Seattle Cisco Users Group

CCNA Lab Project 3

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 Cisco123
        - No requirement to enter a password to access
    b. AUX Access (router only)
        - Create login process to enter exec mode
        - Password Cisco123
        - Login required
    c. VTY Access
        - Create login process to enter exec mode
        - Password Cisco123
        - Login required
3. Basic security settings
    a. Set enable secret password (Cisco123)
    b. Prevent telnet access from outside the network
    c. Allow SSH access from outside the network
4. Other basic settings
    a. Set clocks on all devices to Pacific Time, including Daylight Savings Time settings
    b. Disable devices using DNS lookups
    c. Enable web-based access on all devices and set to port 8080
    d. Set login message to “Welcome to the CCNA VPN 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 (R1/R2/R3 Only)
        - Set VLAN ID to X (X=Site Number)
        - Use ISL encapsulation
        - Create IP addressing to allow for 4 Hosts
    b. Production VLAN (R1/R2/R3 Only)

        - Set VLAN ID to XX (X=Site Number)
        - Use ISL encapsulation
        - Create IP addressing to allow for 32 Hosts
    c. Internet VLAN (Providing Internet Access by Ethernet to all Sites)
        - Set VLAN ID to 99
        - Create IP addressing to allow for 4 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. Internet WAN Interfaces
    a. Create Interfaces for VLAN 99
    b. Create IP Addressing for 6 Hosts
    c. Use ISL Encapsulation
    d. Create a default route pointing to 10.99.99.4 (Internet Service Provider)
5. GRE Interfaces
    a. Create Tunnel Interfaces between R1,R2,R3
    b. Assign IP addresses per diagram, with 8 hosts per subnet

Routing Protocol Configuration Tasks

1. OSPF configuration
    a. Configure OSPF on R3
        - Place the Loopback interface in area 3
        - Place all local VLAN interfaces in area 3
        - Do not specify the router-id
        - Create summary address for OSPF to advertise to the EIGRP network (configured below)
    b. Configure OSPF on R4
        - Place VLAN 33 interface and the loopback interface in area 3
        - Use loopback interface as router-id
2. EIGRP configuration
    a. Configure EIGRP on R1
        - Use AS Number 1003
        - Enable EIGRP on GRE Tunnels
        - Disable auto summarization
    b. Configure EIGRP on R2
        - Use AS Number 1003
        - Enable EIGRP on GRE Tunnels
        - Enable EIGRP on Loopback and VLAN interfaces
        - Disable auto summarization
    c. Configure EIGRP on R3
        - Use AS Number 1003
        - Enable EIGRP on GRE Tunnels
        - Disable auto summarization
3. RIPV2 configuration
    a. Configure RIPV2 on R1

- Enable RIPV2 on VLAN and Loopback Interfaces
- Do not disable auto summarization

4. Redistribution and tuning
    a. Redistribute EIGRP into OSPF
    b. Perform redistribution on R1 so that all RIP interfaces will be accessible to the EIGRP process
    c. Do not configure any static routes to accomplish this task
5. 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 SMTP traffic on R2, using VLAN 22 IP 192.168.22.1

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. Block SMTP access outbound from each site
3. Block TFTP outbound from site 2 only
4. Block all external access trying to reach the management VLAN