Lab Assignment

Cybersecurity Professional Program

Computer Networking

Final Project

NET-13-L1
Computer Networking
Final Project

Lab Objective

Test learner level of knowledge and skill acquired through topics covered in the Computer Networking course. Topics include design and implementation of IP schemes, VLAN configuration, dynamic routing configuration, security solution implementation, and basic network device configuration.

Lab Mission

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

Requirements

- Advanced knowledge of networking concepts and the Cisco IOS

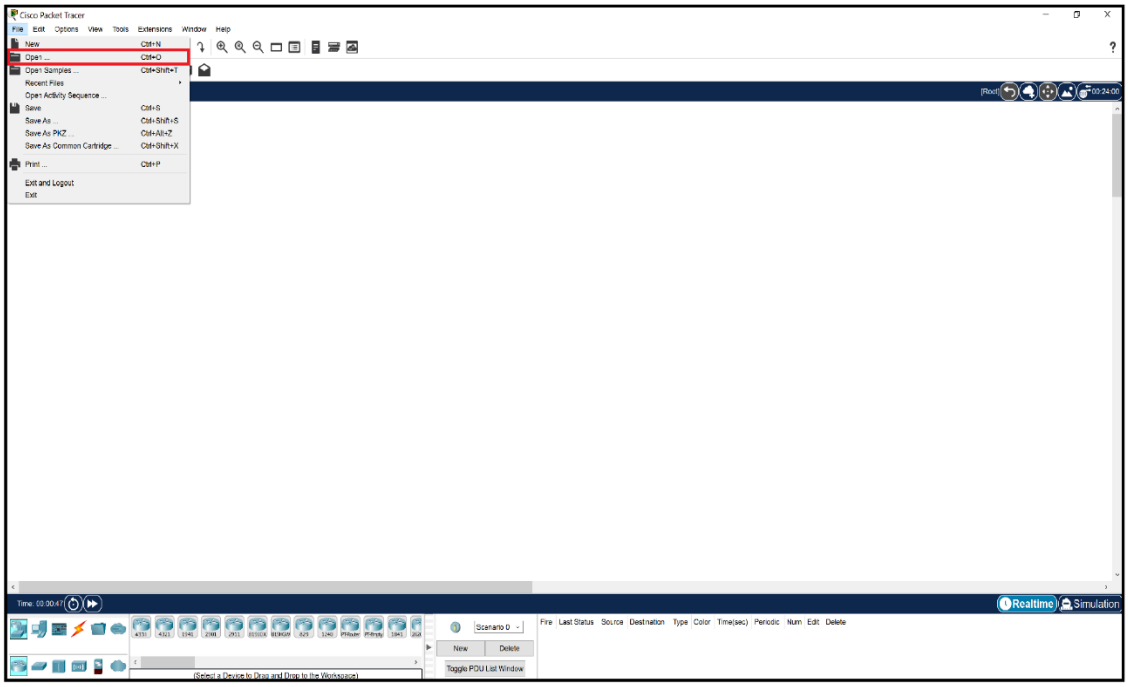
Resources

- Environment & Tools
  - Cisco Packet Tracer 8.0 or later
- Files
  - ***NET-13-L1.pka***

