Report:

Initially, completed the Courses offered by Cisco Network Academy and learnt the basics of networking and cybersecurity. Final Project was to find a solution to the problem statement given by Cisco through ICT Academy. On that account, tasks were done as a part of finding a solution to the Statement. Each of these Tasks were completed as explained below.

Problem Statement:

Choose a university/college campus and analyze its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

Tool used: Cisco Packet Tracer

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is widely used for educational and training purposes to design, configure, and troubleshoot computer networks. Packet Tracer allows users to create virtual network topologies, connect devices, and simulate network behavior without the need for physical hardware.

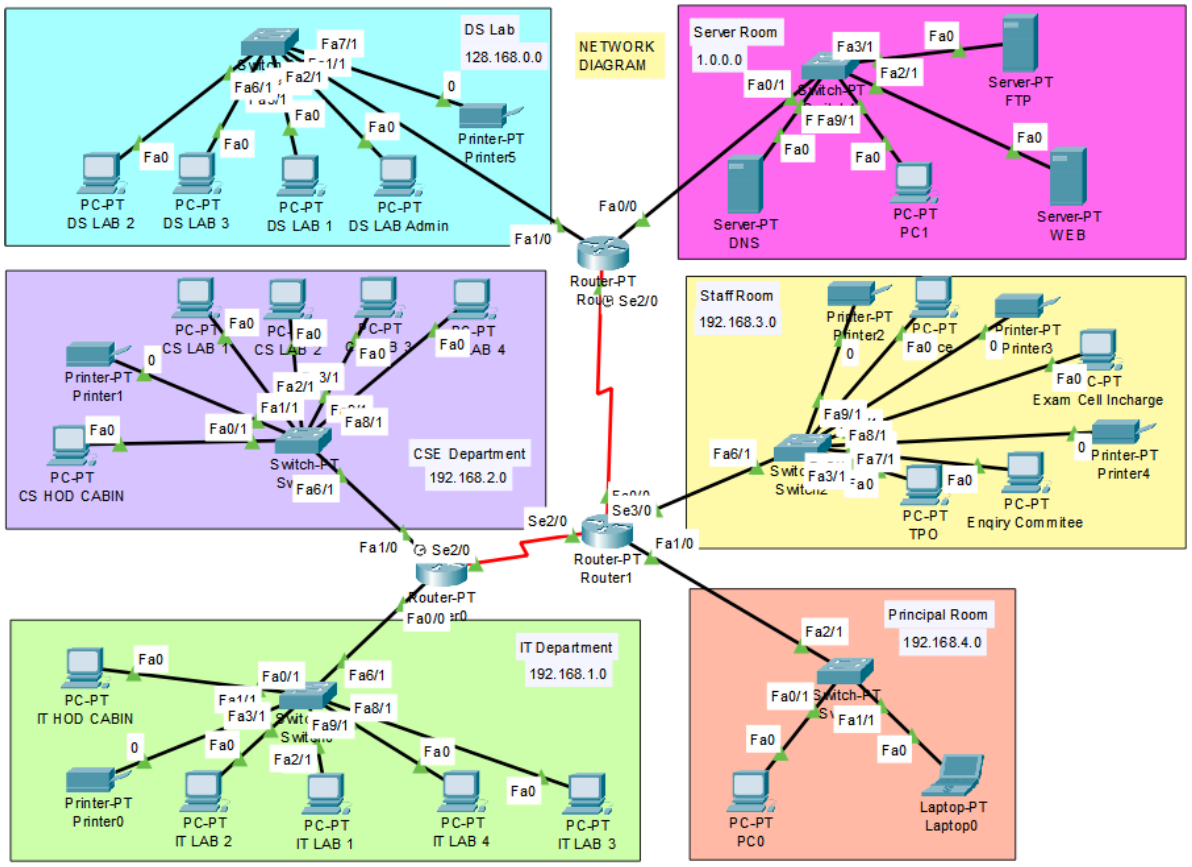
Tasks:

1. Campus Network Analysis
2. Network Mapping
3. Attack Surface Mapping
4. Secure Access Controls

CAMPUS NETWORK ANALYSIS

Network Topology of the campus:

Network topology refers to the arrangement and interconnection of network devices and components in a computer network. This document discusses the topology and various security measures employed in Computer Systems in our Institute. To begin, the campus has sufficient network facilities and security requirements installed priorly.



Nature of the network:

The computers in a computer lab are linked into a local area network (LAN), which allows individual users to share resources.

