2018-2019 Huawei ICT Competition Global Final

Network Track Exam

Lab Exam

HUAWEI

Contents

1 Background of Task Design **2**

2 Exam Description **3**

2.1 Weighting 3

2.2 Device Introduction 3

2.2.1 Device List 3

2.2.2 Exam Tools 3

2.3 Saving Tasks 3

3 Tasks **4**

3.1 Task Contents 8

3.1.1 Device Connection 8

3.1.2 iStack (50 points) 8

3.1.3 Link Aggregation (30 points) 8

3.1.4 VLAN (20 points) 8

3.1.5 IP Address Planning (10 points) 8

3.1.6 DHCP (30 points) 8

3.1.7 Security Zone (30 points) 8

3.1.8 Firewall Security Policy (200 points) 8

3.1.9 OSPF (60 points) 9

3.1.10 IS-IS (50 points) 10

3.1.11 WLAN (100 points) 10

3.1.12 GRE, PPPoE, and IPsec VPN (200 points) 11

3.1.13 BGP and Route Policy (50 points) 13

3.1.14 IPv6, 6to4 and OSPFv3 (120 points) 13

3.1.15 SNMP and eSight (50 points) 13

1 Background of Task Design

The task in this lab involves setting up network services for large technology companies. It includes setting up the campus network of the Headquarters, the network connecting the Headquarters and branches, and the network providing intranet access for remote employees.

To ensure campus network security and implement mobile office, deploy a firewall and a full-coverage WLAN at the Headquarters. Due to limited IPv4 address resources, further development of technologies is hampered. Therefore, Deploy an IPv6 network in Branch 2 and connect it to the Headquarters through carriers, so that employees can use IPv6 to visit the Headquarters.

2 Exam Description

2.1 Weighting

The network track exam contents include three parts: Routing & Switching, Security, and WLAN. The total score is 1000.

Domain	Weight	Score
Routing & Switching	50%	500
Security	40%	400
WLAN	10%	100

2.2 Device Introduction

2.2.1 Device List

- Two USG6550 firewalls (FW1 and FW2)
- Eight AR2220E routers (R1 to R8)
- Four S5720-36C-PWR-EI-AC switches (SW1 to SW4)
- Two AC6005 ACs (AC1 and AC2)
- Two AP4050 APs (AP1 and AP2)
- One RH1288 server (Server)
- Three exam computers for candidates (PC1 to PC3)

2.2.2 Exam Tools

- Three exam computers, on which the SecureCRT, Wireshark, HedEx Lite, and HedEx product documentation about AR routers, switches, firewalls, and ACs are provided.
- Three console cables.
- 30 network cables.

2.3 Saving Tasks

Upon completing the exam, ensure that you save configuration files in the correct directory. You need to take screenshots of the procedure and the final result for eSight operations. For details, see the ***Exam Guidelines***.

