COLLEGE OF ENGINEERING & TECHNOLOGY

Department	: Computer Engineering
Lecturer	: Prof. Yahya Z. Mohasseb
Assoc. Teacher	: Eng. Nourhan Tarek
Course Title	: Computer Networks
Course Code	: CC431

CC431: Computer Networks

Final project

Lab 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

• Environment & Tools

- Cisco Packet Tracer 8.2.1 or later

Team formation

- All students need to form groups consisting of 3-4 students for the project in this course.

Grading Criteria

- Non-working network will be penalized by 50% of the grade (per requirement).

- Failing to adhere to networking concepts will be penalized 40% of the grade (per requirement).

- Any sign of plagiarism will be punished by 100% of the grade.

Deliverables

When you hand in your programming assignment, you should include:

- A packet tracer file that contains the previously mentioned topology and all saved configurations. Any file without the saved configuration will be penalized.

- A separate (typed) document of a page or so containing the addressing table and all steps of configurations used supported by the appropriate screen shots.

Deadline

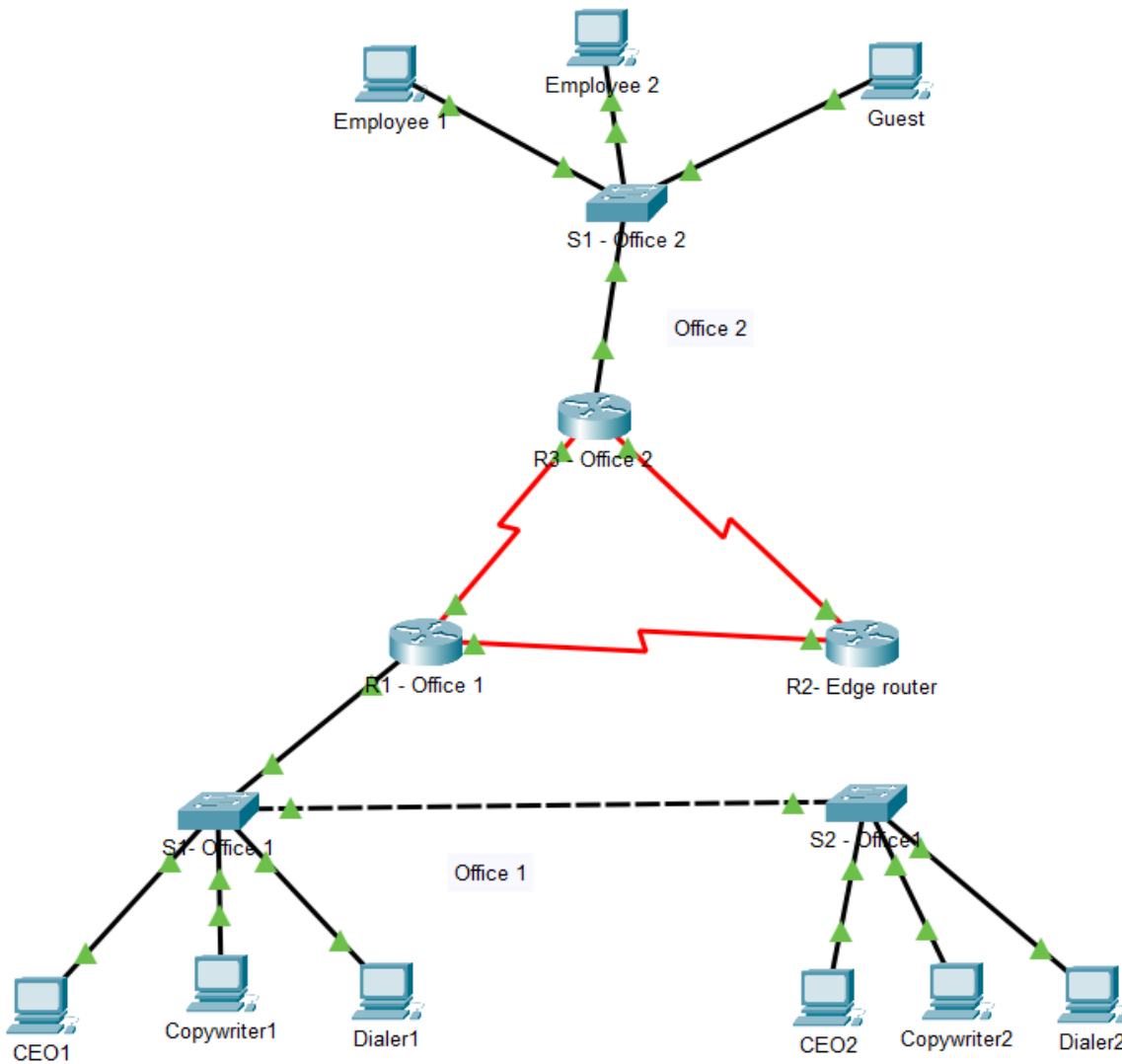You can submit the project at any time before Tuesday, 30/5/2024.