Potential entry points for cyber attack:

1. **Unsecure Trunks**
2. **Unused Open Ports**
3. **Server Vulnerabilities**
4. **Unprotected Endpoints**
5. **Weak Authentication or Security Software**

Findings:

1) **How are routers and switches different?**

Router (L3 Device):

- Role: Routers operate at the network layer (Layer 3) of the OSI model. Their primary function is to forward data packets between different networks or subnets.
- Network Interconnect: Routers connect multiple networks and facilitate communication between them. They determine the best path for data transmission based on destination IP addresses using routing protocols such as RIP, OSPF, or BGP.
- IP Addressing: Routers are responsible for IP address assignment and maintenance. They ensure that data packets reach their correct destination by using destination IP addresses for forwarding decisions.
- Traffic Management: Routers implement Quality of Service (QoS) to prioritize certain types of traffic over others, ensuring smooth and efficient data flow.
- Subnet Segmentation: Routers create separate broadcast domains by dividing a large network into smaller subnets, which improves network performance and security.

Switch (L2 Device):

- Role: Switches operate at the data link layer (Layer 2) of the OSI model. Their primary function is to forward data frames within a local network (LAN).
- Local Network Connectivity: Switches provide high-speed and low-latency connectivity within the same network segment. Devices on the same LAN can directly communicate with each other using MAC addresses.
- Broadcast Domain: Switches create a single broadcast domain, which means that broadcast traffic is limited to the devices connected to the same switch and does not propagate to other network segments.
- Collision Domain: Switches eliminate collisions in full-duplex mode, allowing simultaneous two-way communication between devices on different switch ports.

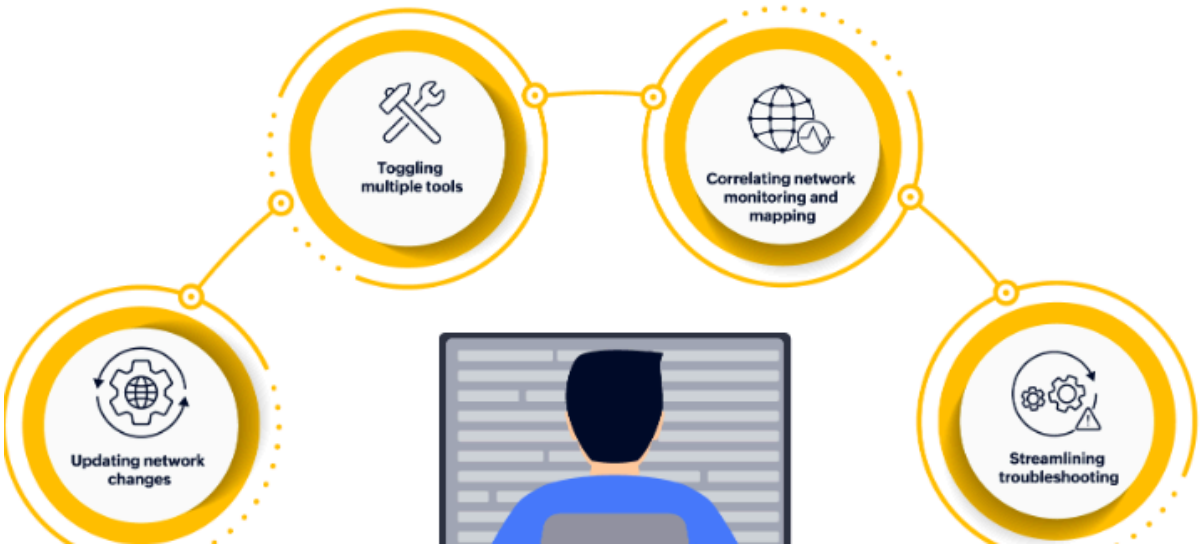
2) **Possible Security Threats in any Network**

- **Distributed denial-of-service (DDoS) attack**, multiple compromised computer systems that attack a target and cause a denial of service for users of the target. The **target** can be the server.
- **Phishing**. An attempt by cybercriminals posing as reputed institutions, usually through email, to obtain sensitive information from targeted resources.
- **SQL injection**, also known as SQLI, is an attack that uses malicious SQL code for backend database manipulation to access valuable information.

- Too many **Internet of Things (IoT) devices** are cheaply made and have inadequate security quality.
- **Buggy / Outdated Software.**
- **Trickery or Deception of Users** can also lead to a vulnerability
- **Hardware Issues** can also be considered as a vulnerability of the network.
- **Firewall Issues.** Firewall is the first layer of defence, failing can be a serious threat.

Network Mapping (with Cisco Packet Tracer)

Network Diagram:



Network mapping refers to the process of creating a **visual representation** of a computer network's structure, layout, and connectivity. It involves discovering and documenting various network elements, such as devices, routers, switches, servers, and their interconnections.