3 Tasks

Figure 3-1 Network topology

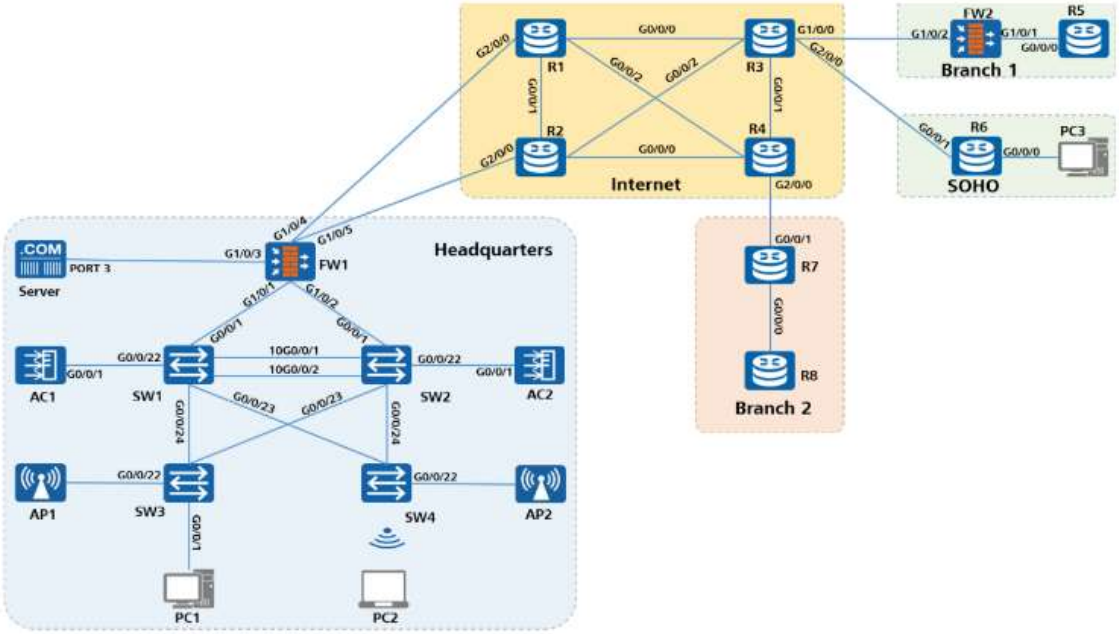

Table 3-1 IP address planning

Device Name	Interface	IP Address
R1	Loopback0	1.1.1.1/32
	G0/0/0	100.1.13.1/30
	G0/0/1	100.1.12.1/30
	G0/0/2	100.1.14.1/30
	G2/0/0	100.1.11.2/30
R2	Loopback0	2.2.2.2/32
	G0/0/0	100.1.24.1/30
	G0/0/1	100.1.12.2/30
	G0/0/2	100.1.23.1/30
	G2/0/0	100.1.22.2/30
R3	Loopback0	3.3.3.3/32

Device Name	Interface	IP Address
	G0/0/0	100.1.13.2/30
	G0/0/1	100.1.34.1/30
	G0/0/2	100.1.23.2/30
	G1/0/0	100.1.35.1/30
	Virtual-Template1	100.1.36.1/30
R4	Loopback0	4.4.4.4/32
	G0/0/0	100.1.24.2/30
	G0/0/1	100.1.34.2/30
	G0/0/2	100.1.14.2/30
	G2/0/0	100.1.47.1/30
R5	Loopback0	5.5.5.5/32
	Loopback1	172.17.30.1/32
	G0/0/0	172.16.25.2/30
R6	Loopback0	6.6.6.6/32
	G0/0/0	172.17.66.1/24
R7	G0/0/0	2002:6401:2F02:78::1/127
	G0/0/1	100.1.47.2/30
	Tunnel0/0/1	2002:6401:2F02::1/48
R8	Loopback0	2002:6401:2F02::8/128
	G0/0/0	2002:6401:2F02:78::2/127
SW1	Loopback0	9.9.9.9/32
	VLANIF 11	192.168.11.1/24
	VLANIF 13	172.16.13.1/30
	VLANIF 100	192.168.100.254/24
	VLANIF 101	192.168.101.254/24
	G0/0/1 (Layer 3)	IPv4: 172.16.11.2/30 IPv6: 2002:6401:B01:11::2/127
SW2	Loopback1	10.10.10.10/32
	VLANIF 24	IPv4: 172.16.24.1/30 IPv6: 2002:6401:B01:24::1/127

Device Name	Interface	IP Address
	G0/0/1 (Layer 3)	IPv4: 172.16.12.2/30 IPv6: 2002:6401:B01:22::2/127
SW3	Loopback0	11.11.11.11/32
	VLANIF 10	172.17.10.254/24
	VLANIF 13	172.16.13.2/30
SW4	Loopback0	12.12.12.12/32
	Loopback1	2002:6401:B01::4/128
	VLANIF 24	IPv4: 172.16.24.2/30 IPv6: 2002:6401:B01:24::2/127
FW1	Loopback0	13.13.13.13/32
	G1/0/1	IPv4: 172.16.11.1/30 IPv6: 2002:6401:B01:11::1/127
	G1/0/2	IPv4: 172.16.12.1/30 IPv6: 2002:6401:B01:22::1/127
	G1/0/3	172.17.100.1/24
	G1/0/4	100.1.11.1/30
	G1/0/5	100.1.22.1/30