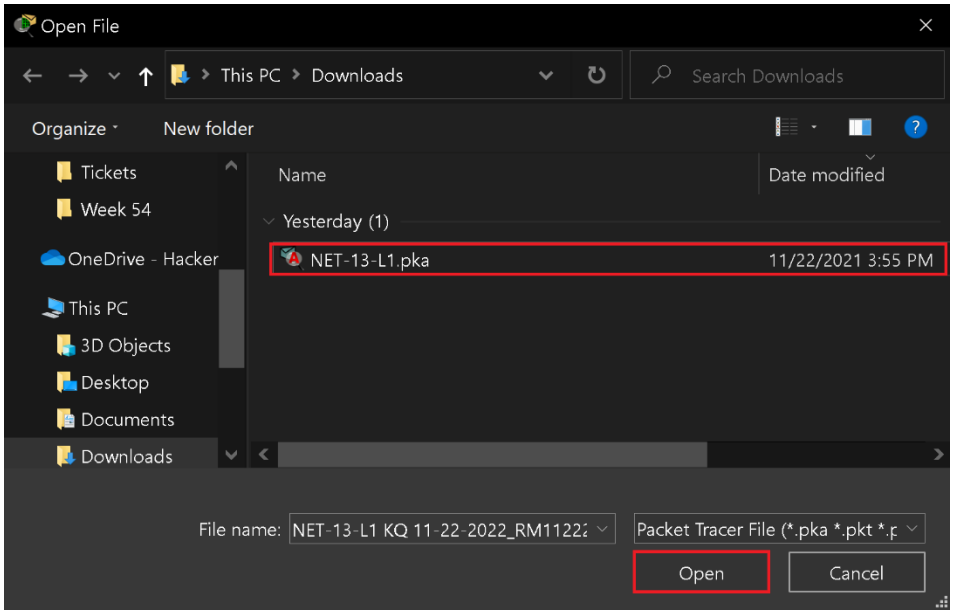
Instructions for PKA Lab Files

Lab materials include the lab document and a PKA lab file.

Open the PKA file through the Cisco Packet Tracer menu by clicking **File** and then ***Open…***.



Navigate to the file's location and open it.



Note: Double-clicking the PKA file in your file explorer may not work (depending on the Packet Tracer version).

When you open a PKA file in Cisco Packet Tracer, two windows appear:

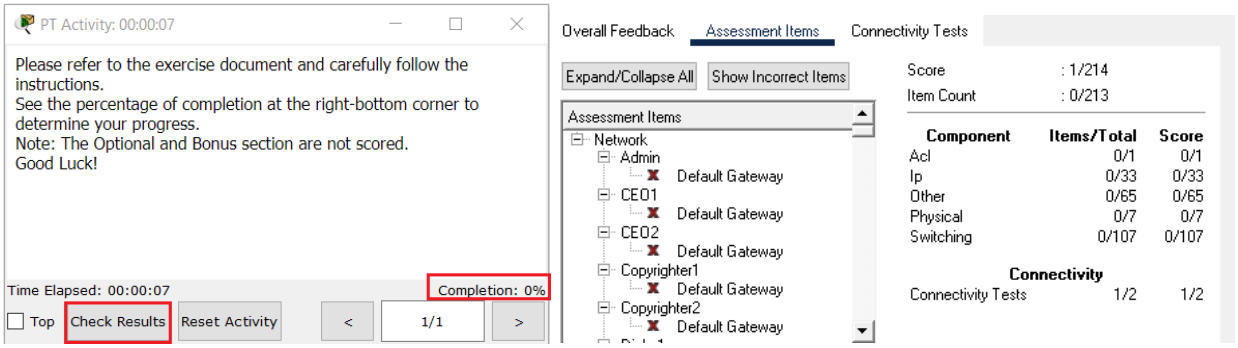
1. **Lab topology** window
2. **Activity** window

PKA Features

Note the following essential information regarding the **Activity** window:

1. **Completion Percentage:** Learner progress appears at the bottom right corner of the window.
2. **Check Result Button:** When you click this button and then click the **Assessment Items** tab, you will find a checklist with lab objectives and status, where **V** means done, and **X** means not done.

Note: Both features help the instructor grade the exercise swiftly and efficiently.

