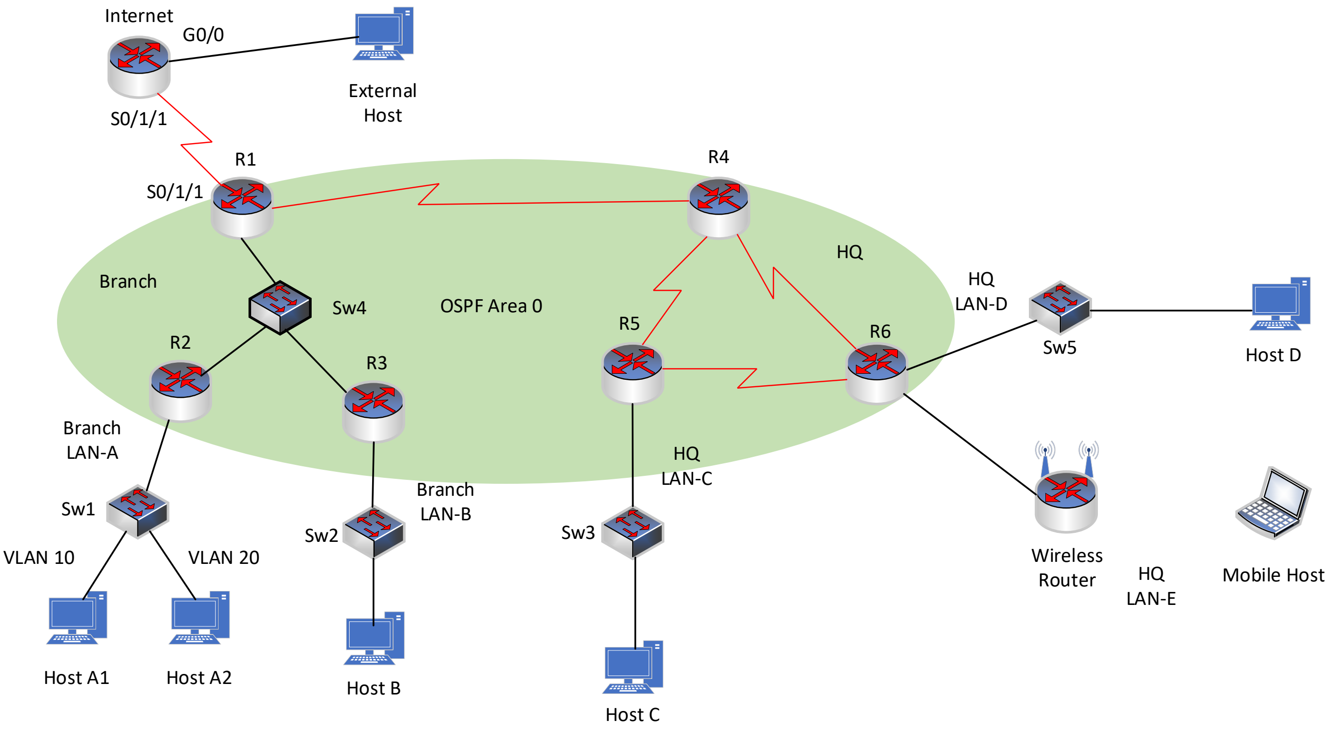
31277 Case Study Instructions

Topology



Addressing Table

Device Name	Interface/Default Gateway	IP address/prefix
Internet	G0/0	138.25.88.85/30
	S0/1/1	209.165.200.1/30
R1	G0/0	
	S0/1/0	
	S0/1/1	209.165.200.2/30
R2	G0/0.10	
	G0/0.20	
	G0/0.99	
	G0/1	
R3	G0/0	
	G0/1	

Device Name	Interface/Default Gateway	IP address/prefix
R4	S0/1/0	
	S0/1/1	
	S0/0/0	
R5	G0/0	
	S0/1/0	
	S0/1/1	
R6	G0/0	
	G0/1	
	S0/1/0	
	S0/1/1	
Sw1	VLAN 99	
	Default Gateway	
Host A1	NIC VLAN 10	DHCP
Host A2	NIC VLAN 20	
	Default Gateway	
Host B	NIC	
	Default Gateway	
Host C	NIC	DHCP
Host D	NIC	
	Default Gateway	
Mobile Host	Wireless NIC	DHCP
External Host	NIC	138.25.88.86/30

Introduction

You will practice and be assessed on the following skills:

- VLSM IP addressing
- Basic device configurations
- Configuration of static routing
- Configuration of OSPFv2 routing
- Customization of OSPF.
- Configuration of VLAN and Inter-VLAN routing
- Configuration of DHCP
- Configuration of WLAN
- Configuration of static NAT.