	Tunnel1	172.16.15.1/30
	Tunnel2	172.16.26.1/30
	Tunnel3	2002:6401:B01::1/48
FW2	Loopback0	14.14.14.14/32
	G1/0/1	172.16.25.1/30
	G1/0/2	100.1.35.2/30
	Tunnel1	172.16.15.2/30
	Tunnel2	172.16.26.2/30
AC1	Loopback0	15.15.15.15/32
	VLANIF 11	192.168.11.2/24
AC2	Loopback0	16.16.16.16/32
	VLANIF 11	192.168.11.3/24
eSight	PORT3	172.17.100.2/24

Table 3-2 Device login information

Device	Management Address	User Name	Password
Router	None	admin	Huawei@ICT2019
Switch	None	admin	Huawei@ICT2019
AC	None	None	Huawei@ICT2019
AP	None	admin	admin@huawei.com
Firewall	https://192.168.0.1:8443	admin	Huawei@ICT2019
eSight	http://172.17.100.2:8080	admin	Huawei@ICT2019

Table 3-3 VLAN planning

Device Name	Interface	Link Type	VLAN Settings
SW1	G0/0/22	Trunk	PVID: 1 Allow-pass: VLAN 11
	Eth-trunk1	Trunk	PVID:1 Allow-pass: VLANs 13, 100, and 101
SW2	G0/0/22	Trunk	PVID: 1 Allow-pass: VLAN 11
	Eth-trunk2	Trunk	PVID: 1 Allow-pass: VLANs 24, 100, and 101
SW3	G0/0/1	Access	PVID: 10
	G0/0/22	Trunk	PVID: 101 Allow-pass: VLANs 100 and 101
	Eth-trunk1	Trunk	PVID: 1 Allow-pass: VLANs 13, 100, and 101
SW4	G0/0/1	Access	PVID: 20
	G0/0/22	Trunk	PVID: 101 Allow-pass: VLANs 100 and 101
	Eth-trunk2	Trunk	PVID: 1 Allow-pass: VLANs 24, 100, and 101

3.1 Task Contents

3.1.1 Device Connection

1. Configure network device names.
2. Connect devices according to the topology shown in **Figure 3-1**.

3.1.2 iStack (50 points)

1. Configure a stack of SW1 and SW2, and add 10GE0/0/1 and 10GE0/0/2 to the stack. Set up a stack system named **iStack** between the two switches.
2. Set the SW1 member ID to 0 and the priority to 200, and set the SW2 member ID to 1.

3.1.3 Link Aggregation (30 points)

1. Configure inter-device link aggregation between the links of **iStack** and SW3, and the links of **iStack** and SW4.
2. Configure MAD in relay mode on SW3 to avoid the impact of a stack split.

3.1.4 VLAN (20 points)

Configure VLANs on SW1 to SW4 according to **Figure 3-1**, **Table 3-1**, and **Table 3-3**.

3.1.5 IP Address Planning (10 points)

Configure interface IP addresses according to the **Table 3-1** IP address planning table.

3.1.6 DHCP (30 points)

1. Enable the DHCP server function on the stack system using the global address pool.
2. Set the name of the address pool to 1, and set the gateway address and DNS server address to 172.17.10.254 and 172.16.13.1 respectively. PC1 needs to dynamically obtain the IP address of VLAN 10 through the DHCP server.

3.1.7 Security Zone (30 points)

1. Add G1/0/1 and G1/0/2 on FW1 to the trust zone, G1/0/4 and G1/0/5 to the untrust zone, and G1/0/3 to the DMZ.
2. Add G1/0/1 on FW2 to the trust zone and G1/0/2 to the untrust zone.

3.1.8 Firewall Security Policy (200 points)

1. Connect FW1 to the Internet through two links, and configure two default routes on FW1 to access the Internet, implementing load balancing.
2. To implement fast convergence, bind the default route which the next hop is R1 with IP-link.

3. Configure a NAT policy in Easy IP mode and name it **outside**, to access the Internet from all devices at the headquarters, and the destination address of the NAT policy cannot be a private network address.
4. All routes on the Headquarters network must be reachable. Routes which are among in the Headquarters, two branches and SOHO must also be reachable.

   Traffic from a higher-priority security zone to a lower-priority zone must be allowed to pass. Only the security policies related to services and interconnection can be enabled on the firewall. The default interzone filtering policy of the firewall cannot be modified.