Groups formation

The deadline for the group formation is Thursday, 16/5/2024.

Please use this link to fill the information of your team members:

https://docs.google.com/spreadsheets/d/1gCRwPxfi9gPuML898484wQdG3HExU
uNJcgtuWiDhr_0/edit?usp=sharing

Topology

Create the preceding topology and configure the devices.

Scenario

As a junior network administrator, you and your team were tasked with 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.

Lab 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 172.16.10.0/16 network into seven 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

Lab 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 S1-Office1 and S2-Office1.

1. Create and name VLANs as follows:

    a. VLAN 10 – Management

    b. VLAN 20 – Marketing

    c. VLAN 30 – Accounting

    d. VLAN 100 – Native

2. On S1-Office1 and S2Office1 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. Configure the S1-Office1 to S2-Office1 interconnecting link as "Trunk" on both.
Note: To simplify the identification of the ports, click "Options…", click "Preferences…" and select "Always Show Port Labels in Logical Workspace".

4. Verify the VLAN and trunk configurations using the appropriate **Show** commands, and save the configuration.

5. On both switches, disable DTP **only** on the access port

Lab 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 1 to the R3 interface connected to the Office2 network. R1's LAN interface will be configured in Task 4.~~

2. ~~Assign the first IPs in subnet 2 to the R1<->R3 WAN link.~~

3. 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.

4. 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).

5. 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).

6. Assign the last useable IP addresses of Subnet 2 (Office 2) to the endpoints in each network or VLAN.

7. For any other networks, you can choose the assigned IP address as you like.

Lab Task 4: Configure R1 for Inter-VLAN Routing

Configure the router on the Office1 network to allow multiple VLANs to communicate on the network.

Perform steps 1-4 on R1.

1. Enable GigabitEthernet 0/0

2. Create three sub-interfaces on GigabitEthernet 0/0 (use any sub-interface IDs you want).

3. Set the correct encapsulation type and VLAN ID for each sub-interface.

4. Configure the appropriate IP address and subnet mask (corresponding to VLAN). Use the first usable address of each subnet.

5. Check the settings on the router using the appropriate show command.

6. On S1-Office1, set GigabitEthernet 0/1 as Trunk, with appropriate Native VLAN.

7. Verify this part of the configuration using the appropriate show commands and save the configuration.

8. Test the inter-VLAN routing by pinging Copyrighter1 and Dialer1 from the CEO1 PC.

Lab Task 5: Static Routing for network devices

Perform steps 1-3 on all routers.

1. Configure the appropriate IP address and subnet mask (according to your addressing table). Hint: you can use the first usable address of each subnet.

2. Configure the suitable static routing technique on all routers.

3. Configure a default route.

Lab Task 6: 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: ACDC1973

2. Secure access to the console line by checking local login credentials.

3. Secure privileged mode access (password: beatles1960).

4. Encrypt all passwords on the device.

5. Configure a suitable security message (hint: MOTD Banner).

Lab Task 7: 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. Make sure they are configured correctly and adjust them if necessary.

3. Go to the command prompt in the admin PC and try to ping CEO1 and Employee1.

4. Go to the command prompt in Employee2's PC and try to ping Copyrighter1 and Dialer1. The results should be successful.

5. If a connectivity test fails, perform troubleshooting.

   Note: If this is your first time pinging the Dialer1 or Copyrighter1 PC from Employee 2's PC, the first ping may fail since the ARP tables are not populated.
   The first ping will aid in populating the ARP tables in the network devices, and future pings should then work.