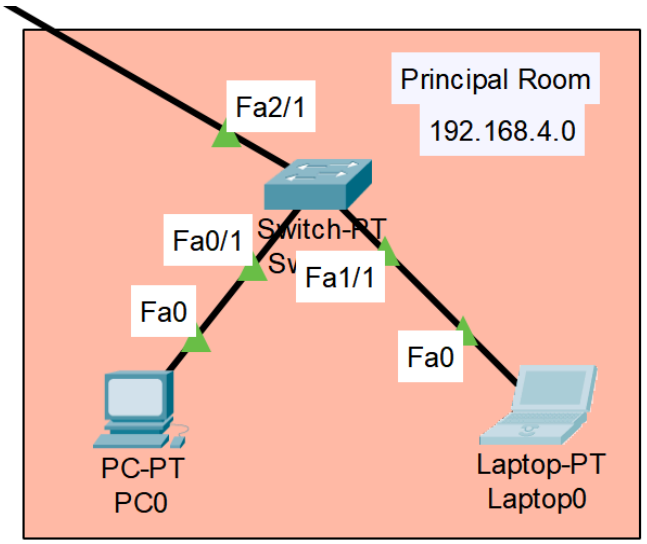
The main purpose of network mapping is to gain a comprehensive understanding of the network's topology, allowing network administrators, engineers, or security professionals to manage, troubleshoot, and secure the network effectively. Here, we use Cisco Packet Tracer for the purpose. The following rooms of the Institute are considered for the network analysis.

