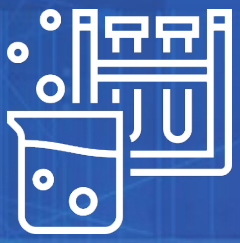
Lab Assignment & Solution



Cybersecurity Professional Program

Computer Networking

Final Project

NET-13-L1
Computer Networking
Final Project

Lab Objective

Test student 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 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.

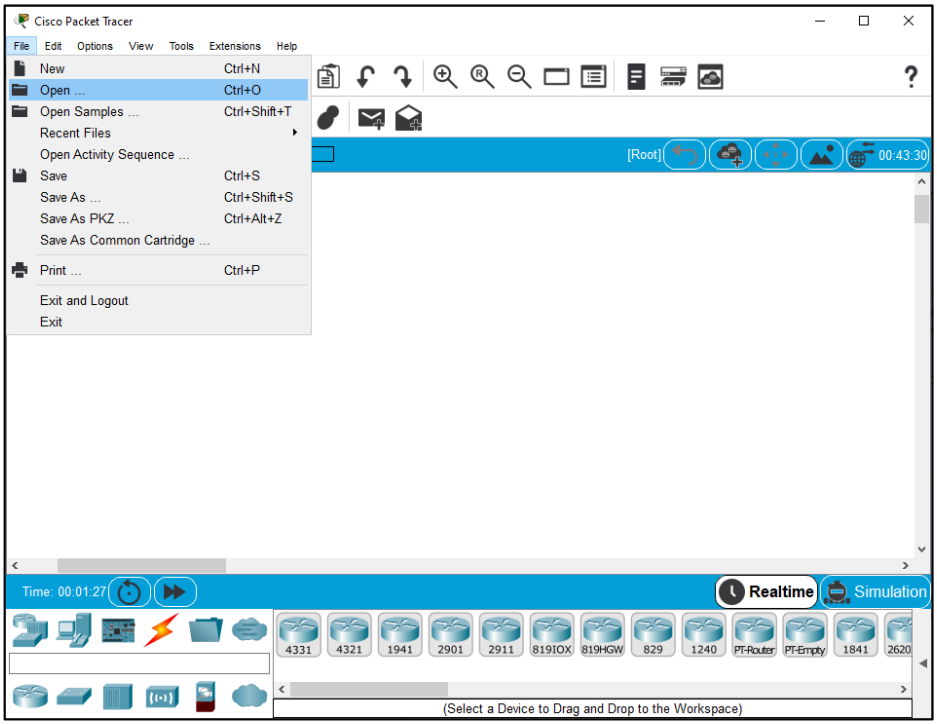
Resources

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

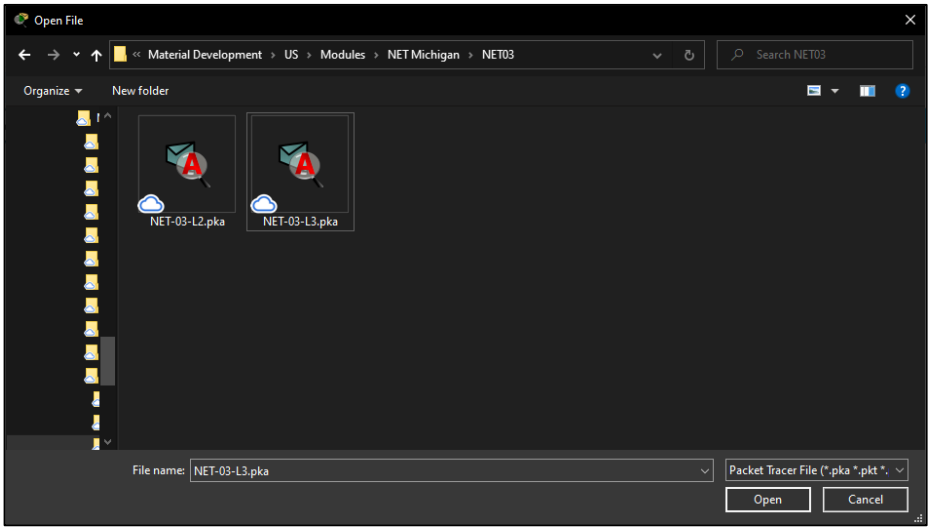
Instructions for PKA Lab Files

Lab material includes 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).

Lab material includes the lab document, and a PKA lab file.

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

1. Lab topology window
2. Activity window

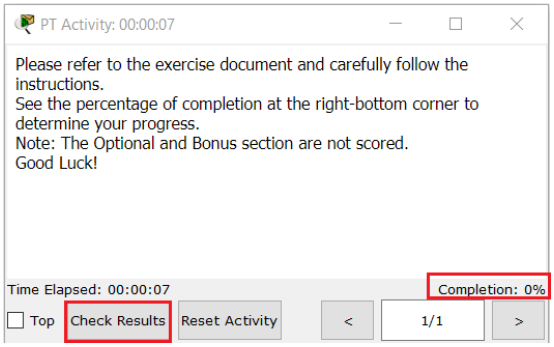
PKA Features

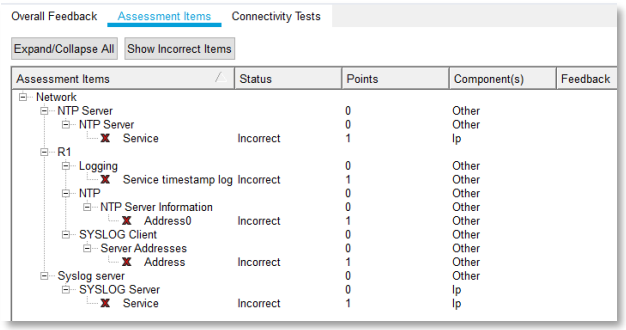
Note the following essential information regarding the Activity window:

1. **Completion Percentage** – Student 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, whereby V=done, X=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.

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 172.16.10.0/24 network into eight 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			
2			
3			
4			
5			
6			
7			
8			

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”. Verify the VLAN and trunk configurations using the appropriate **Show** commands, and save the configuration.
4. On both switches, disable DTP **only** on the access ports

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 Office3 network. R1's LAN interface will be configured in Task 4.
2. Assign an IP address to subnet 2 to the R3 interface connected to the Office2 network.
3. Assign the first IPs in subnet 3 to the R1 <-> R2 WAN link.
4. Assign the first IPs in subnet 4 to the R1<->R3 WAN link.
5. Assign IPs in subnet 5 to the R2<->R3 WAN link.
6. Assign the last usable addresses of Subnet 6 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.
7. Assign the last usable addresses of Subnet 7 to VLAN 20 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).
8. Assign the last usable addresses of Subnet 8 to VLAN 30 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).
9. Assign the last useable IP addresses of Subnet 2 (Office 2) and Subnet 3 (Office 3) to the endpoints for each office network or VLAN.

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: 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.
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 ports 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: 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 8: 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.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>**

   Check all endpoints for connectivity, and troubleshoot any endpoint with a connectivity issue.

Perform steps 1-3 on all devices.

1. Check the following parameters on all devices:
   a. IP Address
   b. Subnet Mask
   c. Default Gateway
   d. 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 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.

Lab Task 9: 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.