3.1.9 OSPF (60 points)

1. Run OSPF on devices according to the information provided in **Table 3-4**. The **network** command with the parameter that completely matches the 32-bit mask is configured.

Table 3-4 OSPF information

Device Name	Interface	Area ID
SW1	Loopback0	0
	G0/0/1	
	VLANIF 13	1
	VLANIF 101	
SW2	G0/0/1	0
	VLANIF 24	1
SW3	Loopback0	1
	VLANIF 10	
	VLANIF 13	
SW4	Loopback0	1
	VLANIF 24	
FW1	Loopback0	0
	G1/0/1	
	G1/0/2	
	G1/0/3	
	Virtual-template1	
FW2	Loopback0	0
	G1/0/1	
R5	Loopback0	0
	Loopback1	

Device Name	Interface	Area ID
	G0/0/0	

2. To reduce the scale of the LSDB in Area 1, set Area 1 as the stub area.
3. Disable SW3 from sending OSPF packets to PC1 through VLANIF 10.
4. To ensure campus network security, configure area authentication for all OSPF routers by using the MD5 authentication, and then set the authentication password to **Huawei@ICT2019**.

3.1.10 IS-IS (50 points)

1. Enable IS-IS on all interfaces and Loopback0 of R1, R2, R3, and R4 in the Internet area.

   The process ID is 1 and the area ID is 49.0001. The system ID of a router is 0000.0000.000*X* (*X* indicates the router number).

   For example, the system ID of R1 is 0000.0000.0001, and all routers are Level-2 routers.
2. Disable Internet routers from sending IS-IS packets to the firewall deployed at the enterprise border.
3. To ensure the security of the Internet area, configure authentication for all IS-IS routers except Hello packet, by using the MD5 authentication, and then set the authentication password to **Huawei@ICT2019**.
4. To speed up network convergence by allowing routers to quickly detect neighbor status changes, configure dynamic BFD. Set the minimum interval for sending and receiving packets to 500ms and the local detection multiplier to 4.

5. Enable IS-IS on AC1 (VLANIF 11 and Loopback0), AC2 (VLANIF 11 and Loopback0), and SW1 (VLANIF 11) at the Headquarters.

   The process ID is 1 and the area ID is 10. The system ID of a device is 0000.0000.00*XX* (*X* indicates the first number of the Loopback0 IP address). For example, the system ID of SW1 is 0000.0000.0009, and all devices are Level-2 devices.

3.1.11 WLAN (100 points)

3.1.11.1 DHCP

1. Configure SW1 as the DHCP server and configure a global address pool named **AP** to assign IP addresses to AP1 and AP2 in VLAN 101.
2. Configure SW1 as the DHCP server and configure a global address pool named **laptop** to assign an IP address to PC2 in VLAN 100. The DNS address is 114.114.114.114
3. Use the method of "Import route" to allow the PC1 to communicate with PC2.

Table 3-5 WLAN Data Planning

Item	Data
Management VLAN for APs	VLAN 101
Service VLAN for PC2	VLAN 100

Item	Data
Backup VLAN for ACs	VLAN 102
DHCP server	SW1 functions as the DHCP server to assign IP addresses for APs and PC2. AP gateway: 192.168.101.254/24 PC2 gateway: 192.168.100.254/24
AC source interface	VLANIF 11
Management IP address of AC1	VLANIF 11: 192.168.11.2/24
Management IP address of AC2	VLANIF 11: 192.168.11.3/24
Active AC (AC1)	Local priority: 0
Standby AC (AC2)	Local priority: 1
AC1 tunnel IP address and port number	IP address: VLANIF 102, 192.168.102.1/24 Port number: 10241
AC2 tunnel IP address and port number	IP address: VLANIF 102, 192.168.102.2/24 Port number: 10241
AP group	Name: **huawei** Reference profiles: VAP profile **huawei** and regulatory domain profile **huawei**
Regulatory domain profile	Name: **huawei** Country code: CN

3.1.11.2 HSB Between ACs

1. Configure HSB between ACs in dual-link mode.
2. AC2 backs up information from AC1 so that AC2 can immediately provide WLAN services if AC1 fails. Services will not be interrupted during the switchover.