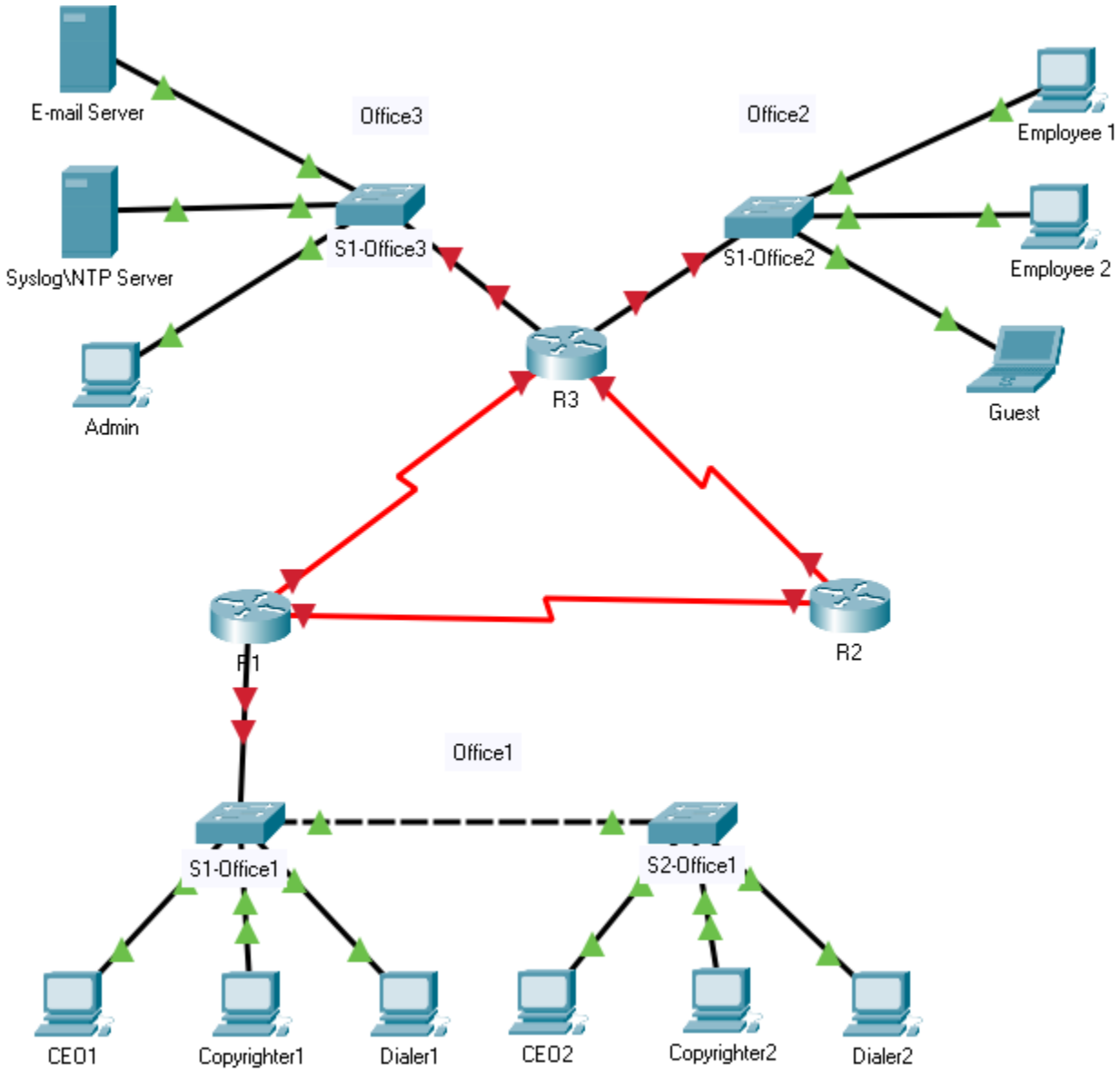


Scenario

As 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.

Note: The correct hostnames are already set on all devices.

Physical Topology



Lab Task 1: Design an IP Address Scheme

Devise a network topology plan for the number of subnets you will need and where you want to assign the IPv4 addresses within each subnet.

1 Divide the ***172.16.10.0/24*** network into eight subnets. Fill out the Addressing Table below:

Table 1:Addressing Table

Subnet Number	Network Address	Usable Host Address Range	Broadcast Address
1			
2			
3			
4			
5			
6			
7			
8			

