.2.9.2 Configuring Static Routes

1. Configure static routes on SW1, on virtual systems **public**, **wired**, and **wireless**, and on R1 to ensure interconnectivity between the intranet and extranet.

2. Enable virtual system **public** to access virtual systems **wired** and **wireless** based on the traffic diversion table.
3. It is required that no private network route to the network segment (192.168.X.X) of wired and wireless services be configured on R1 or in the virtual system **public**.

3.3 Configuring an Internal ISP Network

3.3.1 Configuring IP Addresses

Set interface IP addresses according to the IP network topology shown in Figure 3-1 and the IP address planning listed in Table 3-3.

3.3.2 Configuring OSPF

Table 3-5 OSPF interface information

Device Name	Port	Area ID
R1	Loopback0	0
	Loopback1	
	G0/0/0	
R2	Loopback0	0
	G0/0/0	
	G0/0/1	1
R3	Loopback0	1
	Loopback1	
	G0/0/1	
	G0/0/2	2
R4	Loopback0	2
	Loopback1	
	G0/0/2	

1. Enable OSPF on R1, R2, R3, and R4 according to Table 3-5.
2. The OSPF router ID must be X.X.X.X, where X is the device ID. For example, the router ID of R1 is 1.1.1.1.

3. IP addresses must be matched accurately when OSPF interfaces are advertised. For example, to advertise an interface with address 100.1.12.1/24, you can run the **network 100.1.12.1 0.0.0.0** command.
4. To safeguard the ISP area, enable OSPF area authentication on all OSPF routers and set the authentication mode to MD5, encryption type to plain, and authentication key to **Huawei@ICT2020**.
5. After the preceding configurations are complete, it is expected that Loopback 1 on R1 can communicate with Loopback 1 on R4.

3.3.3 Intranet and Extranet Communication

After you finish the configuration of this part, STA1 and PC1 at the HQ can access Loopback 1 on R3 of ISP.

3.4 Configuring the Network of BR-1

3.4.1 Configuring IP Addresses

Set interface IP addresses according to the IP network topology shown in Figure 3-1 and the IP address planning listed in Table 3-3.

3.4.2 Configuring OSPFv3

1. Enable OSPFv3 on R4, R5, and R6, and set the process ID to 1.
2. Enable OSPFv3 on G0/0/0 and G0/0/1 of R4, G0/0/0 and G0/0/1 of R5, and G0/0/1 and G0/0/2 on R6. Ensure that all these interfaces are in area 0.

3.4.3 Configuring SLAAC

1. Enable PC2 to obtain an IPv6 address using the stateless address autoconfiguration function.
2. Configure R5 as the active gateway of PC2, and configure R6 as the standby gateway of PC2. (This configuration can be performed only on R5, and VRRP cannot be used.)

NOTE

PC2 is simulated using a router and has been pre-configured. No additional configuration is required.

3.5 Inter-Network Communication

3.5.1 Establishing an IPv6-to-IPv4 Tunnel

On R1 and R4, use Tunnel0/0/0 to establish an IPv6-to-IPv4 tunnel. Ensure that mutual access traffic between R1's Loopback2 and BR-1's IPv6 intranet can pass through the intermediate IPv4 network.

4 Task Saving

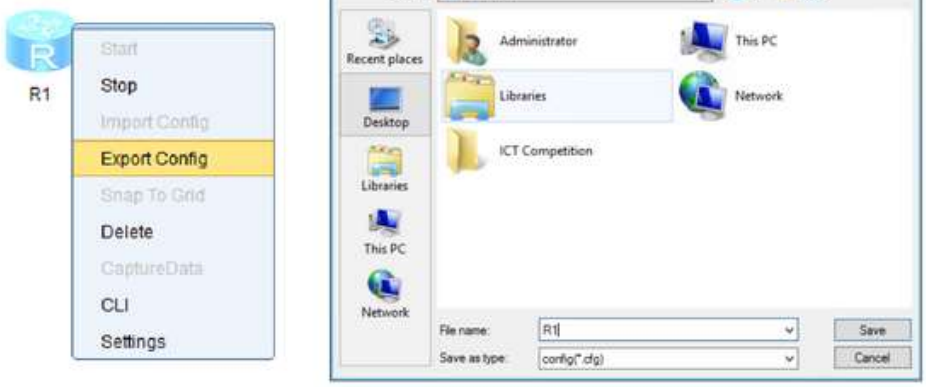
4.1 Save Answer

(1) Create a folder on PC1's desktop and name it with the **team name**.

(2) Export the complete configuration of each device to the **.cfg** file. The **.cfg** file is named after the device name (for example, R1).

Note: *if you fail to export the configuration, please copy the complete configuration of each device to the* ***.txt*** *file. The* ***.txt*** *file is named after the device name.*

```
<R1>save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<R1>
```

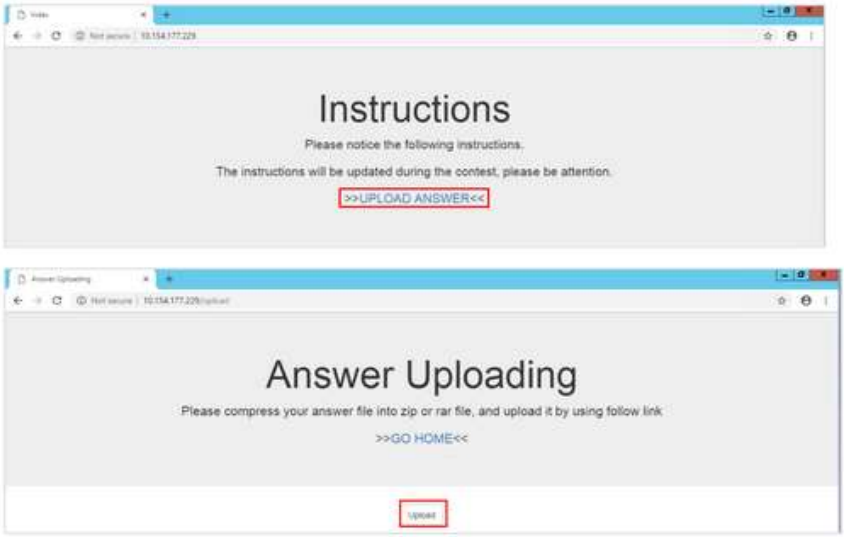


(3) Save the **.cfg** files to the folder and compress the folder into a **.rar** file.

4.2 Submit Answer

(1) Log in to the server: **10.154.177.229**.

(2) Upload answers to the server.



4.3 Attention

If the answer file fails to be uploaded, ensure that the answer file is saved on the desktop of PC1 and contact the examiner.