UNDER THE SUPERVISION OF:

DR/MOHAMMED FAYSAL

Team Members:

1. Roshan Mostafa
2. Menna tallah Khaled
3. Merna Ezzat
4. Shahd Hegazy
5. Marwa Atef

Course Name: Computer Networks

Department:

Electronics and Communication Engineering

Title:

Simulated University Network designed using Cisco Packet Tracer

Table of content

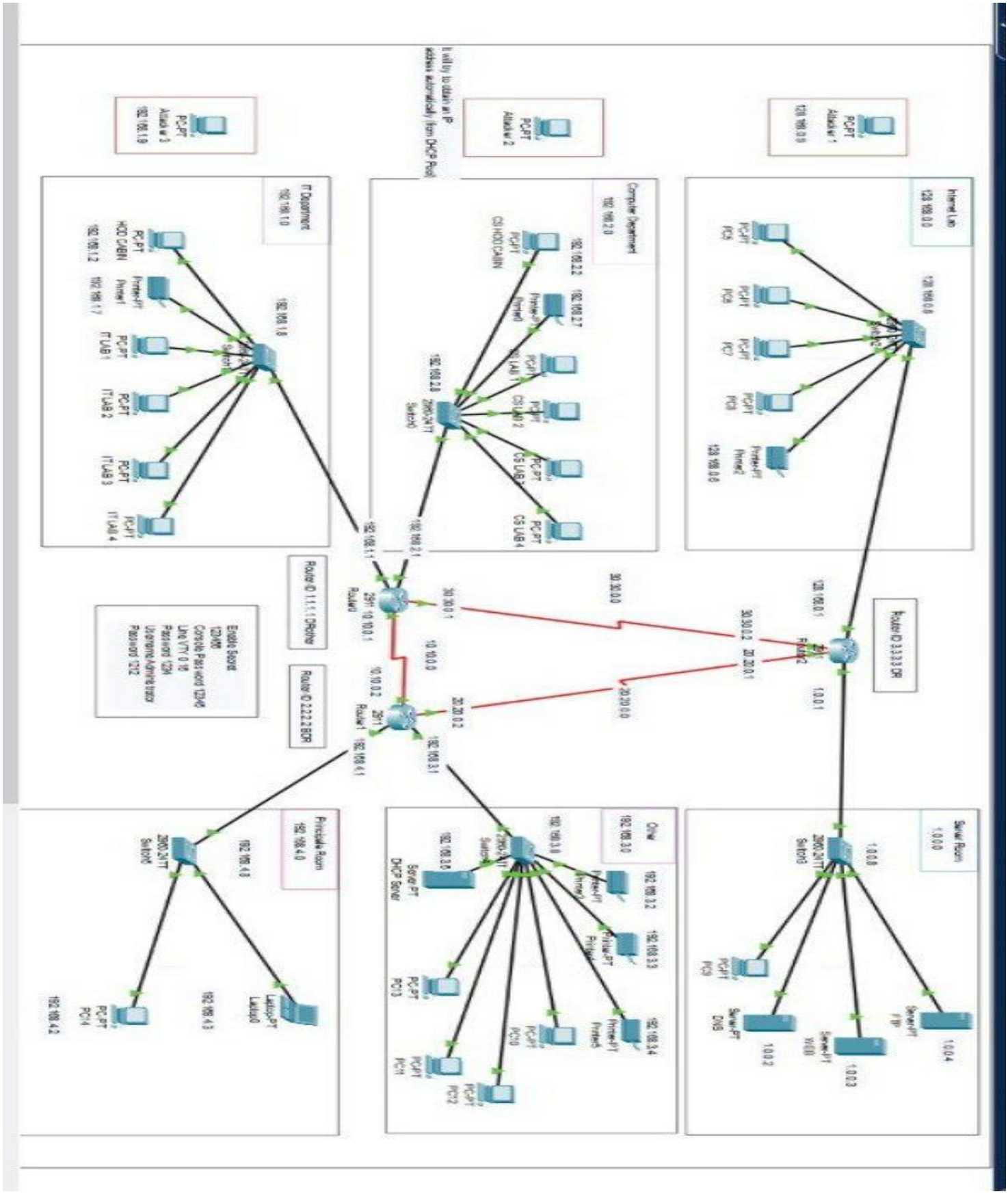
Project overview:

Our project represents a simulated University network designed using Cisco Packet Tracer. The network is divided into multiple sections including the Internet Lab, Computer Department, IT Department, Server Room, and the Principal's Room. All sections are interconnected through routers and switches, with a clearly defined IP addressing scheme and routing configuration.

Sections of the project:

- The **Internet Lab** is used by students for browsing and general use.
- The **Computer Department** serves as a programming or computer science lab.
- The **IT Department** handles support, maintenance, and administration.
- The **Server Room** hosts services such as FTP, Web, and DNS servers.
- The **Principal's Room** is the management office with connected devices.
- The **Other Section** includes devices that receive IPs dynamically from a DHCP server.

