Computer Networks

Project

Mission

Set up a Wide Area Network for a mock bank that includes three LANs (one of which will be partitioned with two VLANs) and configure all network devices and endpoints to communicate with the entire WAN.

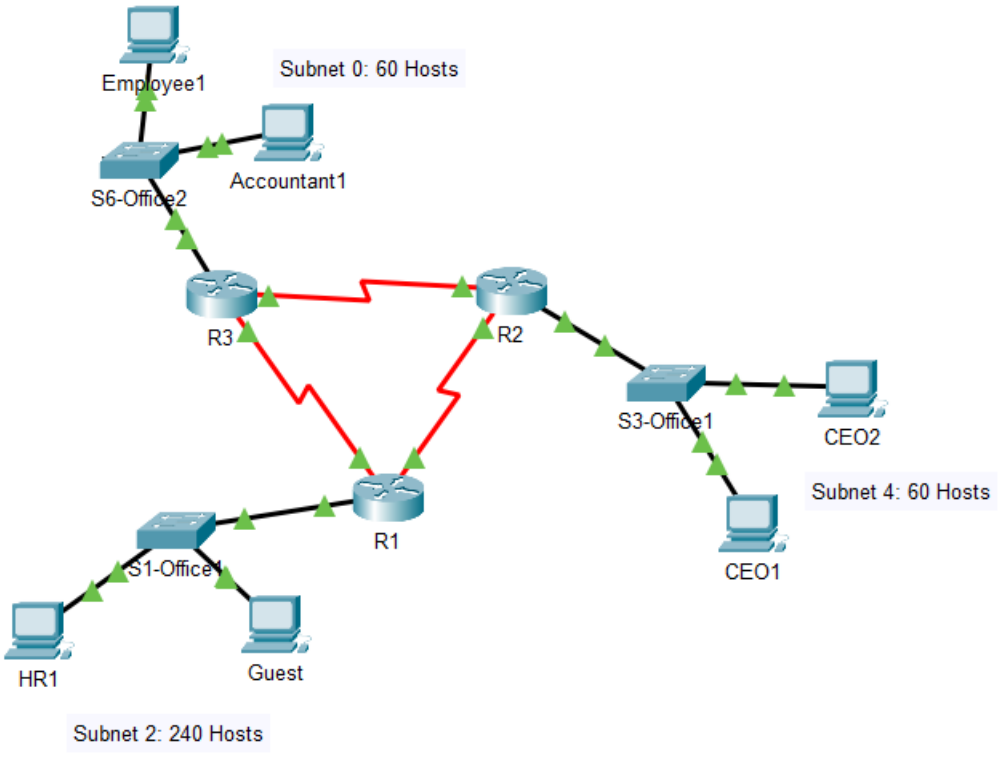
Requirements

- Advanced knowledge of networking concepts and the Cisco IOS.

Resources

- Cisco Packet Tracer 8.2.1.0118

Topology



Preceding topology and configure the devices.

Scenario

As a junior network administrator, the task is planning and configuring a corporate network for a new bank branch. It is your duty to set up the network correctly and implement basic security settings on all systems.

Task 1: Design an IP Address Scheme

Devise a Network Topology plan for the amount of subnets you will need, and where you want to assign the IPv4 addresses within each subnet.

1. Divide the 10.1.32.0/22 network into Six subnets.
2. What is the value of the new subnet mask?
3. How many usable host addresses exist per subnet?

4. Fill in the following table with the resulting subnets (from step 1 above):

Subnet Number	Network Address	Usable Host Address Range	Broadcast Address
1	10.1.32.0/25	10.1.32.1 - 10.1.32.126	10.1.32.127
2	10.1.33.0/25	10.1.33.1 - 10.1.33.126	10.1.33.127
3	10.1.34.0/25	10.1.34.1 - 10.1.34.126	10.1.34.127
4	10.1.35.0/25	10.1.35.1 - 10.1.35.126	10.1.35.127
5	10.1.36.0/25	10.1.36.1 - 10.1.36.126	10.1.36.127
6	10.1.37.0/25	10.1.37.1 - 10.1.37.126	10.1.37.127

Task 2: Implement VLANs and Trunk

Configure VLANs and set trunks on the appropriate network and its associated devices.

Note: Perform steps 1-4 on S1to S6 switches.

1. Create and name VLANs as follows:
    a. VLAN 10 – Management
    b. VLAN 20 – Accounting
    c. VLAN 30 – Employment
2. On S1to S6 switches configure the interfaces as "Access" mode, and assign VLANs as follows:
    a. VLAN 10: FastEthernet0/1-10
    b. VLAN 20: FastEthernet0/11-20
    c. VLAN 30: FastEthernet0/21-24
3. Verify the VLAN configurations using the appropriate **Show** commands, and save the configuration.
4. On both switches, disable DTP **only** on the access port

Task 3: Assign IP Addresses

Using the table you made in Task 2, assign subnets to the topology.
Note: Make sure to document the assignment of the IP addresses in a separate file, to keep track of them.

1. Assign an IP address to subnet 0 to the R3 interface connected to the S6 - switch network.
2. Assign the first IPs in subnet 1 to the R1<->R3 WAN link.
3. Assign the first IPs in subnet 2 to the R1<->R2 WAN link.
4. Assign the first IPs in subnet 3 to the R2<->R3 WAN link.
5. Assign the last usable addresses of Subnet 3 to VLAN 10 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).
   Note: Layer 3 connectivity with VLANs requires Router-on-a-Stick setup.
6. Assign the last usable addresses of Subnet 4 to VLAN 20 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).
7. Assign the last usable addresses of Subnet 5 to VLAN 30 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).
8. Assign the last usable IP addresses of Subnet 2 (Office 2) to the endpoints in each network or VLAN.

Task 4: Initial and Security Settings for Network Devices

Configure all network devices with basic security settings to prevent unauthorized access.
Perform steps 1-5 on all routers and switches.

1. Create a user account with the following login credentials:
   - Username: admin
   - Password: 123
2. Secure access to the console line by checking local login credentials.

3. Secure privileged mode access (password: 123).
4. Encrypt all passwords on the device.
5. Configure a suitable security message (hint: MOTD Banner).

Lab Task 5 (Bonus): Secure Remote Access

Configure SSHv2 services on all routers to allow for remote administration.
Perform steps 1-4 on R1, R2, and R3.

1. Set the IP domain name to aast.com.
2. Generate secure keys (minimum key length is 1024 bits).
3. Set SSH version 2.
4. Configure VTY lines to check for local login credentials, and allow only incoming SSH sessions.
5. Verify this part of the configuration using the appropriate show commands, and save the configuration.
6. Configure the correct default gateway on the Admin PC and try to log in to routers from admin PCs, using SSH.

   Run the command: **ssh -l <username> <target-ip>**

Perform steps 1-3 on all devices.

1. Check the following parameters on all devices:
   a. IP Address
   b. Subnet Mask
   c. Default Gateway
2. Go to the command prompt in the admin PC and try to ping CEO1 and Employee1.
3. Go to the command prompt in Employee2's PC and try to ping Accountant1 and Accountant2. The results should be successful.
4. If a connectivity test fails, perform troubleshooting.