I) Principal Room

1.1. 1 PC

1.2. 1 Laptop

1.3. 1 Switch

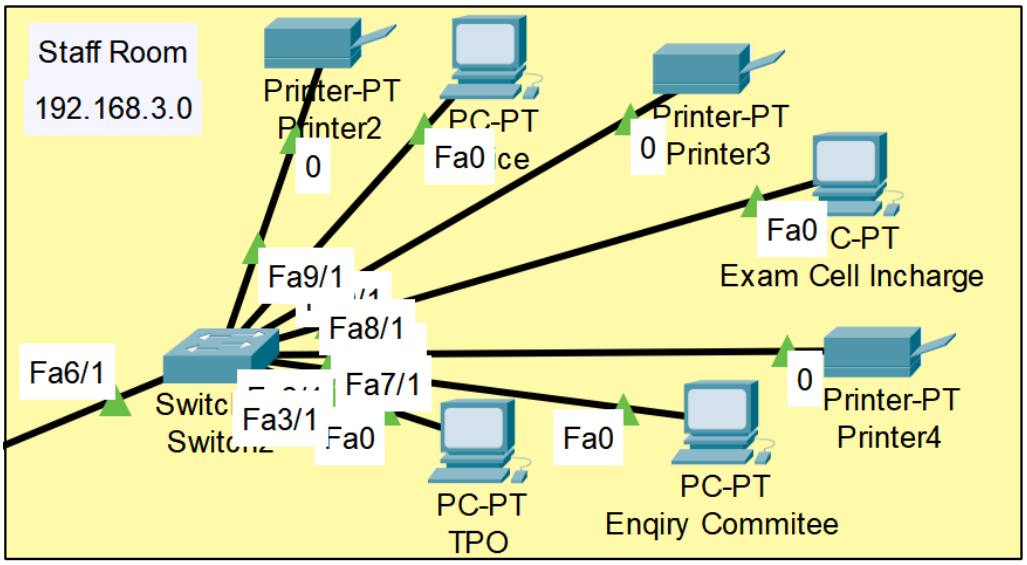


II) Staff Room

2.1. 4 PCs

2.2. 3 Printers

2.3. 1 Switch

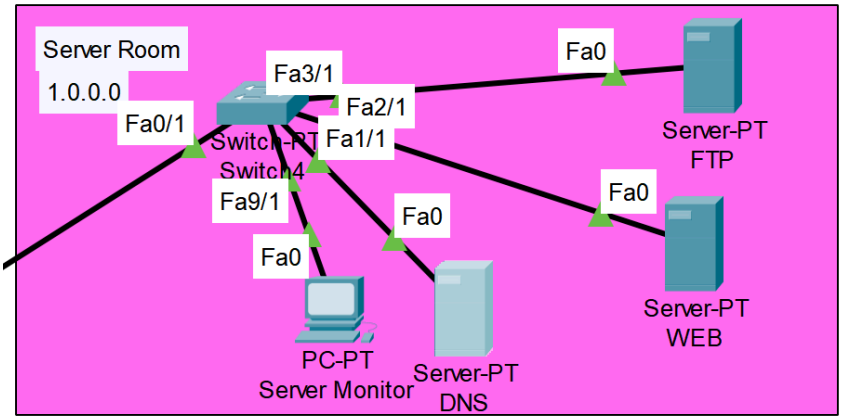


III) Server Room

3.1. 3 Servers

3.2. 1 PC

3.3. 1 Switch

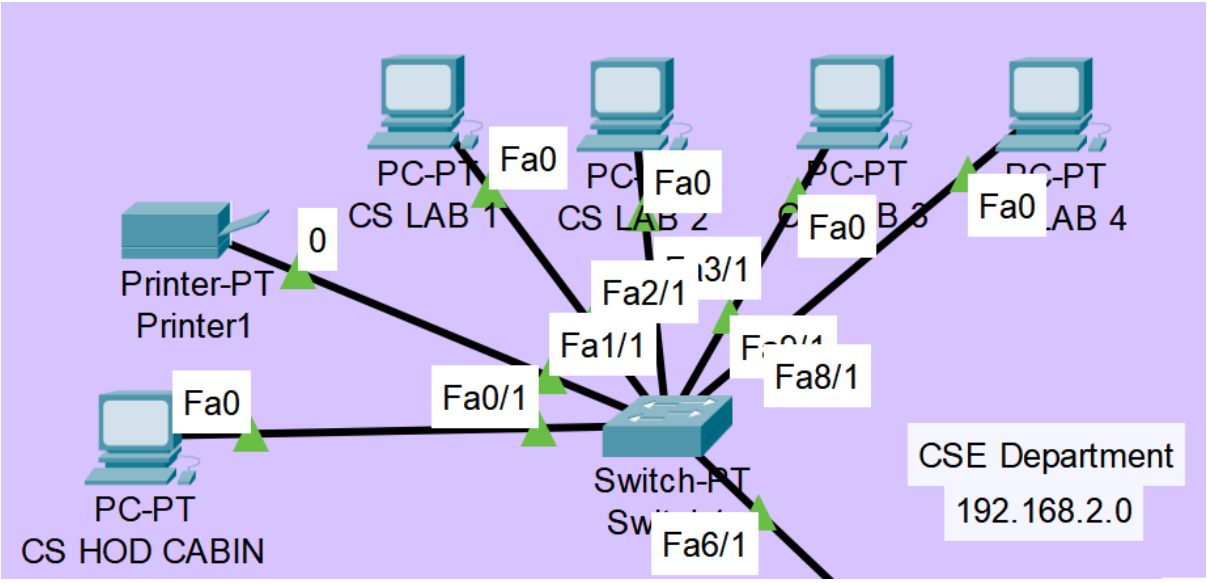


IV) IT Lab

4.1. 1 Printer

4.2. 4 x 10 PCs + 1 PC

4.3. 1 Switch

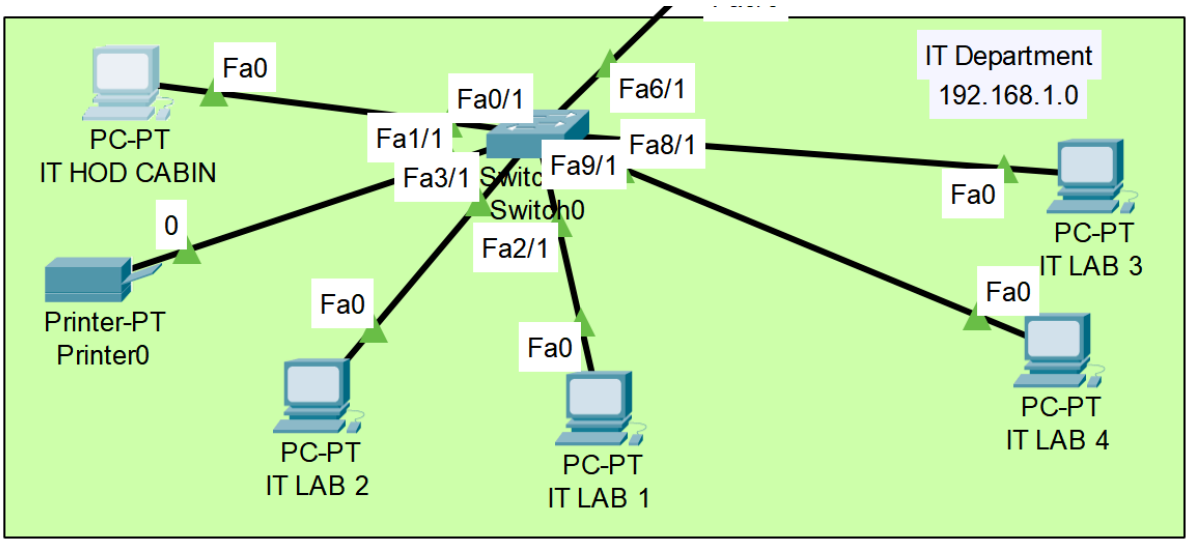


CSE Lab

5.1. 1 Printer

5.2. 4 x 10 PCs + 1 PC

5.3. 1 Switch

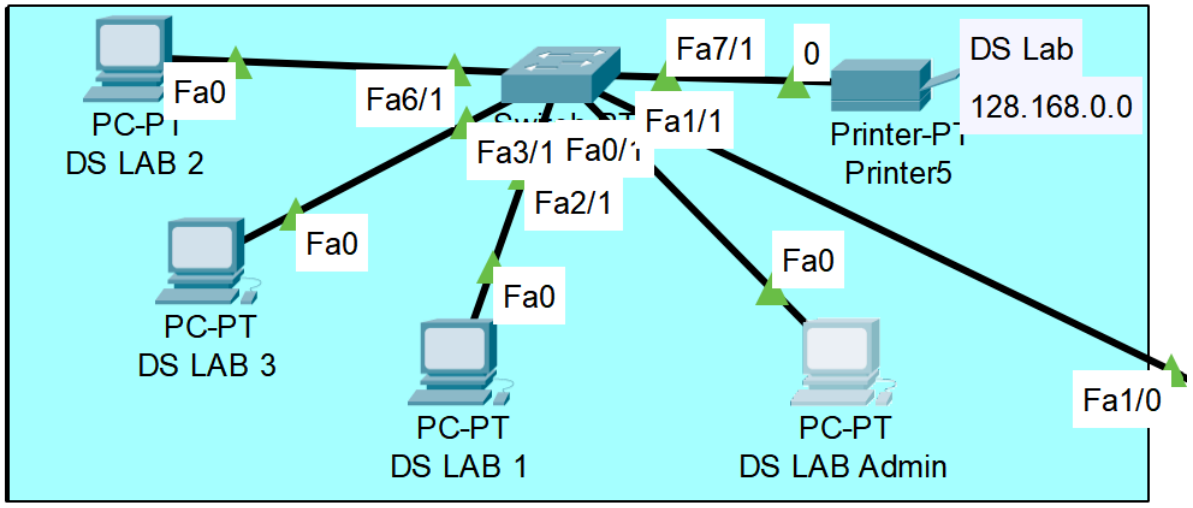


DS Lab

6.1. 1 Printer

6.2. 4 x 10 PCs + 1 PC

6.3. 1 Switch



Learnings:

1. **Role of Routers and Switches:**

Routers focus on interconnecting multiple networks and making intelligent forwarding decisions based on IP addresses at the network layer. On the other hand, switches are responsible for local network connectivity and use MAC addresses at the data link layer to efficiently forward data frames within the same LAN, while reducing collision domains and creating a single broadcast domain. Both devices play critical roles in ensuring effective and

scalable network communication.The switch is the network equipment to which all the computers are connected. A switch can be configured so the clients cannot connect to each other, to limit communication to groups created for a specific project and to grant or refuse access to external resources.

2. **Functions of Servers**

The function of a server is to receive, store, and share data. From there, you can run virus scans, manage spam filters, and install programs across the network. That makes network security management a lot less demanding, even when you have more members on your team. The server can also be used to filter the external information the clients can access, for example, blocking Facebook but leaving the Library of Congress accessible. The server can also store the profile of each student and back up their work from session to session.The researchers concluded that having a server for the computer laboratory will help the facilitator manage and maintain the security of the client's computers, such as monitoring applications, proper file sharing, and data keeping for better computer laboratory management.

3. **Access ports**

An access port is a type of switch port that is assigned to a specific VLAN (Virtual Local Area Network). Its primary function is to provide network connectivity to end-user devices, such as computers, printers, IP phones, and other network peripherals, within a local area network (LAN).

4. **Other End Devices**

In Cisco Packet Tracer, end devices refer to network devices that serve as the sources or destinations of data packets in a simulated network. These devices are usually located at the edges of the network and represent devices that users interact with directly.

Attack Surface Mapping

Attack surface mapping is a process used to identify and analyze potential points of vulnerability in a system, application, or network that could be exploited by attackers to gain unauthorized access or compromise the security of the target. By understanding and mapping the attack surface, organizations can proactively assess and strengthen their security defenses to reduce the risk of successful cyber-attacks.

The "ping" command

When a user enters the "ping" command in the command-line interface (CLI) of a device, they specify the IP address or hostname of the destination device they want to test. The "ping" command sends an ICMP Echo Request message from the source device to the destination device, and the destination device responds with an ICMP Echo Reply message. It displays the result of the communication test, showing the number of packets sent, received,

lost (if any), and the minimum, maximum, and average RTT values. The results help network administrators assess the quality of the network link and identify potential issues, such as high latency or packet loss.