Network Topology Diagram



IP Addressing and Subnetting:

1. Final Subnet Table

Department	Network Address	Subnet Mask	Address Range	Devices Covered	IP Allocation Type
Internet Lab	128.168.0.0	255.255.255.0	128.168.0.1–128.168.0.254	PC6–PC9 (DHCP), Printer0 (Static)	DHCP via Router + Static
Computer Dept.	192.168.2.0	255.255.255.0	192.168.2.1–192.168.2.254	CS LAB 1–4 (DHCP), Printer2, CS HOD	DHCP via Router + Static
IT Dept.	192.168.1.0	255.255.255.0	192.168.1.1–192.168.1.254	IT LAB 1–4 (DHCP), Printer1, IT HOD	DHCP via Router + Static
Server Room	1.0.0.0	255.255.255.0	1.0.0.1–1.0.0.254	FTP, Web, DNS Servers, PC0	DHCP via Router + Static
Other Department	192.168.3.0	255.255.255.0	192.168.3.1–192.168.3.254	PC10–13 (DHCP), Printer5, DHCP Server	DHCP via Server + Static
Principal Room	192.168.4.0	255.255.255.0	192.168.4.1–192.168.4.254	Laptop0, PC14 (static)	Static
Router Interconnects	10.10.0.0/ 20.20.0.0/ 30.30.0.0	255.255.255.252	10.10.0.x/ 20.20.0.x/ 30.30.0.x	Router-to-Router Connections	Static

2.Address Allocation Summary

The network utilizes a combination of static and dynamic IP addressing to ensure both stability and flexibility across different departments:

- **Static IP Addressing** was manually assigned to critical devices such as:
  - Servers (FTP, Web, DNS)
  - All printers
  - Administrative machines (e.g., CS HOD, IT HOD, Principal Room devices)
  - Network infrastructure (routers and switches)
- **Dynamic IP Addressing (DHCP)** was implemented in two forms:
  - **DHCP via Router:** Most departments such as the Computer Department, IT Department, Internet Lab, and Server Room use the router to automatically assign IPs to general-use PCs.

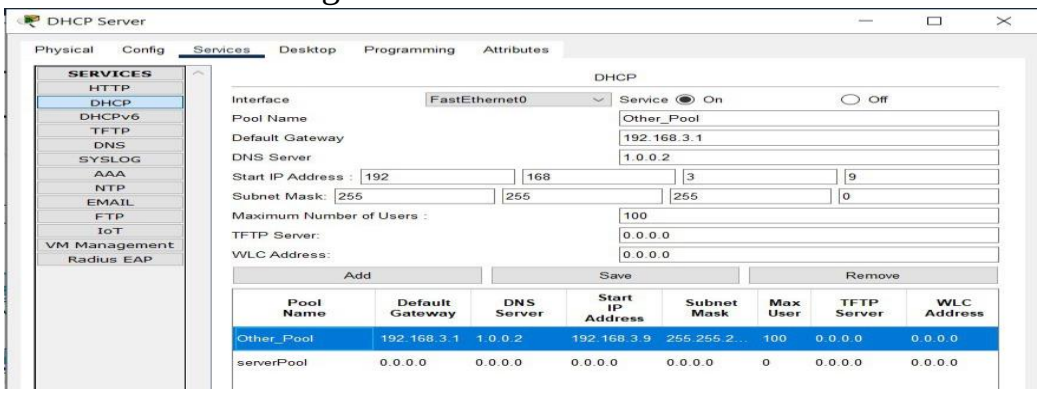
```
ip dhcp excluded-address 192.168.2.1 192.168.2.2
ip dhcp excluded-address 192.168.2.7
ip dhcp excluded-address 192.168.1.1 192.168.1.2
ip dhcp excluded-address 192.168.1.7
ip dhcp excluded-address 192.168.2.8
ip dhcp excluded-address 192.168.1.8
ip dhcp excluded-address 192.168.2.9
ip dhcp excluded-address 192.168.1.9
ip dhcp pool Computer-Department
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 1.0.0.2
ip dhcp pool IT-Department
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 1.0.0.2
```

DHCP configuration on R-0 for computer dep and IT dep.

```
R-2#show running-config | section dhcp
ip dhcp excluded-address 128.168.0.1
ip dhcp excluded-address 128.168.0.6
ip dhcp excluded-address 1.0.0.1 1.0.0.4
ip dhcp excluded-address 30.30.0.2
ip dhcp excluded-address 128.168.0.8 255.255.255.0
ip dhcp excluded-address 1.0.0.8
ip dhcp excluded-address 128.168.0.9
ip dhcp pool Internet_Lab
 network 128.168.0.0 255.255.255.0
 default-router 128.168.0.1
 dns-server 1.0.0.2
ip dhcp pool Server_Room
 network 1.0.0.0 255.255.255.0
 default-router 1.0.0.1
 dns-server 1.0.0.2
```

DHCP configuration on R-2 for server room and internet lab.

  - **DHCP via Dedicated Server:** The Other Department relies on a dedicated DHCP server to manage dynamic IP distribution, offering better control and centralized management.



2. Static IP Justification

- **CS HOD (Computer Science Head of Department):**
  Assigned a static IP to ensure **reliable remote access, ease of management, and quick troubleshooting** as this device is considered a key administrative endpoint.
- **Principal Room:**
  Given static IPs due to the **critical nature of the office**, requiring **consistent access, high stability, and enhanced network security**.
- **Printers (All Departments):**
  Configured with static IPs to prevent address changes, ensuring **uninterrupted printing services and easier configuration on client devices** across the network.

Routing Protocols:

The network uses **the OSPF (Open Shortest Path First)** dynamic routing protocol to enable communication between the different departmental subnets across the routers.