- Configuration of dynamic NAT with PAT.
- Configuration of various types of ACLs.

Instructions

Part 1: VLSM IP addressing

a. Use the IP address range 192.168.0.0/24 for Branch and 172.10.0.0/24 for HQ. Left hand side of the internal network is Branch, right hand side of the internal network is HQ.

b. Design the addresses for all internal subnets with VLSM, conserve as much addresses as possible. Number of hosts in each LANs are as follows:

- Branch LAN-A: VLAN 10: 25 hosts
- Branch LAN-A: VLAN 20: 35 hosts
- Branch LAN-A: VLAN 99: 4 hosts
- Branch LAN-B: 4 hosts
- HQ LAN-C: 10 hosts
- HQ LAN-D: 100 hosts

Note: WAN links should be considered when you design your IP addressing. WAN links between Branch and HQ can use either Branch or HQ’s address range. Wireless Router uses static IP address for the Internet port to R6.

Note: Follow the WLAN part for the HQ LAN-E addresses design.

c. Assign the first valid host address in each subnet to the Default Gateway.

d. Assign the 2nd valid host address in each subnet to the Host PC or Switch.

e. Some IP addresses that are pre-defined or marked as DHCP. Enter the IP addresses in your design to blanks the IP address table above.

Part 2: Construct the network

Step 1: Basics.

a. Choose suitable routers, switches and end devices, add interfaces to the devices if needed.

b. Cable the devices.

c. Configure device name.

d. Configure IP addresses on the interfaces following the IP addressing table. Configure default gateway where needed.

Note: Some interfaces should be changed to obtain IP address from DHCP after implementing DHCP.

e. Disable DNS lookup on the routers.

Step 2: Configure Routers (R1, R2, and R3) on Branch

a. Assign class as the privileged EXEC encrypted password.

b. Assign cisco as console password, enable login and enable synchronization with the debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

c. Assign cisco as vty password, enable login and enable synchronization with the debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

d. Encrypt the clear text passwords.

e. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

f. Enable SSH on R3, create a user with username admin and secret adminpass.

Part 3: Configure Static Routing to and from Internet

Configure static routing between Internet and R1 with the next hop IP address. Ensure ALL internal addresses (including translated) are routed.

Note: your static routing may need to be revised after implementing NAT.

Part 4: Configure OSPF

Step 1: Activate OSPF.

Use process ID **10** for OSPF activation on all routers.

a. Activate OSPF by configuring the interfaces of the network devices in the Branch and HQ networks, where required.

b. Activate OSPF using network statements and inverse masks on the routers.

Step 2: Configure router IDs.

Configure router IDs on the multiaccess network routers as follows:

R1: 9.9.9.9

R2: 8.8.8.8

R3: 7.7.7.7

You will need to restart the OSPF process after changing the router IDs.

Step 3: Customise OSPF operation.

a. Configure router R1 with the highest OSPF interface priority so that it will always be the designated router of the multiaccess network.

b. On router R1, configure a default route to the Internet with the next hop IP address.

c. Automatically distribute the default route to all routers in the network.

d. Configure OSPF so that routing updates are not sent into networks where OSPF updates are not required.

Part 5: Configure VLAN and Inter-VLAN Routing

Step 1: Configure VLANs on Sw1

a. Configure VLANs: VLAN 10, 20 and 99, with names, students, staff and management respectively

b. Configure trunk link to allow eligible VLANs and with native VLAN 99.

c. Assign access ports to VLAN 10 and 20, design your own VLAN and interfaces mapping. Describe your design in your report.

Step 2: Configure Inter-VLAN Routing on R2

a. Configure subinterfaces.

b. Assign IP addresses to the subinterfaces according to your design in Part 1.

c. Use the VLAN number as the subinterface ID

Part 6: Configure NAT

In this part of the skills assessment, you will configure static and dynamic NAT at the network edge.