3.1.11.3 Configuration and Delivery

1. Set up a wireless signal with SSID **Huawei-ICT@*X*** (X indicates the group name. For example, if the group name is China, the SSID is Huawei-ICT@China.)
2. Set the data forwarding mode to direct forwarding.

3.1.12 GRE, PPPoE, and IPsec VPN (200 points)

1. Establish two GRE tunnels between FW1 at the Headquarters and FW2 in Branch 1.

Use the public network outbound interface addresses as source and destination addresses of the GRE tunnels to implement the communication between the Headquarters and Branch 1.

2. HQs establishes SOHO branch due to service expansion. R3 as PPPoE server, dynamically assigns global IP address to PPPoE client (R6).

   Configure the global IP address pool so that the PPPoE server can dynamically assign IP addresses to R6. Configure a PPPoE user according to **Table 3-7 3-6** so that the PPPoE server can authenticate the user.

Table 3-6 PPPoE Information

Item	Data
PPPoE server	R3
PPPoE client	R6
IP pool	Name:1 Network:100.1.36.0/30 gateway: 100.1.36.1/30
PPPoE user	Username: huawei Password: Huawei@123

3. SOHO employees need to access the server at the Headquarters. Because data transmitted over the Internet is insecure and the server information is confidential, use the **Template** to establish an IPsec tunnel according to **Table 3-7 3-7** to encrypt the traffic from PC3 to the Headquarters server.

Table 3-7 IPsec Information

Device	IPsec Configuration	
FW1 R6	Peer address: public network outbound interface address Authentication mode: pre-shared key authentication Pre-shared key: **huawei** Local ID type: IP Remote ID type: any	
	IPsec policy	Name: map1 Mode: isakmp
	Ike peer	Name: 1
	Ike proposal	Name: 1 Encryption algorithm: 3DES Authentication algorithm: SHA1

	IPsec proposal	Name: 1 Security proposal: ESP Encapsulation mode: tunnel encapsulation Encryption algorithm: 3DES Authentication algorithm: SHA1

3.1.13 BGP and Route Policy (50 points)

1. FW1 and SW1 use Loopback0 as the update source to establish an IBGP peer relationship, and the AS number is 64512.

   FW2 and R5 in Branch 1 use Loopback0 as the update source to establish an IBGP peer relationship, and the AS number is 64513.
2. Establish EBGP peer relationships between FW1 and FW2 through tunnel 1 and tunnel 2, respectively.
3. Run the **network** commands to enable FW1 to learn the Loopback0 route of FW2, and the Loopback0, Loopback1 routes of R5.
4. Use the method of "Import route" to allow the Headquarters to communicate with Branch 1.
5. Use the **MED** attribute on FW1 to configure a route policy so that the traffic from Branch 1 to the Headquarters (172.17.10.0/24) is preferentially forwarded to G1/0/5 on FW1.

   Requirement: Examinees must use ip-prefix to match routes.

3.1.14 IPv6, 6to4 and OSPFv3 (120 points)

1. Establish a 6to4 tunnel between FW1 and R7.
2. Run OSPFv3 on SW1 (G0/0/1), SW2 (VLANIF 24 and G0/0/1), SW4 (Loopback1 and VLANIF 24), FW1 (G1/0/1, G1/0/2). The process ID is 1 and the area ID is 0. The router ID of a device is the Loopback0 IP address. For example, the router ID of FW1 is 13.13.13.13.
3. Run OSPFv3 between R7 (G0/0/0) and R8 (G0/0/0 and Loopback0). The process ID is 1 and the area ID is 1. In this case, Loopback0 on R8 in Branch 2 can communicate with Loopback1 on SW4 at the Headquarters.

3.1.15 SNMP and eSight (50 points)

1. Configure SNMPv2c on devices, and set the read community name and write community name to **Admin@123** and **Huawei@123**, respectively.
2. Create subnet **Huawei-ICT** on eSight.
3. Create an SNMP template on eSight.
4. Use SNMP on eSight to discover devices (SW1, SW2, SW3, SW4, AC1, AC2, FW1, FW2, R5) one by one and generate a network topology.

Requirement of screenshot

1. Create a subnet Huawei-ICT on the eSight server, screenshot, save it and name it **1-1-subnet**.

2. The eSight server monitors the network topology, screenshot, save and names it as **1-2-network topology**.