Protocol Used:

- **OSPF (Open Shortest Path First)** is an Interior Gateway Protocol (IGP) designed for use within a single Autonomous System (AS). It is a link-state routing protocol that dynamically finds the shortest path to each destination using the Dijkstra (SPF) algorithm.
- It was chosen for its scalability, fast convergence, and ability to efficiently manage routing across a multi-departmental campus network.

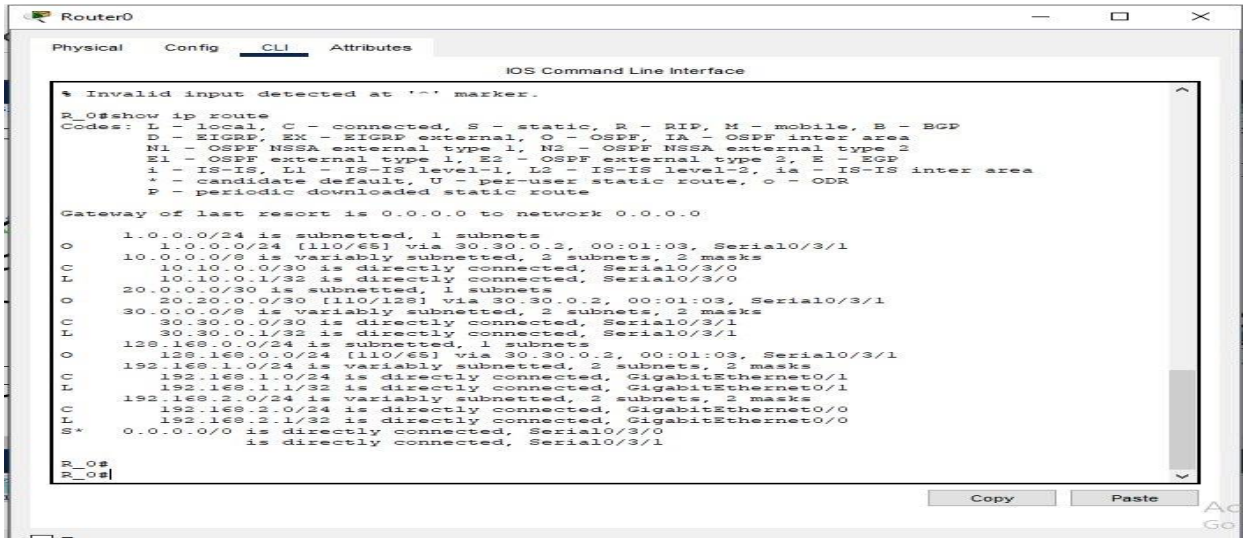
Core Concepts:

- **Router ID (RID):** Unique ID for each OSPF router, usually the highest IP on a loopback or active interface.
- **Area:** Logical grouping of networks. All OSPF networks must connect to Area 0 (the backbone area).
- **Neighbors:** Routers that exchange OSPF Hello packets.
- **DR/BDR:** Designated Router and Backup DR for multi-access networks to reduce OSPF traffic.
- **LSA (Link State Advertisement):** Used by routers to advertise their links.
- **LSDB (Link State Database):** Contains the full OSPF topology.

How OSPF Works (Simplified)

- Routers send Hello packets to discover neighbors.
- They establish adjacencies with neighbors.
- Routers exchange LSAs (Link State Advertisement) describing their network links.
- Each router builds the LSDB (Link State Database) from received LSAs.
- The router runs the SPF algorithm to calculate the shortest paths.

Routing table



OSPF Configuration on R-0

```
R-0#show running-config | section ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 30.30.0.0 0.0.0.3 area 0
 network 10.10.0.0 0.0.0.3 area 0
```

OSPF Configuration on R-1

```
R-1#show running-config | section ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 10.10.0.0 0.0.0.3 area 0
 network 20.20.0.0 0.0.0.3 area 0
```

OSPF Configuration on R-2

```
R-2#show running-config | section ospf
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 128.168.0.0 0.0.0.255 area 0
 network 1.0.0.0 0.0.0.255 area 0
 network 20.20.0.0 0.0.0.3 area 0
 network 30.30.0.0 0.0.0.3 area 0
```

OSPF Neighbor Table

```
R-0#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:34    30.30.0.2       Serial0/3/1
2.2.2.2           0   FULL/  -        00:00:37    10.10.0.2       Serial0/3/0
```

OSPF Database (LSDB)

```
R-0#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1019        0x80000008 0x00a2cd 6
2.2.2.2         2.2.2.2         1021        0x80000008 0x000688 6
3.3.3.3         3.3.3.3         1021        0x80000008 0x00e703 6
```

Security Considerations:

1. **SSH Configuration for Secure Remote Access**

   In this project, we implemented SSH (Secure Shell) to enable secure remote management of routers and switches. By configuring SSH, we ensured that remote access to network devices is encrypted and protected from unauthorized access. This setup replaces insecure protocols like Telnet and allows us to manage the network infrastructure securely from remote terminals.

   SSH was configured on each router and switch to allow encrypted command-line access using a secure username and password, providing a safe and efficient way to manage devices remotely.