ARP Tables

Manage the Address Resolution Protocol (ARP) cache. By using "arp -d", you can delete entries from the ARP cache, and with "arp -a", you can view the contents of the ARP cache, which provides information about the IP-to-MAC address mappings. When attempting to ping one PC from the other, the ping operation fails. The objective is to investigate the reason behind this failed ping, despite the direct connection between the computers. We observe that the ARP resolution is not occurring, leading to the failure of the ping. The Address Resolution Protocol (ARP) is responsible for mapping IP addresses to MAC addresses. In this case, since the computers are on different subnets, they are not in the same broadcast domain. As a result, the ARP messages from one PC cannot reach the other PC, preventing the MAC address resolution and subsequent successful communication.

This situation highlights the need for routers. Routers are devices that operate at the network layer (Layer 3) of the OSI model and facilitate communication between different subnets or networks. By connecting the two computers through a router, it can perform the necessary routing functions, including ARP resolution between subnets. This enables successful communication between devices on different subnets by forwarding packets between them.

MAC table

Performing "ping" tests between neighbouring computers to verifies connectivity. Additionally, we will explore the MAC table in the switch and gain an understanding of its fundamental functionalities such as learning, flooding, and forwarding.

RIB

The RIB is a database that contains routing information, including static routes, dynamic routes, and administrative distance values. It helps the router determine the best path for forwarding packets based on the destination IP address.

OSPF

We will utilize OSPF-specific show commands to examine how OSPF works. These commands provide insights into OSPF's behavior, including the OSPF neighbor relationships, the states of OSPF interfaces, and the OSPF routing table. By using the show ip route command, we can check the resulting IP route table, which contains information about OSPF-learned routes and their associated next hops.

By configuring OSPF, analyzing the OSPF show commands, examining the IP route table, and reviewing the show ip int brief table, we can gain a deeper understanding of how OSPF facilitates efficient routing within a network and how it dynamically builds the routing table to determine the best paths for packet forwarding.

Secure Access Controls

The setup involves connecting the computers to the switch, which in turn is connected to the router, thereby enabling communication between the two networks.

1. **Create Secure Trunks:**

To enhance security, it is recommended to disable DTP on trunk ports and explicitly configure them as trunk ports. **[I've pasted some terminal commands which I implemented in the CLI of some switches]**

```
Switch(config-if)# switchport nonegotiate

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q
```

Manually **configure trunk ports** on both ends of the link with the appropriate trunking encapsulation. Specify the allowed VLANs on the trunk using the following commands.

```
switchport trunk allowed vlan

Switch(config-if)# switchport trunk allowed vlan 10,20,30

Switch(config)# vlan pruning
```

Some switches support trunk port security to **limit the number of MAC addresses** allowed on a trunk port. This feature helps prevent MAC address spoofing and unauthorized devices from connecting to trunk ports.

```
Switch(config-if)# switchport port-security maximum 5

Switch(config-if)# switchport port-security violation {shutdown |
restrict | protect}
```

Disable any trunk ports that are not in use. If a trunk port is not needed, it's best to shut it down to reduce the attack surface.

```
Switch(config-if)# shutdown
```

2. **Secure Unused SwitchPorts**

Given below are the steps to disable unused switch ports.

1. Open the created network topology with **Cisco Packet Tracer**
2. Click on the switch to open the **configuration** options.
3. Access the **CLI** of the switch by clicking on the "CLI" tab at the bottom of the switch configuration window.
4. Enter the **global configuration** mode by typing enable and then configure terminal:

```
Switch> enable

Switch# configure terminal

Switch(config)# interface FastEthernet0/1

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security mac-address
0011.2233.4455

Switch(config-if)# switchport port-security violation shutdown
```

5. Exit the interface configuration mode and save the configuration

```
Switch(config-if)# end
Switch# write memory
```

Now, if an unauthorized device with a MAC address not listed in the allowed list tries to connect to the port, port security will be triggered based on the violation mode you set.

