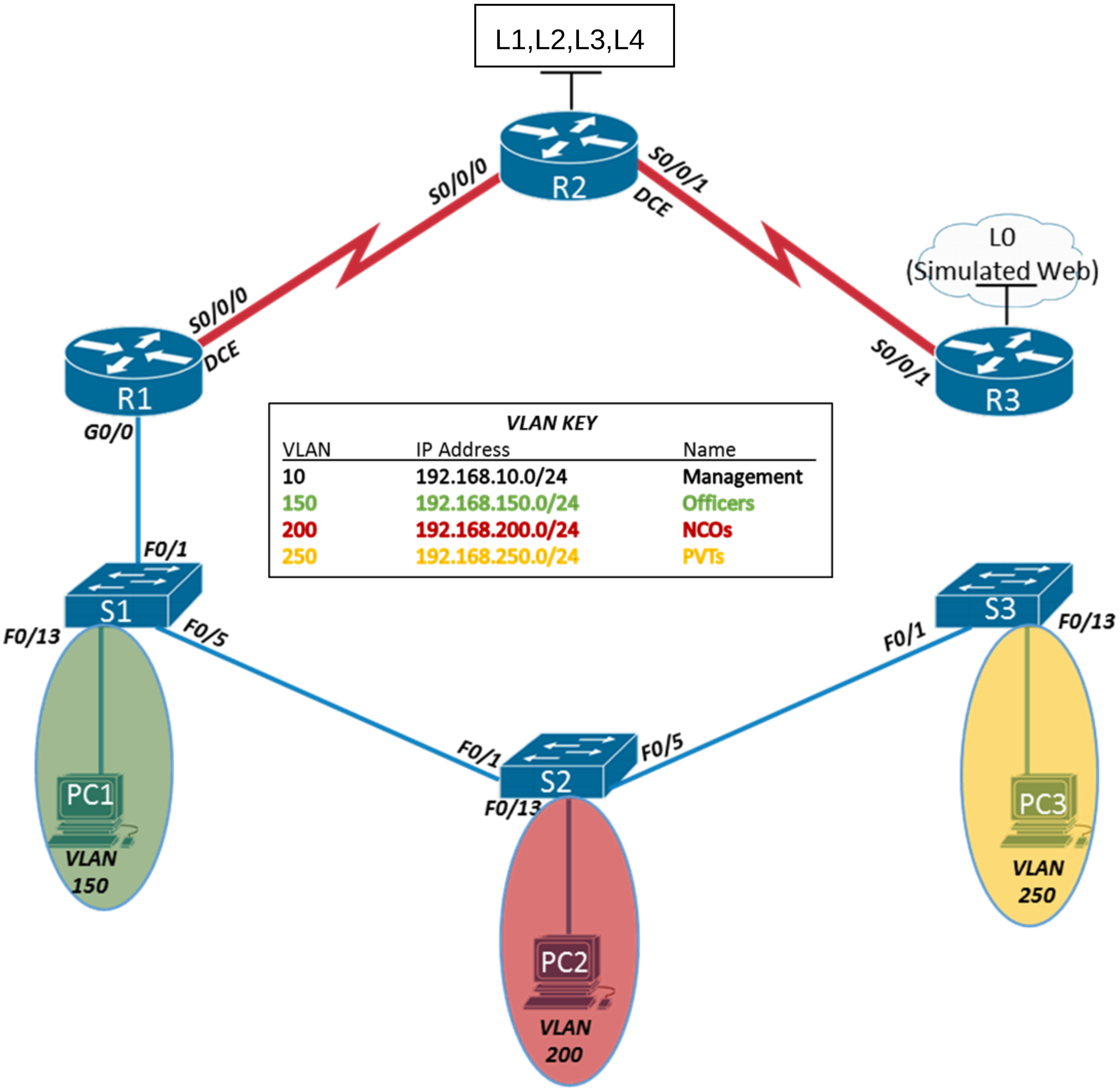
Version A

Semester 2: Practice Hands-on Exam

TOPOLOGY:



VLAN KEY

VLAN	IP Address	Name
10	192.168.10.0/24	Management
150	192.168.150.0/24	Officers
200	192.168.200.0/24	NCOs
250	192.168.250.0/24	PVTs

ADDRESSING TABLE:

Device	*Interface*	*IP Address*	*Subnet Mask*	*Default Gateway*
R1	S0/0/0	10.123.12.1	255.255.255.252	N/A
	S0/0/0	2001:ACAD:CAFE:12::1	/64	N/A
	G0/0	N/A	N/A	N/A
	G0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0.150	192.168.150.1	255.255.255.0	N/A
	G0/0.200	192.168.200.1	255.255.255.0	N/A
	G0/0.250	192.168.250.1	255.255.255.0	N/A
R2	S0/0/0	10.123.12.2	255.255.255.252	N/A
	S0/0/0	2001:ACAD:CAFE:12::2	/64	N/A
	S0/0/1	10.123.23.1	255.255.255.252	N/A
	S0/0/1	2001:ACAD:CAFE:23::1	/64	N/A
	Loopback1	172.16.10.1	255.255.255.0	N/A
	Loopback2	172.16.20.1	255.255.255.0	N/A
	Loopback3	172.16.30.1	255.255.255.0	N/A
	Loopback4	2001:ACAD:CAFE:2::1	/64	N/A
R3	S0/0/1	10.123.23.2	255.255.255.252	N/A
	S0/0/1	2001:ACAD:CAFE:23::2	/64	N/A
	Loopback0	3.3.3.3	255.255.255.255	N/A
	Loopback0	3::3	/128	N/A
S1	VLAN10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN10	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN10	192.168.10.13	255.255.255.0	192.168.10.1
PC1	NIC	192.168.150.10	255.255.255.0	192.168.150.1
PC2	NIC	Configured via DHCP	Configured via DHCP	Configured via DHCP
PC3	NIC	Configured via DHCP	Configured via DHCP	Configured via DHCP

---

1) **Connect all devices per the topology diagram:**

   a) Use correct cables (Assume MDIX is not in use).

2) **Configure basic security parameters for R1, R2 and R3:**

b) Configure the hostname as applicable (reference the topology)

c) Disable DNS lookup

d) Set the domain to CCNA-SEM2.com

e) Set an encrypted priv. exec. password to ccnaenpass

f) Set the console password to ccnacon

g) Set the VTY telnet password to ccnavty

h) Create a MOTD banner stating “Unauthorized access is prohibited”

i) Encrypt all clear text passwords

3) **Configure basic security parameters for S1, S2, and S3:**

a) Configure the hostnames as applicable (reference the topology)

b) Disable DNS lookup

c) Set the domain to CCNA-SEM2.com

d) Set an encrypted priv. exec. password to ccnaenpass

e) Set the console password to ccnacon

f) Set the VTY telnet password to ccnavty

g) Create a MOTD banner stating “Unauthorized access is prohibited”

h) Encrypt all clear text passwords

4) **Configure the Layer 3 interfaces for R1, R2 and R3:**

a) Set the IPv4 and IPv6 addresses for serial interfaces 0/0/0 on R1. Add an interface description indicating which router it connects to. Ensure the interface is activated.

b) Set the IPv4 and IPv6 addresses for serial interfaces 0/0/0 and 0/0/1 on R2. Add interface descriptions indicating which routers they connects to. Also, configure IPv4 and IPv6 addresses for loopback interfaces. Ensure the interface is activated.

c) Set the IPv4 and IPv6 addresses for serial interface 0/0/1 on R3. Add an interface description indicating which router it connects to. Ensure the interface is activated.

d) Set the IPv4 and IPv6 addresses and subnet mask for loopback interfaces on R2 and R3

5) **Configure the Layer 3 interfaces for S1, S2, and S3:**

a) Create the VLAN databases in all switches, adding the VLANs listed in the VLAN KEY.

b) Set the IPv4 address and subnet mask for the management VLAN (10). Ensure the VLAN interface is active.

c) Assign a default gateway for the switches (the gateway is R1’s management VLAN IP address).

d) VLAN 1 will be the native VLAN for all trunk ports. Configure unconditional (forced) trunk on the interfaces connecting switches to switches, and from switch to router.

e) Assign the PC-connected ports to the proper VLANs. Configure PC-connected ports with port security.

   i. Maximum number of MAC’s: 3
   ii. Configure sticky MAC learning

f) Configure all other ports as access ports and shutdown all unused ports.

6) **Configure the Layer 3 sub-interfaces for R1:**

a) Activate G0/0 interface on R1.

b) Create sub-interfaces on G0/0 for all VLANs (see addressing table).

c) Set the 802.1Q encapsulation for the sub-interfaces.

d) Set the IPv4 address and subnet mask for each sub-interface. Add an interface description indicating which VLAN it connects to.