Basic Configuration and SSH enabling

```
line con 0
 password 7 08701E1D5D4C
 login
!
line aux 0
!
line vty 0 4
 password 7 08701E1D5D
 login
 transport input ssh
line vty 5 15
 password 7 08701E1D5D
 login
 transport input ssh
!
!
!
end
```

2. Port Security Configuration for Switch Access Control

In this project, Port Security was configured to enhance the security of switch ports by controlling access based on MAC addresses. We applied the three different violation modes on different switches:

- Shutdown mode on S-Internet-Lab – the port is disabled upon violation.
- Protect mode on S-Computer-Dep – frames from unknown MAC addresses are dropped silently.
- Restrict mode on the remaining switches– unknown traffic is dropped and a security violation is logged.

```
S-Internet-lab#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)       (Count)        (Count)
---------------------------------------------------------------------
       Fa0/1        1           1              0         Shutdown
       Fa0/2        1           1              0         Shutdown
       Fa0/3        1           1              0         Shutdown
       Fa0/4        1           1              0         Shutdown
       Fa0/5        1           0              0         Shutdown
       Fa0/6        1           1              0         Shutdown
       Fa0/7        1           0              0         Shutdown
       Fa0/8        1           0              0         Shutdown
       Fa0/9        1           0              0         Shutdown
      Fa0/10        1           0              0         Shutdown
      Fa0/11        1           0              0         Shutdown
      Fa0/12        1           0              0         Shutdown
      Fa0/13        1           0              0         Shutdown
      Fa0/14        1           0              0         Shutdown
      Fa0/15        1           0              0         Shutdown
      Fa0/16        1           0              0         Shutdown
      Fa0/17        1           0              0         Shutdown
      Fa0/18        1           0              0         Shutdown
      Fa0/19        1           0              0         Shutdown
      Fa0/20        1           0              0         Shutdown
      Fa0/21        1           0              0         Shutdown
      Fa0/22        1           0              0         Shutdown
      Fa0/23        1           0              0         Shutdown
      Fa0/24        1           0              0         Shutdown
---------------------------------------------------------------------
```

```
S-Computer-Dep#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)       (Count)        (Count)
---------------------------------------------------------------------
       Fa0/1        1           1              0         Protect
       Fa0/2        1           0              0         Protect
       Fa0/3        1           1              0         Protect
       Fa0/4        1           1              0         Protect
       Fa0/5        1           1              0         Protect
       Fa0/6        1           1              0         Protect
       Fa0/7        1           0              0         Protect
       Fa0/8        1           0              0         Protect
       Fa0/9        1           0              0         Protect
      Fa0/10        1           0              0         Protect
      Fa0/11        1           0              0         Protect
      Fa0/12        1           0              0         Protect
      Fa0/13        1           0              0         Protect
      Fa0/14        1           0              0         Protect
      Fa0/15        1           0              0         Protect
      Fa0/16        1           0              0         Protect
      Fa0/17        1           0              0         Protect
      Fa0/18        1           0              0         Protect
      Fa0/19        1           0              0         Protect
      Fa0/20        1           0              0         Protect
      Fa0/21        1           0              0         Protect
      Fa0/22        1           0              0         Protect
      Fa0/23        1           0              0         Protect
      Fa0/24        1           0              0         Protect
---------------------------------------------------------------------
```

```
S-IT-Dep#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)       (Count)        (Count)
---------------------------------------------------------------------
       Fa0/1        1           1              0         Restrict
       Fa0/2        1           0              0         Restrict
       Fa0/3        1           1              0         Restrict
       Fa0/4        1           1              0         Restrict
       Fa0/5        1           1              0         Restrict
       Fa0/6        1           1              0         Restrict
       Fa0/7        1           1              0         Restrict
       Fa0/8        1           0              0         Restrict
       Fa0/9        1           0              0         Restrict
      Fa0/10        1           0              0         Restrict
      Fa0/11        1           0              0         Restrict
      Fa0/12        1           0              0         Restrict
      Fa0/13        1           0              0         Restrict
      Fa0/14        1           0              0         Restrict
      Fa0/15        1           0              0         Restrict
      Fa0/16        1           0              0         Restrict
      Fa0/17        1           0              0         Restrict
      Fa0/18        1           0              0         Restrict
      Fa0/19        1           0              0         Restrict
      Fa0/20        1           0              0         Restrict
      Fa0/21        1           0              0         Restrict
      Fa0/22        1           0              0         Restrict
      Fa0/23        1           0              0         Restrict
      Fa0/24        1           0              0         Restrict
---------------------------------------------------------------------
```

3. DHCP Snooping Configuration

is a security feature available on most Cisco switches. It acts as a firewall between untrusted hosts and trusted DHCP servers, filtering DHCP messages and protecting the network from rogue (unauthorized) DHCP servers, DHCP starvation, and spoofing attacks.

When do PCs accept IPs from a rogue DHCP server?

When DHCP snooping is OFF, the switch does not block DHCP server messages from any port. So, any DHCP server on the network can respond to DHCP requests. If the rogue DHCP server answers before the real DHCP server, the client will accept the rogue IP lease. This usually happens if:

- The rogue DHCP server is physically closer (lower network latency).
- The rogue DHCP server's response arrives faster.

The client sends a broadcast DHCP Discover, and rogue DHCP server replies quickly.

Victim PCs don't distinguish between "legitimate" or "fake" DHCP servers so they accept the first valid offer they get.

What are the consequences?

Victim PCs get wrong IP address, gateway, or DNS.

