Final Project

Cyber Security Professional Program

Computer Networking

Final Project

NET-13-L1
Computer Networking
Final Project

Contents

Requirements 2

Resources 2

Scenario 3

Lab Tasks 4

Part 1 – Examine the Topology 4

Part 2 – Design IP Address Scheme 5

Part 3 – Implement VLANs and Trunk 6

Part 4A – Assign IP Addresses 7

Part 4B – Inter-VLAN Routing 8

Part 5 – Secure Switch Physical Ports 9

Part 6 – Configure OSPF 10

Part 7 – Initial and Security Settings for Network Devices 11

Part 8 – Secure Remote Access 12

Part 9 – Full Connectivity Test 13

Part 10 – Extended ACL (Bonus) 14

Project Objective

The objective of this project is to test the level of knowledge and skill acquired through topics learned in the Computer Networking course. The tasks involve designing an IP scheme and implementing it on networks and end devices, working with VLANs and trunks, and setting up dynamic routing using OSPF.

Estimated Project Duration

4-6 hours

Requirements

- Advanced knowledge of networking concepts and the Cisco IOS.

Resources

- Environment & Tools
  (1) Cisco Packet Tracer 7.2.2 or later
- Files
  (1) NET-13-L1.pkt

Scenario

You are a junior network administrator.

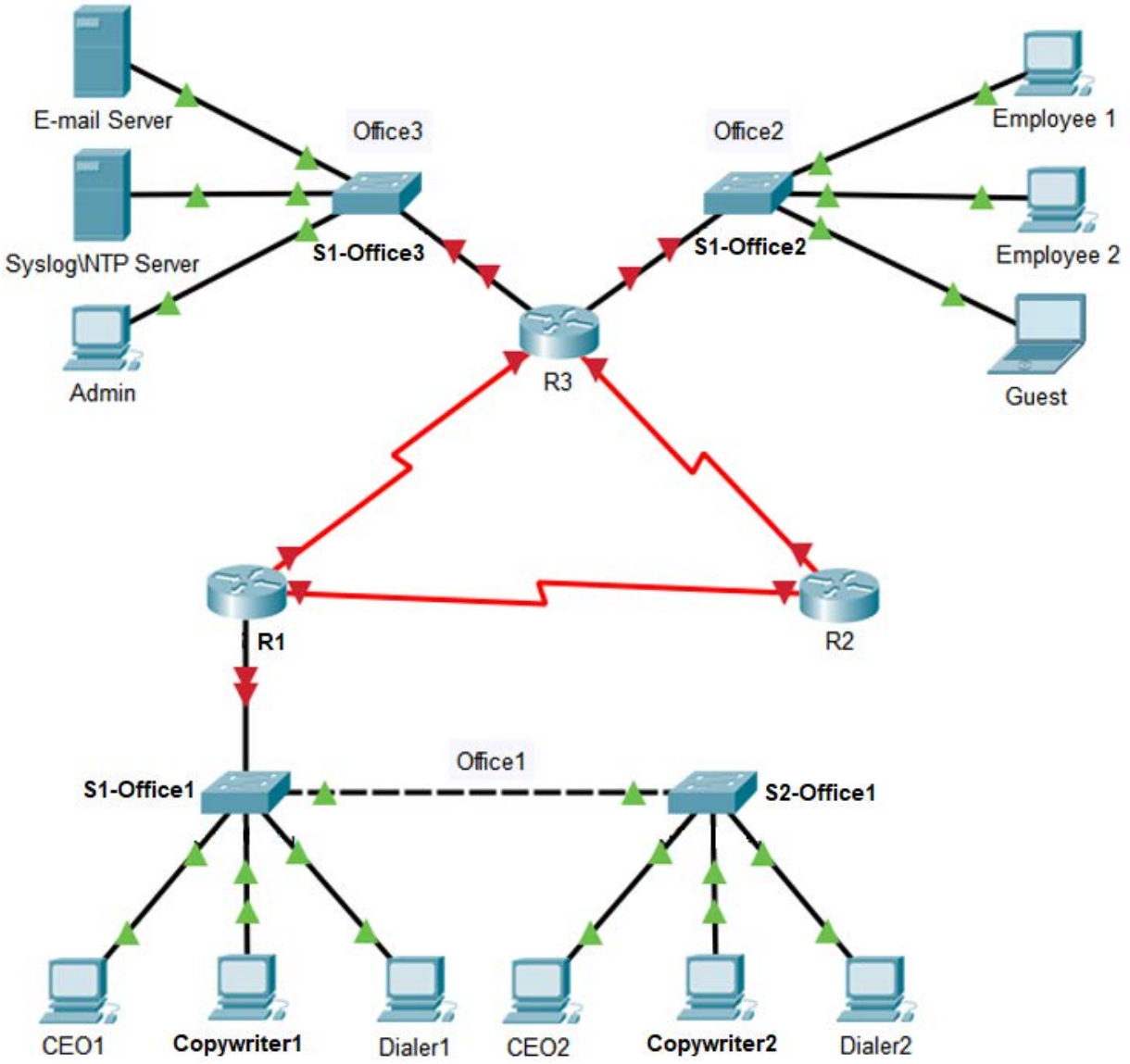
You and your team were tasked with planning and configuring a corporate network for a new bank branch in Miami.

It is your duty to set up the network correctly and implement basic security settings on all systems.

Good Luck!

Lab Tasks

Part 1 – Examine the Topology



Note: The correct host names are already set on all devices.