2 What is the value of the new subnet mask?

3 How many usable host addresses exist per subnet?

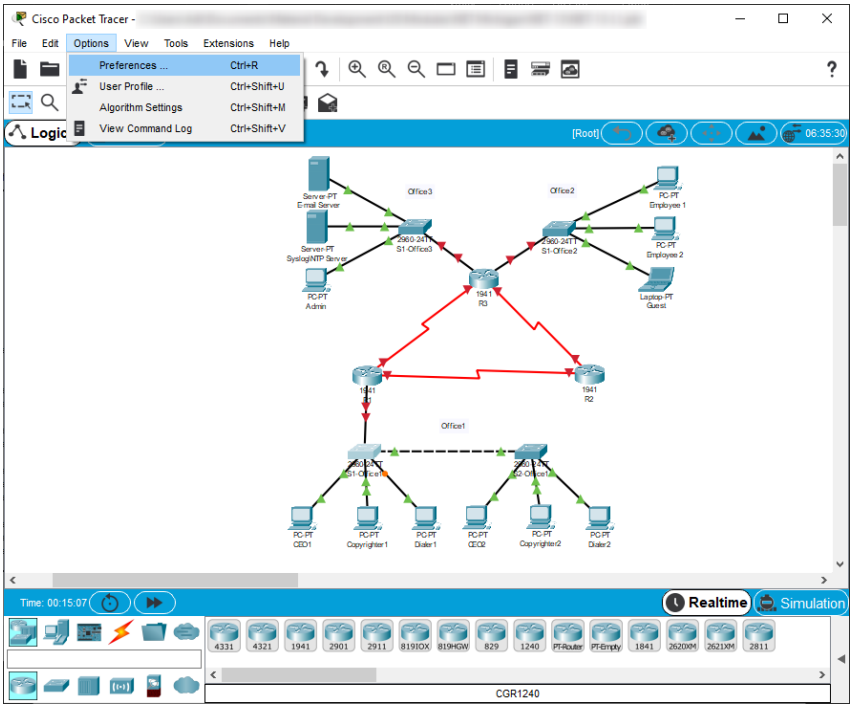
Lab Task 2: Implement VLANs and Trunk

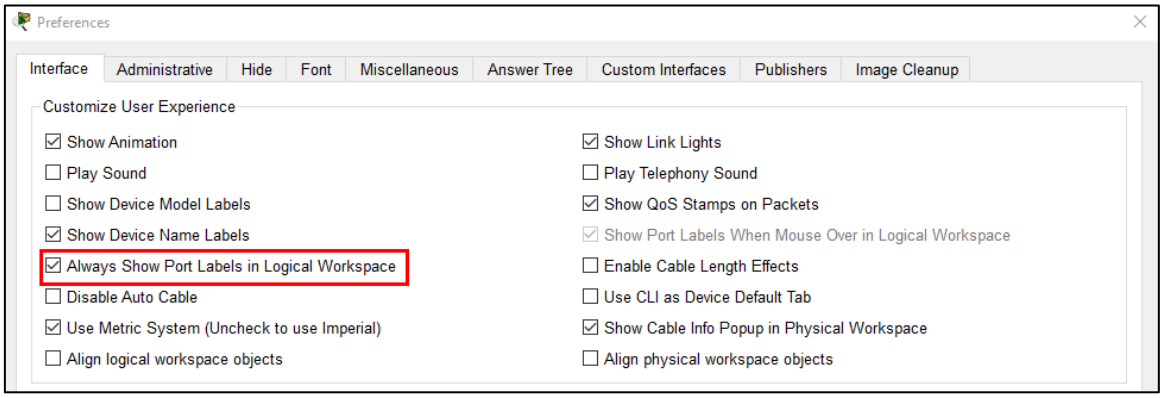
Configure VLANs and set trunks on the appropriate network and its associated devices.

Note: Perform steps 1–4 on S1-Office1 and S2-Office1.

1. Create and name VLANs as follows:
   - VLAN 10: Management
   - VLAN 20: Marketing
   - VLAN 30: Accounting
   - VLAN 100: Native
2. On S1-Office1 and S2Office1, configure the interfaces as ***access*** mode and assign VLANs as follows:
   - VLAN 10: FastEthernet0/1-10
   - VLAN 20: FastEthernet0/11-20
   - 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.

```
S1-Office1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1
10   Management                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   Marketing                         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
30   Accounting                        active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1-Office1#
```

```
S1-Office1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/2      1,10,20,30,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      1,10,20,30,100

S1-Office1#
```

```
S2-Office1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Gig0/2
10   Management                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   Marketing                         active    Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20
30   Accounting                        active    Fa0/21, Fa0/22, Fa0/23,
Fa0/24
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2-Office1#
```

```
S2-Office1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      100
```