This can cause:

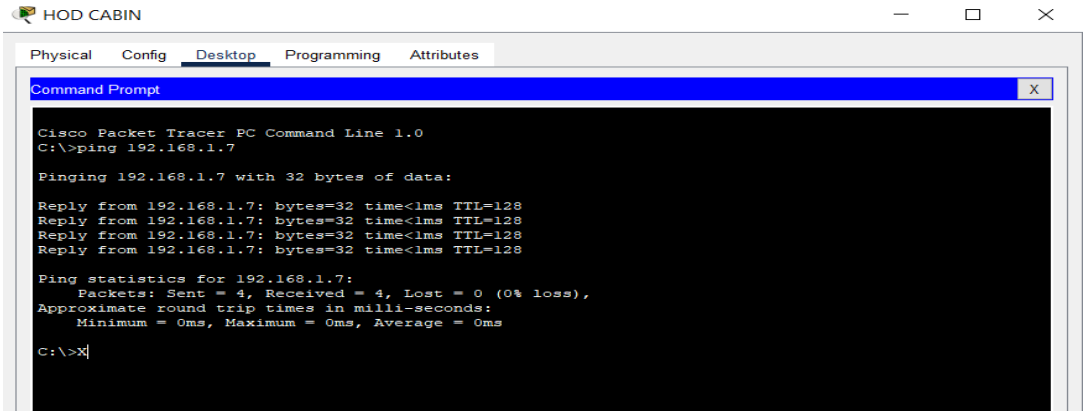
Attack Type	Brief Description	Consequence
1. Man-in-the-Middle (MITM)	The attacker pretends to be the default gateway and intercepts traffic.	Attacker can **read, modify, or steal data** (passwords, logins...).
2. Denial of Service (DoS)	Attacker gives wrong or duplicated IPs to devices to cause confusion	Devices lose network/internet access
3. DNS Spoofing	Attacker provides fake DNS server to redirect users to **fake websites**.	Victims may enter sensitive data on **phishing sites**.
4. Loss of Connectivity	Devices receive incorrect network settings (IP, Gateway, DNS).	Device is **completely disconnected** from the network.

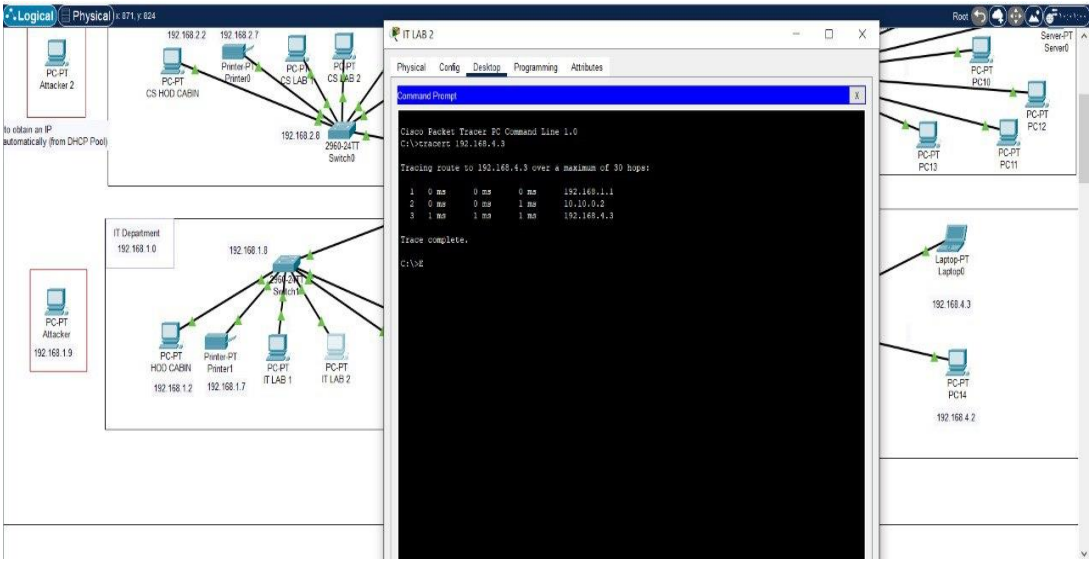
```
S-other#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/9            yes        unlimited
FastEthernet0/3            no         unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/7            no         unlimited
FastEthernet0/5            no         unlimited
S-other#
```

Testing Connectivity & Verification

- Basic Configuration: Devices were pinged successfully, confirming proper IP setup.

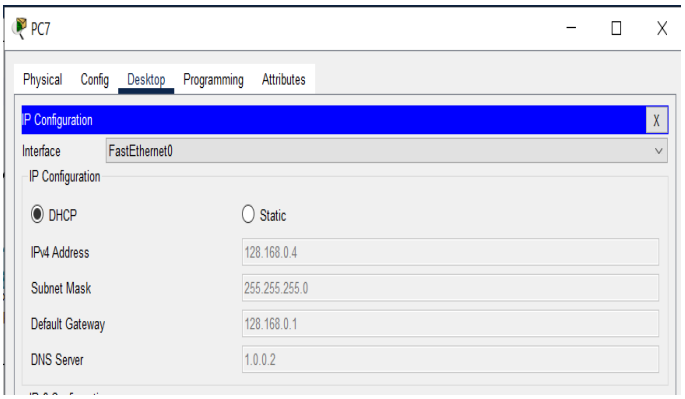
Pinging verification from 192.168.1.1 to 192.168.1.7



