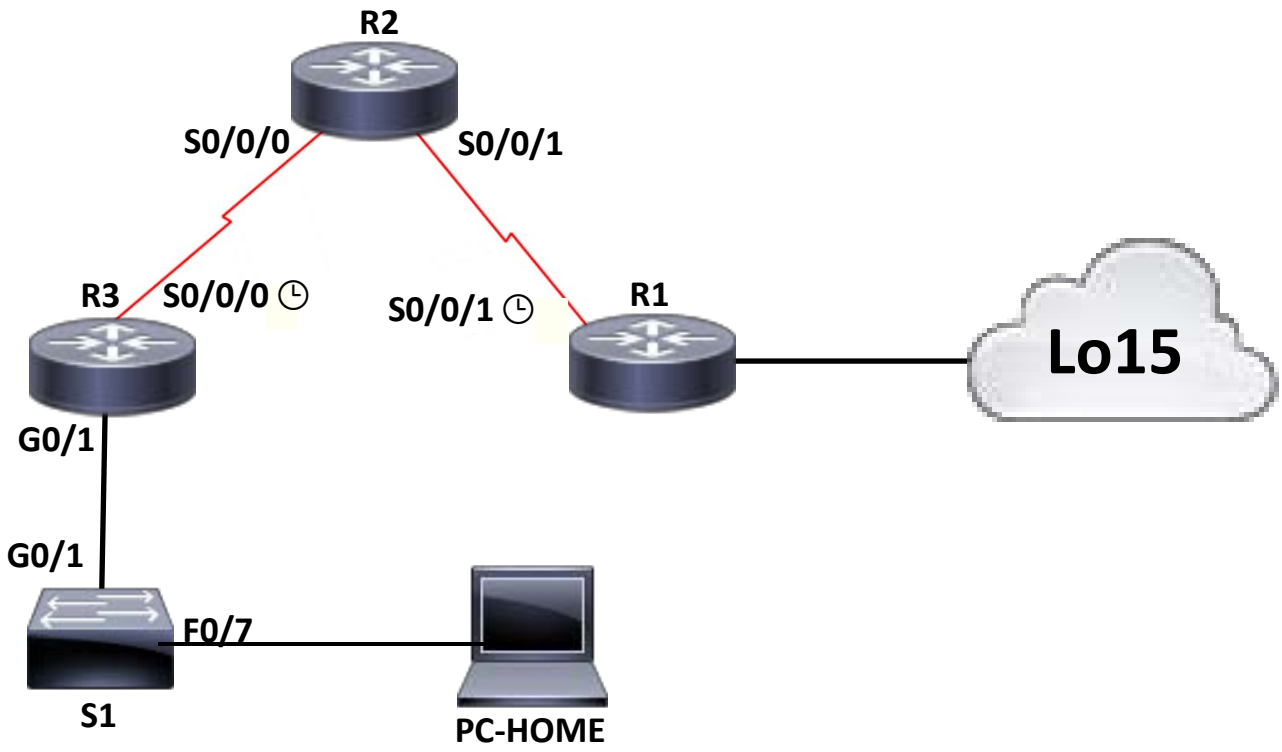
RSE Skills Review 2.1



Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway
R1	S0/0/1	172.20.5.1	255.255.255.252	N/A
	Lo15	200.56.53.129	255.255.255.128	N/A
R2	S0/0/0	172.20.5.5	255.255.255.252	N/A
	S0/0/1	172.20.5.2	255.255.255.252	N/A
R3	S0/0/0	172.20.5.6	255.255.255.252	N/A
	G0/1.10	192.168.0.254	255.255.255.0	N/A
	G0/1.20	192.168.1.254	255.255.255.0	N/A
	G0/1.30	192.168.2.254	255.255.255.0	N/A
	G0/1.75	192.168.3.254	255.255.255.0	N/A
	G0/1.99	192.168.99.254	255.255.255.0	N/A
S1	VLAN 10	192.168.0.200	255.255.255.0	
	VLAN 20	192.168.1.200	255.255.255.0	
	VLAN 30	192.168.2.200	255.255.255.0	
	VLAN 75	192.168.3.200	255.255.255.0	
	VLAN 99	192.168.99.200	255.255.255.0	
PC-HOME	NIC	DHCP	DHCP	DHCP

VLAN Port Assignment and DHCP Information

Device	Ports	VLAN Numbers	VLAN Name	Network
S1	F0/15-23	VLAN 10	Teachers	192.168.0.0/24
	F0/1-10	VLAN 20	Students	192.168.1.0/24
	F0/11-12	VLAN 30	Admin	192.168.2.0/24
	F0/13-14	VLAN 75	IT	192.168.3.0/24
		VLAN 99	Management	192.168.99.0/24

Scenario

In this activity, you will configure VLANs, trunks, DHCP, NAT, ACLs, static routes, and OSPFv2.

