
# Seattle Cisco Users Group

***CCNA Lab Project 2***

**Initial Configuration Tasks**

1. Device host names: Configure Hostnames as Follows
    a. Routers: RX (X=Site Number)
    b. Switches: SWX (X=Site Number)
    c. Internet Router, Site 3: R4
2. Device access
    a. Console Access
        - Create login process to go directly to privileged mode
        - Password cisco
        - No requirement to enter a password to access
    b. AUX Access (router only)
        - Create login process to enter exec mode
        - Password cisco
        - Login required
    c. VTY Access
        - Create login process to enter exec mode
        - Password cisco
        - Login required
3. Basic security settings
    a. Set enable secret password (cisco)
    b. Prevent telnet access from outside the network
4. Other basic settings
    a. Set clocks on all devices to Pacific Time
    b. Disable devices using DNS lookups
    c. Disable web-based access on all devices.
    d. Set login message to "Welcome to the CCNA Metro-E Lab!"
    e. Set all devices to update their clocks based on the time configured on R4

**Local Device Interface Configuration Tasks**

1. VLAN interfaces
    a. Management VLAN
        - Set VLAN ID to X (X=Site Number)
        - Create IP addressing to allow for 5 Hosts
    b. Production VLAN
        - Set VLAN ID to XX (X=Site Number)
        - Create IP addressing to allow for 20 Hosts
    c. Internet VLAN (Providing Internet Access by Ethernet to all Sites)

        - Set VLAN ID to 99
        - Create IP addressing to allow for 15 Hosts
2. Loopback interfaces
    a. Create loopback interfaces on each router.
    b. Assign IP subnet for a single host: 10.Y.Y.Y (Y=device number)
3. Metro-Ethernet WAN Interfaces
    a. Create Subinterfaces using Site numbers as reference (e.g., Fast Ethernet 0/0.1 for Site 1)
    b. Specify 802.1Q Encapsulation and Assign to VLAN 123
    c. Assign IP addresses per diagram, with 12 hosts per subnet.
4. Internet WAN Interfaces
    a. Create Interface for VLAN 99
    b. Use Dot1Q Encapsulation
    c. Do not supply any Internet addresses but allow DHCP to assign them
5. DHCP Configuration
    a. Enable DHCP on R4 to supply Internet IP addressing to R1,R2, R3 on VLAN99
    b. Identify the following parameters:
        - Network
        - Default Gateway
        - DNS (use 216.145.1.2 and 216.145.1.3)
5. GRE Interfaces
    a. Create Tunnel Interfaces between R1,R2,R3
    b. Assign IP addresses per diagram, with 5 hosts per subnet

**Routing Protocol Configuration Tasks**

1. OSPF configuration
    a. Configure OSPF on R1
        - Place the Metro Ethernet interface in area 0
        - Place all local VLAN interfaces and the loopback interface in area 1
        - Use loopback interface as router-id
    b. Configure OSPF on R2
        - Place the Metro Ethernet interface in area 0
        - Place all local VLAN interfaces and the loopback interface in area 2
        - Use loopback interface as router-id
    c. Configure OSPF on R3
        - Place the Metro Ethernet interface in area 0
        - Place all local VLAN interfaces and the loopback interface in area 2
        - Configure loopback in area 0
        - Use loopback interface as router-id
2. EIGRP configuration
    a. Configure EIGRP on R1

        - Use AS Number 111
        - Enable EIGRP on GRE Tunnels
        - Disable auto summarization
    b. Configure EIGRP on R3
        - Use AS Number 111
        - Enable EIGRP on GRE Tunnels
        - Disable auto summarization
3. Redistribution and tuning
    a. Do not redistribute EIGRP or OSPF
    b. Configure EIGRP to Perform Backup Routing upon Failure of the Metro Ethernet Service
    c. Do not configure any static routes to accomplish this task
4. Verifying full reachability
    a. Ping all other devices in the network from each device.
    b. Successfully telnet to all devices in the network from each device.

**Network Address Translation Tasks**

1. Configure Port Address Translation/Overloading on R1,R2, & R3 on the Internet Interface
2. Configure static NAT for inbound web traffic on R2, using VLAN 22 IP 192.168.22.4

**Security Configuration**

1. Create and apply an access that will only allow internal devices to access the management VLAN on all devices at each site.
2. Prevent web access to R1
3. Block SNMP access to all devices
4. Block all external access trying to reach the management VLAN