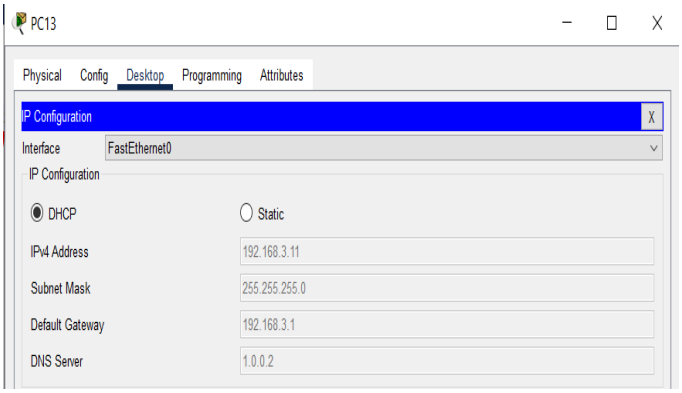


- DHCP: Devices received IPs automatically; reserved addresses were excluded correctly.

Automatic IP from DHCP via router

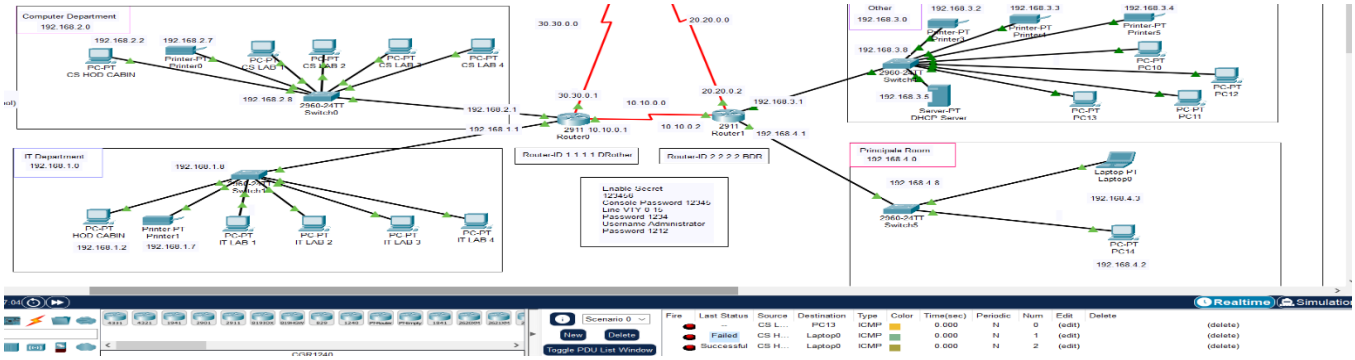


Automatic IP from DHCP via DHCP Server



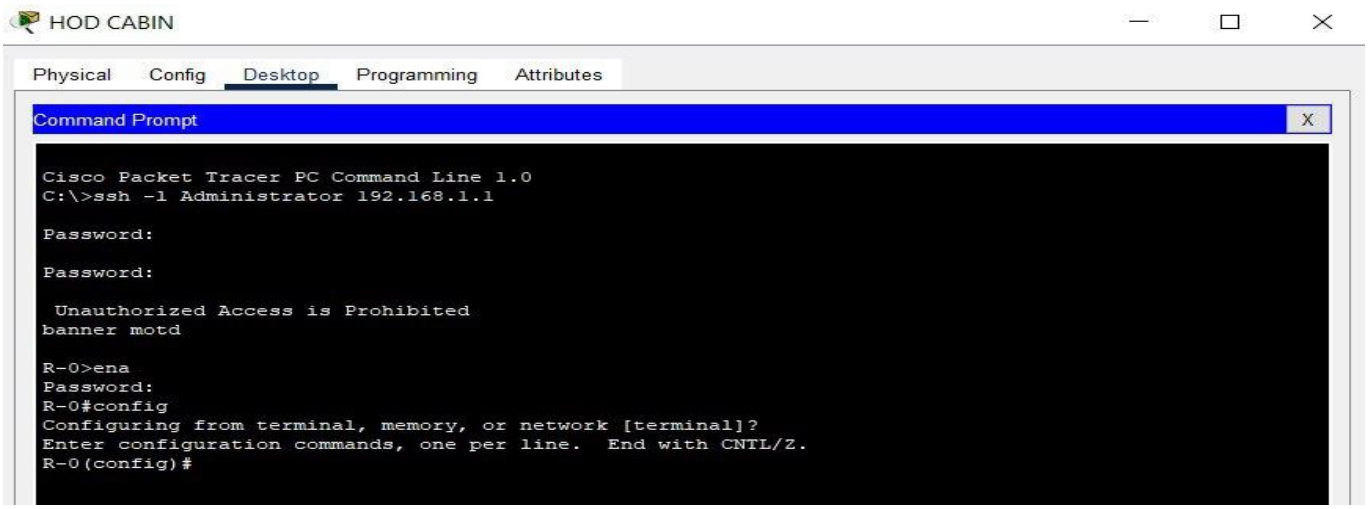
- OSPF: Routes appeared correctly in routing tables using show ip route.