Step 1: Configure static NAT

Configure static NAT to translate the address of the Host D on HQ LAN D to the External Host using the public address **209.165.200.228**. Verify that the translations are occurring.

Step 2: Configure dynamic PAT.

a. Create access list **1** to allow all addresses in the networks in Branch LAN-A, including VLAN 10 and VLAN 20.

b. Create a NAT pool named **POOL-1**. It should use address in the range **209.165.200.226-209.165.200.227**.

c. Configure NAT to dynamically use the addresses in the pool for all traffic entering and exiting the company network. Remember that it is likely that more than three hosts will be accessing traffic on the Internet. Verify that the translations are occurring.

Part 7: Configure ACLs

Configure access control lists to meet the following requirements. All ACLs should be placed in the most efficient location possible according to the guidelines specified in the curriculum.

a. Create a named standard access list to explicitly prevent all external traffic accessing the SSH lines on R3. Name the list **VTY-BLOCK.** All addresses on the Branch LAN-B network only should be allowed to access the VTY lines.

b. Create a numbered standard ACL to prevent all hosts on HQ LAN-D from accessing HQ LAN-C. Use **10** as the number for the list.

Part 8: Configure DHCP

Step 1: Configure R4 as DHCP server

a. Configure a DHCP address pool for Branch LAN-A VLAN 10, with the addresses designed in Part 1, use pool name POOL_LAV10, exclude the first 5 valid host addresses, set Host A as obtaining address from DHCP.

b. Configure a DHCP address pool for HQ LAN-C, with the addresses designed in Part 1, use pool name POOL_LC, exclude the first 5 valid host addresses, set Host C as obtaining address from DHCP.

Step 2: Configure DHCP relay agent

a. Choose the routers that can should be the DHCP relay agents for Branch LAN-A VLAN 10 and HQ LAN-C.

b. Configure DHCP relay agents to forward all DHCP requests to the R4 DHCP server. Choose the suitable interfaces for Branch LAN-A VLAN 10 and HQ LAN-C to configure the IP helper addresses.

Part 9: Configure WLAN

Step 1: Configure Internet Port (Port to R6)

Configure the Internet port of the Wireless Router following the IP addresses designed in Part 1.

Step 2: Configure DHCP on Wireless Router

a. Use the DHCP pool 192.168.1.0/24, excluding the first 5 host addresses.

b. Use the first valid host address as the Default Gateway.

c. Set the maximum number of users as 100.

Step 3: Configure Wireless basics and security

a. Configure the Wireless SSID to LANE for only 2.4GHz

b. Use WPA2 for the security mode

c. AES for the encryption method

d. Use password cisco. You can choose another password, please note it in your report

e. Configure the Mobile host to connect to Wireless Router

Part 10: Test Connectivity and troubleshoot

Test connectivity and troubleshoot if needed. Save the file in .pkt file.

Report:

Report should include the following sections:

- Problem Statement, define the engineering problem that needs to be addressed
- Project Task Allocation: Task allocation for each member in the group
- Project Weekly schedule and completion: Project plan (weekly) and completion in each week
- Project Design and Implementation: Design ideas and considerations, design details in your implementations, do NOT include screenshots of your configurations as they can been seen from your packet tracer model
- Discussion and Troubleshooting: Problems that you have encountered in the project and the solutions you used to solve them

Marking criteria:

Criteria	Pts:10
Report: Problem Statement	1 pts
Report: Project Task Allocation	1 pts
Report: Project Weekly schedule and completion	1 pts
Report: Project Design and Implementation	1 pts
Report: Discussions and Troubleshooting	1 pts
PT: Part 1 IP addressing	0.5 pts
PT: Part 2 Network model and connections	0.5 pts
PT: Part 3 Static Routing	0.5 pts
PT: Part 4 OSPF	0.5 pts

PT: Part 5 VLAN and Inter-VLAN Routing	0.5 pts
PT: Part 6 NAT	0.5 pts
PT: Part 7 ACL	0.5 pts
PT: Part 8 DHCP	0.5 pts
PT: Part 9 WLAN	0.5 pts
PT: Part 10 Connectivity	0.5 pts