7) **Configure RIPv2 routing protocol:**

a) Configure RIPv2 on R1. Advertise the appropriate connected networks. Set the appropriate interfaces to passive. Disable auto-summarization.

b) Configure RIPv2 on R2. Advertise the appropriate connected networks. Set the appropriate interfaces to passive (including loopbacks). Disable auto-summarization.

c) Configure RIPv2 on R3. Advertise the appropriate connected network. Do NOT advertise Loopback0 network. Set the appropriate interface to passive. Disable auto-summarization.

8) **Configure Default Routes**

a) Enable IPv6 routing.

b) Configure both an IPv4 and an IPv6 default route from R1 leaving S0/0/0 towards R2.

c) Configure both an IPv4 and an IPv6 default route from R2 leaving S0/0/1 towards R3;

d) Configure a static route on R2 (used for NAT) for net 209.165.0.0/16, exit interface of S0/0/0 towards R1.

e) Configure both an IPv4 and an IPv6 default route from R3 leaving Loopback0 to the simulated web.

f) Configure an IPv4 static route on R3 (used for NAT) for net 209.165.0.0/16, exit interface of S0/0/1 towards R2.

g) Configure a IPv6 static route on R3, for net 2001:ACAD:CAFE/48, exit interface S0/0/1 towards R2.

9) **Verify Layer 3 Connectivity**

a) Verify that PC1 can ping all sub-interfaces and all loopback interfaces (except IPv6 loopbacks).

10) **Implement DHCP**

a) Reserve the first 10 IP addresses in all VLANs for static configurations.

b) Configure R1 as the DHCP server for VLANs 150, 200, and 250.

iii. Create the DHCP pool for VLAN 150-

- DNS-server: 209.244.0.3 209.244.0.4
- Domain-name: CISCO-LAB150.COM
- Network: (see VLAN key)
- Default Gateway: (see addressing table)

iv. Create the DHCP pool for vlan 200-

- DNS-server: 209.244.0.3 209.244.0.4
- Domain-name: CISCO-LAB200.COM
- Network: (see VLAN key)
- Default Gateway: (see addressing table)

v. Create DHCP pool for VLAN 250:

- DNS-server: 209.244.0.3 209.244.0.4
- Domain-name: CISCO-LAB250.COM
- Network: (see VLAN key)
- Default Gateway: (see addressing table)

vi. Verify that both PC's receive a DHCP assigned IP address in the correct vlan.

11) <u>Implement NAT</u>

a) Configure Static NAT

i. On R1, configure static NAT to map the inside local IP address for PC1 to an Inside Global address of 209.165.150.254.

ii. On R1, define the inside and outside NAT interfaces for VLAN 150

b) Configure Dynamic NAT

iii. On R1, create an access control list named ACCESS-LIST250 to permit VLAN 250 for dynamic NAT.

iv. On R1, create a NAT pool named NAT-POOL250 using addresses 209.165.250.100-103/24.

v. On R1, configure NAT to use the inside source list and outside pool. Allow multiple PCs access to these few Inside Global address.

vi. On R1, define the inside and outside NAT interfaces for VLAN 250.

12) <u>Configure NTP</u>

a) Set the clock on R1 to a date and time specified for 31 December 2017, 11:59pm

b) Configure R1 as the NTP Master with a stratum of 3.

c) Configure R2 and R3 so that they use R1 as their NTP Server.

13) <u>Configure Syslog</u>

a) Enable the timestamp service on R1, R2, and R3 for system logging purposes (include milliseconds).

b) Enable logging of messages on R1, R2, and R3 to PC1 (syslog server). Ensure that routers are configured to send log messages to correct IP address (IP address may be translated via NAT).

c) Change message trapping level on R1, R2, and R3 to debugging.

14) <u>Configure Access-Lists</u>

a) Configure a standard named access-list to block PC1 from reaching R3 (ensure you enable http services on R3). The ACL name should be PC1_BLOCK.

b) Apply the access-list to the appropriate interface.

c) Verify the access-list is blocking traffic from PC1 to R3.

d) Configure a standard, named access-list to allow only R1 to telnet to R3. The ACL name should be ADMIN_MGMT.

e) Apply the access-list to the appropriate router's vty lines.

f) Verify the access-list is working as expected.

COMMAND REFERENCE:

1) Command that displays only RIPv2 routes (not the running-config)?

____

2) Command that displays the default admin distance for RIPv2 routers?

____

3) Command that displays current active NAT translations?

____

4) Command that displays configured DHCP pools?

____

5) Command that displays the date and time?

____

6) Command that displays port security settings for a specific port?

____

7) Command that displays all configured access lists?

____

8) Command to reset access list counters?

____