Due to using OSPF (routing protocol) all the networks can connect to each other ,So we tried to send a message from PC in the IT-Dep to a PC in the Principle Room to verify the connectivity.



- SSH: Remote login worked securely using encrypted access.

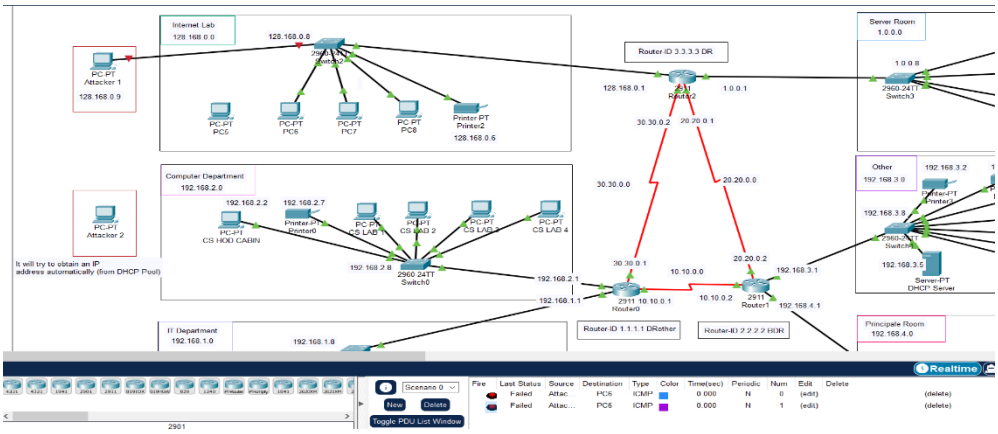
Verifying secure remote management via SSH from a client device to the router R-0.



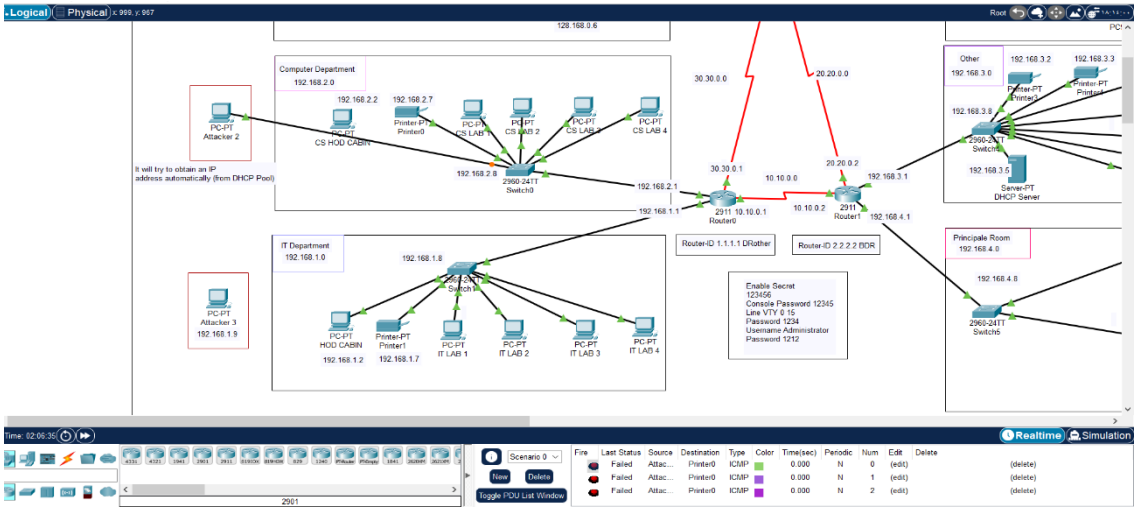
- Port Security: Unauthorized devices triggered the correct port violation actions.

The result of testing the three types of violation modes:

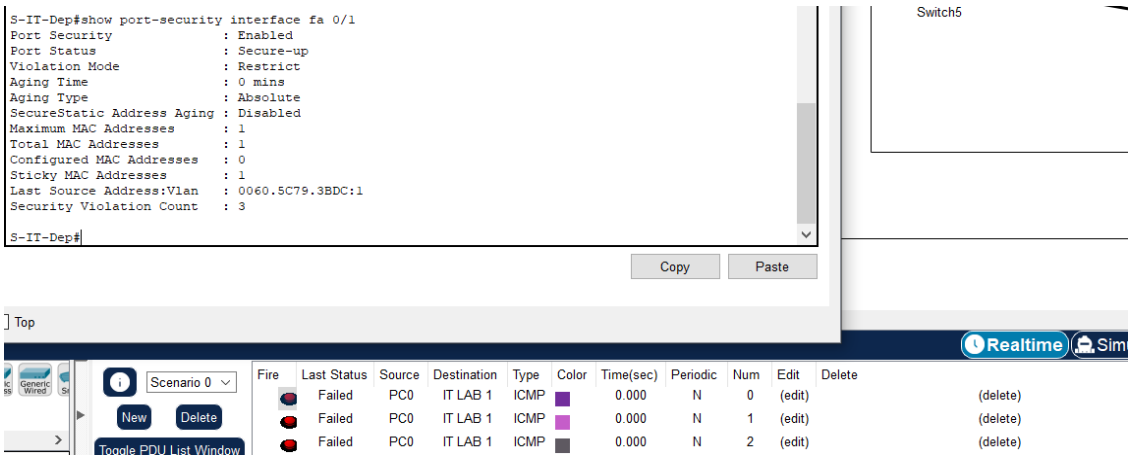
1. Testing the Shutdown mode by sending a packet from an attacker