Part 2 – Design IP Address Scheme

1. Divide the 172.16.10.0/24 network into eight subnets.
2. What is the value of the new subnet mask?
3. How many usable hosts 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			
2			
3			
4			
5			
6			
7			
8			

Part 3 – Implement VLANs and Trunk

Perform steps 1-4 on S1-Office1 and S2-Office1

1. Create and name VLANs as follows:
   VLAN 10 – Management
   VLAN 20 – Marketing
   VLAN 30 – Accounting
   VLAN 100 – Native
2. Configure the interfaces as "Access" and assign VLANs as follows:
   VLAN 10: FastEthernet0/1-10
   VLAN 20: FastEthernet0/11-20
   VLAN 30: FastEthernet0/20-24
3. Configure the switch interconnected link as "Trunk" and set VLAN 100 as the Native.
4. Verify the VLAN and trunk configurations using the appropriate **Show** commands, and save the configuration.

Bonus: Disable DTP only on access ports.

Part 4A – Assign IP Addresses

Assign subnets to the topology as follows (according to the table in Part 2 above):

Guidelines:

- Assign the first usable IP address to the router's LAN interfaces (which will then be the default gateway).
- Assign the first IP addresses to the router's WAN links.
- **Bonus:** Assign the second usable IP address and the correct default gateway to the switches.
- Assign the last usable IP addresses to the hosts.
- **Document the addressing scheme.**

1. Assign Subnet 1 to Office3.
2. Assign Subnet 2 to Office2.
3. Assign Subnet 3 to R1>R2 WAN link.
4. Assign Subnet 4 to R1>R3 WAN link.
5. Assign Subnet 5 to R2>R3 WAN link.

Note: Layer 3 connectivity with VLANs requires Router-on-a-Stick setup.

6. Assign Subnet 6 to VLAN 10.
7. Assign Subnet 7 to VLAN 20.
8. Assign Subnet 8 to VLAN 30.

Part 4B – Inter-VLAN Routing

Perform steps 1-4 on R1

1. Enable GigabitEthernet0/0.
2. Create three sub-interfaces on GigabitEthernet 0/0 (use whichever sub-interface IDs you want).
3. Set the correct encapsulation type and VLAN ID.
4. Configure the appropriate IP address and subnet mask (corresponding to VLAN).
5. On S1-Office1 set gigabitEthernet 0/1 as Trunk.
6. Verify this part of the configuration using the appropriate Show commands, and save the configuration.
7. Test Connectivity - Go to CEO1, and ping the default gateway. Do the same for Copryrighter1 and Dialer1, each to its corresponding default gateway. Correct the configuration if necessary.

Part 5 – Secure Switch Physical Ports

Perform steps 1-4 on S1-Office1 and S2-Office1 switches

1. Enable port security (only on ports connected to end devices).
2. Set the violation mode to Restrict.
3. Secure authorized MAC addresses using sticky learning.
4. Verify the port security configuration using the appropriate Show commands, and save the configuration.

Bonus: Disable all remaining unused ports.

Part 6 – Configure OSPF

Perform all steps on R1, R2, and R3

1. Configure the following for OSPF:
   - Process ID: 1
   - Router ID: R1-1.1.1.1 | R2 - 2.2.2.2 | R3 - 3.3.3.3
   - Area 0
2. Configure the appropriate network address and the corresponding wildcard on each router.
3. Set ports connected to the LAN to “Passive”.
4. Verify the OSPF configuration using the appropriate Show commands, and save the configuration.

Bonus: Change the default interval setting to “Hello”, every 1 second, and “Dead” every 4 seconds, on all of the router’s interconnected ports. Verify settings at finish.

Part 7 – Initial and Security Settings for Network Devices

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).

Note: Use the IP scheme documentation in Part 4A above to complete steps 6 and 7. (NTP and Syslog services are pre-enabled.)

6. Configure the NTP server's IP address.
7. Display the device's time and date settings and make sure they are correct.
8. Configure the Syslog server's IP address.
9. Enable the timestamp service.
10. Go to R1 global configuration mode, and issue the **shutdown** command on Gigabitethernet0/0. A log will immediately appear, reporting the event. Re-enable Gigabitethernet0/0 by running the **no shutdown** command.
11. In the topology, go to NTP\Syslog Server -> Services tab, click Syslog, and view the logs on the server.

Note: Switches not configured with IPs and default gateways will not sync with the Syslog/NTP server.

12. Verify this part of the configuration using the appropriate Show commands, and save the configuration.

Part 8 – Secure Remote Access

Perform steps 1-4 on R1, R2, and R3

1. Set the IP domain name to **Cyber.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. Attempt to log in to routers from admin PCs, using SSH.
   Run the command: **ssh -l <username> <target-ip>**

Bonus: Using a standard ACL, grant access only to the admin PC via SSH (hint: access-class).

Part 9 – Full Connectivity Test

Perform steps 1-3 on all devices

1. Check the following parameters on all devices:
   IP Address
   Subnet Mask
   Default Gateway
   Wildcard Mask

   Make sure they are configured correctly, and adjust them if necessary.

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 Copywriter1 and Dialer1.

The results should be successful.

Perform troubleshooting steps if a connectivity test fails.

Part 10 – Extended ACL (Bonus)

Perform steps 1-3 on R3

1. Configure a Numbered Extended ACL with the following parameters:
   - Traffic from the guest PC to the NTP/Syslog server is not permitted.
   - All other network traffic is permitted.
   - Apply an ACL on the correct interface and traffic direction.
2. Verify ACL configuration.
3. From the guest's PC, test the ACL by pinging the NTP server and E-mail server.