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

Lab Task 3: Assign IP Addresses

Using the table, you made in Task 1, assign subnets addresses 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 the first usable IP address and appropriate subnet mask of subnet 1 to the R3 interface connected to the Office3 network.
2. Assign the first usable IP address and appropriate subnet mask of subnet 2 to the R3 interface connected to the Office2 network.
3. Assign the first and second usable IP address and appropriate subnet mask of subnet 3 to the R1 <-> R2 WAN link.
4. Assign the first and second usable IP address and appropriate subnet mask of subnet 4 to the R1 <-> R3 WAN link.
5. Assign the first and second usable IP address and appropriate subnet mask of subnet 5 to the R2 <-> R3 WAN link.
6. Assign the last usable addresses of subnet 6 to the Office1 network **CEO** end devices. Also, assign a subnet mask and the default gateway (first address in the subnet).
   Note: Layer 3 connectivity with VLANs requires a router-on-a-stick setup.
7. Assign the last usable addresses of subnet 7 to the Office1 network **Copyrighter** end devices. Also, assign a subnet mask and the default gateway (first address in the subnet).
8. Assign the last usable addresses of subnet 8 to the Office1 network **Dialer** end devices. Also, assign a subnet mask and the default gateway (first address in the subnet).
9. Assign the last useable IP addresses of subnet 2 (Office2) and subnet 1 (Office3) to the endpoints for each office network or VLAN. Also, assign the default gateway (first address in the subnet).

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 interface.
2. Create the following three sub-interfaces on GigabitEthernet 0/0: Sub-interface 10, 20, and 30.
3. Set the correct encapsulation type and VLAN ID for each sub-interface. Sub-interface 10 will route for VLAN 10, sub-interface 20 will route for VLAN 20, and sub-interface 30 will route for VLAN 30.
4. Using the following **Sub-Interface Addressing Table**, configure the appropriate IP address and subnet mask (using the first usable IP address of each subnet) for each sub-interface. Refer to table you made in Task 1 for subnet IDs.

Table 2:Sub-interface Addressing Table

Sub-Interface #	Subnet ID/VLAN #
Sub-interface 10	Subnet 6 (VLAN 10)
Sub-interface 20	Subnet 7 (VLAN 20)
Sub-interface 30	Subnet 8 (VLAN 30)

5. Check the settings on the router using the appropriate ***show*** command.
6. On S1-Office1, set both GigabitEthernet interfaces as **trunk** with appropriate native VLAN. On S2-Office1, set only GigabitEthernet 0/1 interface 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: Secure Switch Physical Ports

Configure all switches on the network to work with port security.

Perform steps 1–4 on the S1-Office1 and S2-Office1 switches.

1. Enable port security (only on ports connected to end devices).

   Note: Implement port security only on access ports connected to end devices (never on trunk ports).

   Set the violation mode to **restrict**.

2. Secure authorized MAC addresses using sticky learning.

3. Verify the port security configuration using the appropriate ***show*** commands.

```
S2-Office1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security
Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------
        Fa0/1         1           0                0         Restrict
       Fa0/11         1           0                0         Restrict
       Fa0/21         1           0                0         Restrict
---------------------------------------------------------------------
S2-Office1#
```

4. Disable all remaining unused ports and save the configuration.

Lab Task 6: Configure OSPF

Configure all routers on the network with OSPF to enable all subnets to communicate.

Perform all steps on R1, R2, and R3.

1. Turn on the connected **serial** interfaces on each router using the ***no shutdown*** command.
2. Turn on the connected **gigabit** interfaces on R3 using the ***no shutdown*** command.
3. Configure the following for OSPF on each router:
   - Process ID: 1
   - Network IP for each network
   - Router ID: R1-1.1.1.1 | R2 - 2.2.2.2 | R3 - 3.3.3.3
   - Area 0
4. Set interfaces connected to a LAN to ***passive***.
5. Verify the OSPF configuration on R1 using the appropriate ***show*** commands and save the configuration.

Lab Task 7: Extended ACL

Configure ACLs to prevent guests on the network from connecting to the NTP/Syslog server.

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 with a ***show*** command.
   Note: The IP addresses may vary depending on those assigned.
3. From the guest's PC, test the ACL by pinging the NTP server and email server.

Lab Task 8: 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. Configure console line to use local username **Admin** and password **ACDC1973** for access.
2. Secure privileged mode access with the password **beatles1960**.
3. Encrypt all passwords on the device.
4. Configure the following security message (hint: MOTD Banner): **Only authorized personnel are allowed accessing this device!**
5. Save all running configurations to NVRAM.

Lab Task 9: 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 ***Cyber.local***.
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 the routers from the admin PC using SSH.
   Run the command ***ssh -l <username> <target-ip>***
7. Go to the Command Prompt in the admin PC and try to ping CEO1 and Employee1.
8. Go to the Command Prompt in Employee2's PC and try to ping Copyrighter1 and Dialer1. The results should be successful. 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.