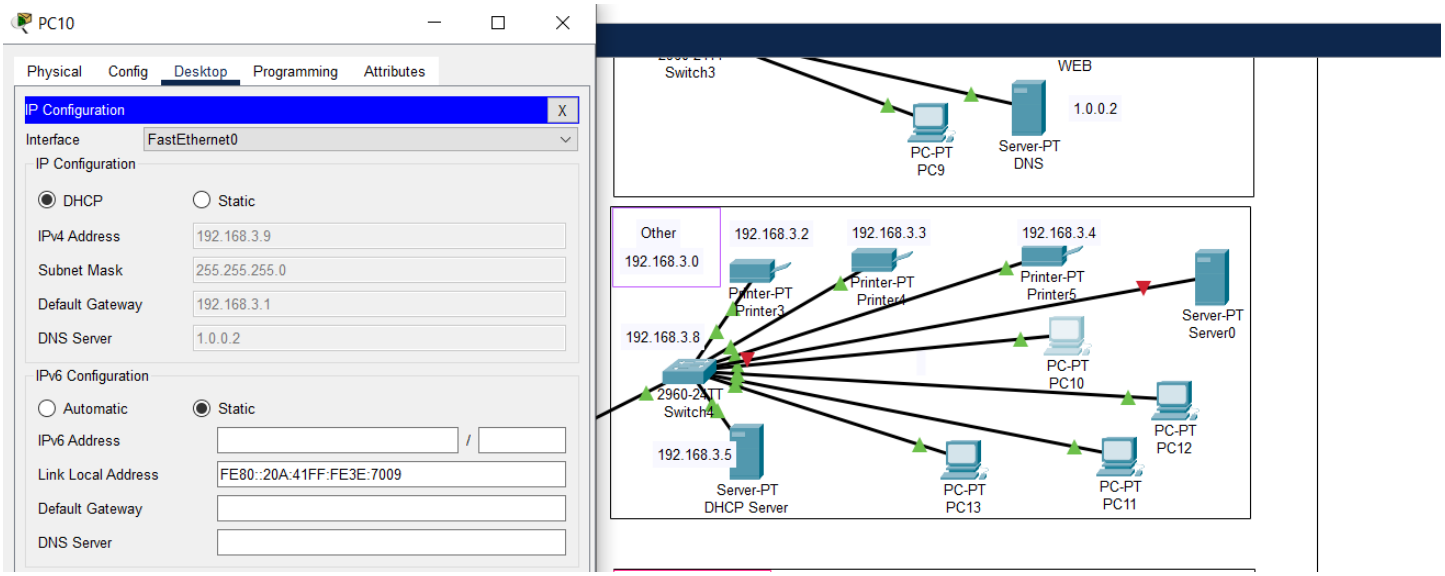
2. Testing the Protect mode by sending a packet from an attacker



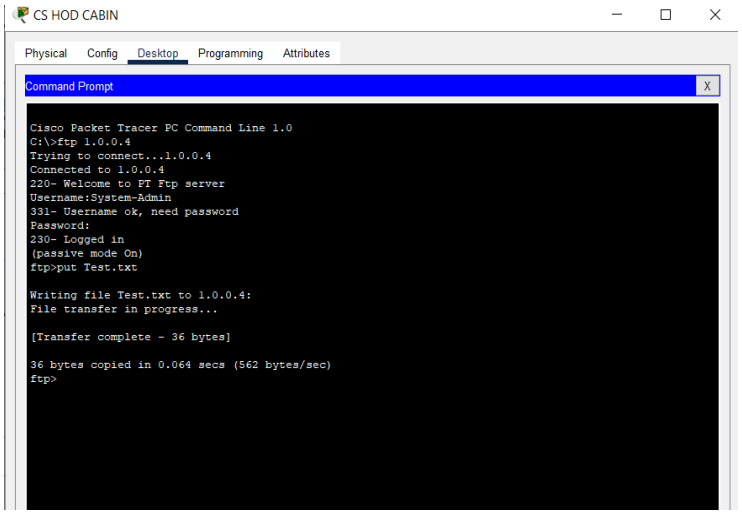
3.Testing the Restrict mode by sending a packet from an attacker



➢ DHCP Snooping: Rogue DHCP offers were blocked on untrusted ports.



➢ The result of requesting services from FTP , Web , and DNS Server



Future Enhancements

• Implement VLANs:

Dividing the network into VLANs for each department would improve performance and security.

• Advanced Security Configurations:

Add Access Control Lists (ACLs)

• Add Network Monitoring Tools:

Implement SNMP or other monitoring solutions to track performance and detect issues quickly.

Conclusion

This project helped us understand and apply key networking concepts using Cisco Packet Tracer. We successfully configured devices with IP addresses, set up dynamic IP assignment using DHCP and implemented secure routing with OSPF. Features like SSH, Port Security and DHCP Snooping added extra layers of security and control to the network.

Throughout the process, We faced real-world issues such as misconfigurations and connectivity problems, which improved our troubleshooting skills. This experience gave us a solid foundation in building and securing networks and We are excited to keep learning and exploring more advanced setups in the future.