3. Implement Port Security

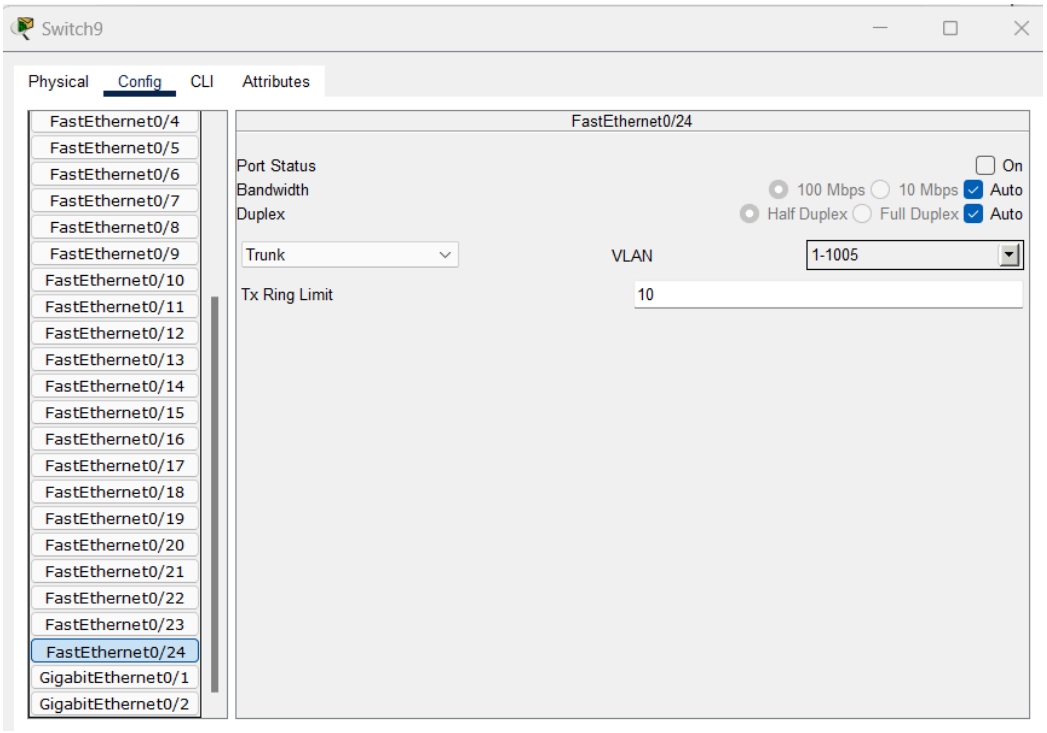
Private VLANs provide additional isolation and segregation within a single VLAN. PVLANs restrict communication between certain ports within the same VLAN, enhancing security and preventing lateral movement between devices.

The Port Status of the unused one can be turned OFF. This is a simple method of ensuring Port Security. But there are other methods to ensure similar actions. VLAN pruning is an optional step to limit unnecessary broadcast traffic on trunk links.

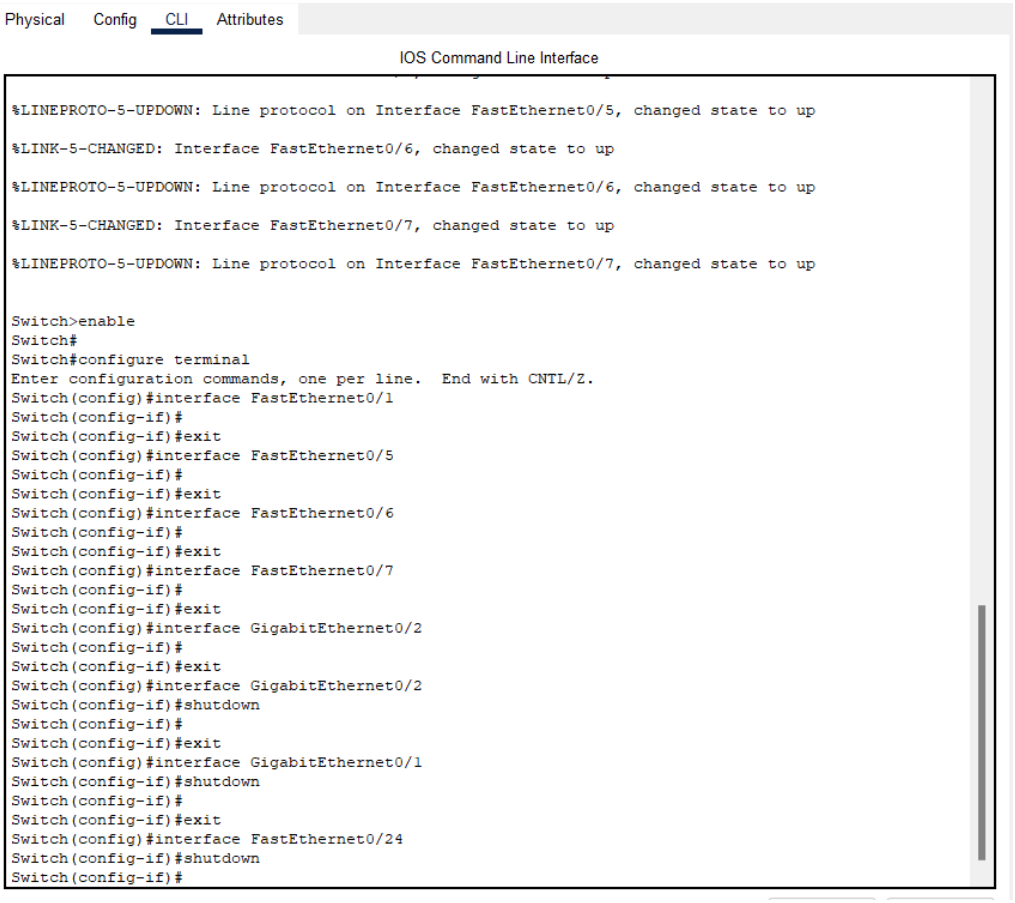
One another is using commands for the same action performed in the first technique. It simply requires the keyword ‘shutdown’. However, directly using this type of switching them down is not always preferred.

```
Switch(config-if)# switchport port-security violation protect

Switch(config)# vlan pruning
```