Requirements

Using the information in the topology and the tables above, implement the following requirements:

S1

- Disable DNS lookup
- Assign **class** as the privileged EXEC mode password
- Assign **cisco** as the console and VTY password
- Enable Telnet access only on VTY line
- Encrypt all clear text passwords in current running configuration
- Disable CDP globally
- Create a banner stating “This is a Switch”
- Configure, name, and assign VLANs
- Configure trunking
- Set the default gateway with VLAN 99
- Configure all other ports as access ports
- Disable All unused Ports

R3

- Disable DNS lookup
- Assign **class** as the privileged EXEC mode password
- Assign **cisco** as the console and vty password
- Set a MOTD banner to “This is router three”
- Configure SSH
    - Domain-Name: RSEREVIEW.com
    - Create a username of **Hank** with an encrypted password of **cisco**
- Enable only SSH access on VTY line
- Encrypt all plain text passwords
- Configure Inter-Vlan Routing and Set Appropriate Descriptions
- Apply IP addresses according to the Addressing Table
    - Use a clock rate of 128000 on DCE interface
- Configure Single-Area OSPFv2
    - Process ID 1
    - Area 50
    - Router ID: 3.3.3.3
    - Advertise all networks configured
    - Do not send OSPF updates out appropriate interfaces
- Create a Standard Named ACL "NO_ACCESS" blocking Students VLAN from accessing the Teachers VLAN. Allow everything else.
- Apply ACL NO_ACCESS on the interface closest to the destination
- Create an ACL numbered 50 allowing only the IT VLAN to access the 192.168.2.0/24 network
- Apply ACL 50 on the interface closest to the destination
- Disable CDP on the interface G0/0
- Set up DHCP for VLAN 20
    - Pool Name: Students
    - Domain Name: RSE.com
    - DNS Server: 8.8.4.4
    - Exclude the Last 10 Usable
- Allow only the PC to connect via VTY using ACL 75

R2

- Disable DNS lookup
- Assign **class** as the privileged EXEC mode password
- Assign **cisco** as the console and vty password
- Set a MOTD banner to "This is router two"
- Configure SSH
  - Domain-Name: RSEREVIEW.com
  - Create a username of **Hank** with an encrypted password of **cisco**
- Enable only SSH access on VTY line
- Apply IP addresses according to the Addressing Table
- Configure Single-Area OSPFv2
  - Process ID 1
  - Area 50
  - Router ID: 2.2.2.2
  - Advertise all networks configured
- Set the time and date

R1

- Disable DNS lookup
- Assign **class** as the privileged EXEC mode password
- Assign **cisco** as the console and vty password
- Set a MOTD banner to "This is router one"
- Configure SSH
  - Domain-Name: RSEREVIEW.com
  - Create a username of **Hank** with an encrypted password of **cisco**
- Enable only SSH access on VTY line
- Apply IP addresses according to the Addressing Table
  - Use a clock rate OF 128000 on DCE interface
- Configure a default route out of Lo15
- Configure Single-Area OSPFv2
  - Process ID 1
  - Area 50
  - Router ID: 1.1.1.1
  - Advertise all networks configured **Except** the Lo15 network
  - Propagate Default Route
  - Make Lo15 a passive interface
- Configure NAT
  - Configure a standard ACL numbered 15 to allow only the IP address within the 192.168.0.0/22 network
  - Configure NAT overload with a pool named PUBLIC with the following range of public IP addresses: 200.56.53.200 to 200.56.53.250 with a CIDR of /25
  - Apply to the correct NAT interfaces
- Verify Connectivity
  - From the PC Ping Lo15 IP Address 200.56.53.129