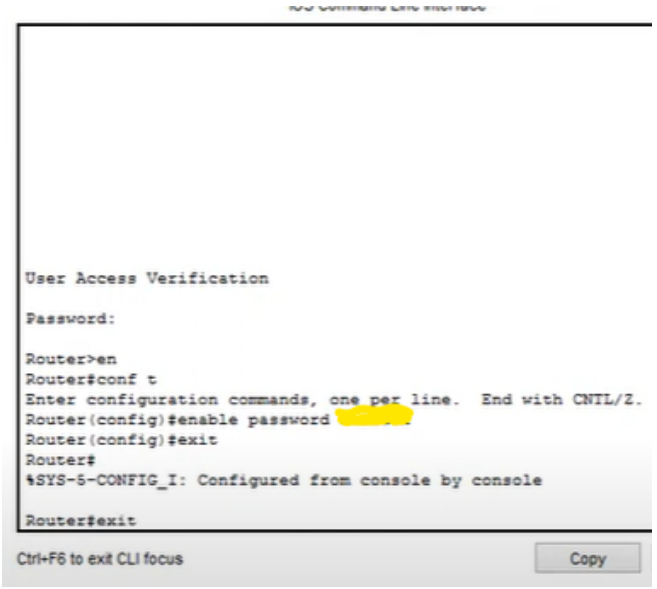
[Port Status turned OFF]



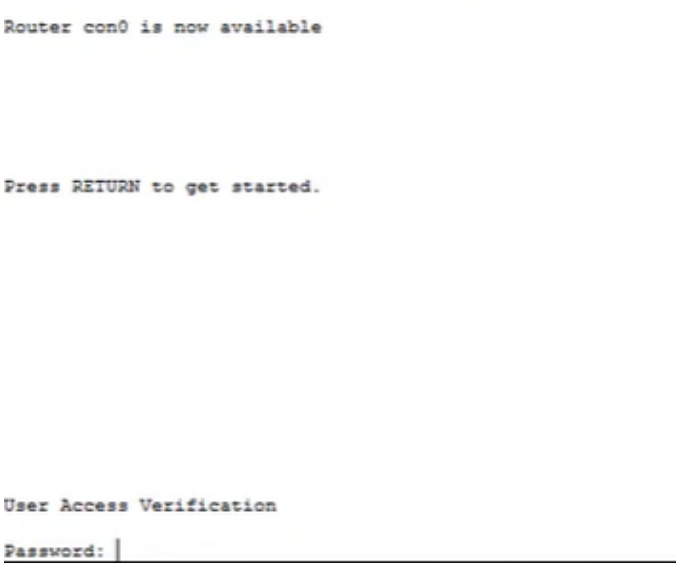
[Using CLI for the same process]

4. Secure Access Controls

Password management is a crucial aspect of cybersecurity that involves creating, storing, and safeguarding passwords to protect sensitive information and online accounts from unauthorized access. Proper password management practices help reduce the risk of security breaches and maintain the confidentiality, integrity, and availability of personal and organizational data.



[set password as my name for example]



Enter the password to acquire details

Mitigation countermeasures

These measures wrap up the following such as

- Network Segmentation,
- Intrusion,
- Detection Systems,
- Firewalls,
- Authentication and
- Authorization systems

Conclusion:

I am grateful for the trust and responsibility given to me during this internship, allowing me to take on challenging tasks and contribute meaningfully to the success of the projects. The Institute had already resolved all security issues except the open, unused switch ports in the Data Science(DS) Lab which was recently opened. On the whole, a proper security analysis was done in the Admin Block and Lab Block 1 of the Institute to ensure secure environment without cyber threats.

End Note:

Throughout my time at Cisco, I have had the privilege of working with a team of talented professionals who have been incredibly supportive and encouraging. The experience I gained during this internship has been both enriching and transformative, helping me develop in the Cybersecurity domain.

The exposure to real-world projects, cutting-edge technologies, and the collaborative work environment has been instrumental in broadening my understanding of the industry and enhancing my skills. The mentorship and guidance I received from my supervisors and colleagues have been invaluable in shaping my career path.