



University of Information Technology
Faculty of Computer Systems and Technologies
CST – 32406 Network Design and Engineering
Network Design (Individual Assessment)

Presented by Thiri Shwe Sin
(UIT-1145)

September 2023

Introduction

This is an individual network project for designing and implementing a campus network topology. In this project, a simple network design for the medium-sized technology training school is implemented using Cisco Packet Tracer, a powerful simulation tool for designing networks. The necessary configurations and experiments will also be done with the use of Cisco Packet Tracer.

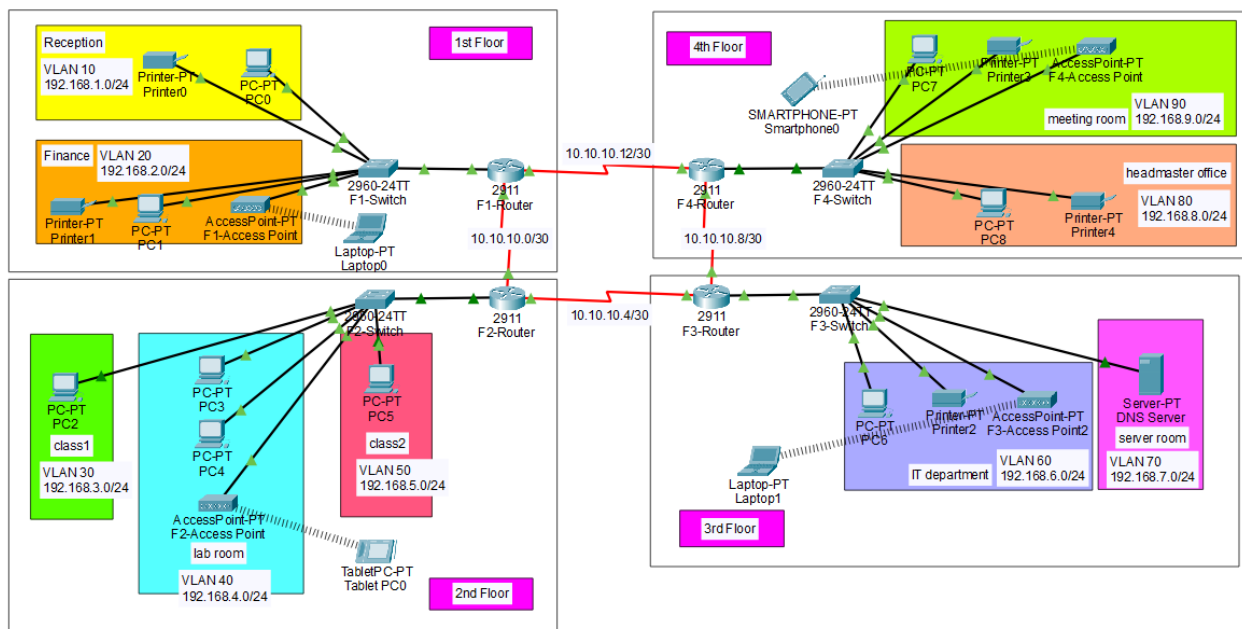
Part A: Design Scenario

This network design is intended for a medium-sized technology training school called Tech Academy. As for the medium-sized campus, a simple network design is implemented based on four routers and four layer 2 switches along with other additional devices such as access points, pcs, printers, etc..... The school consists of four floors and the network design for each floor is as follows:

1. 1st Floor – On the first floor, there are two departments, Reception and Finance. Both departments have their own PCs, and Printers. There is an access point in the Finance Department.
2. 2nd Floor – There are two classrooms and one lab room on the second floor of the school. Both the classrooms have one PC each while the lab room contains two PCs and an access point.
3. 3rd Floor – The third floor has two sections with the IT department and the Server room. The IT department has one PC, one printer and one access point and there is a DNS server in the server room.

4. 4th Floor – The meeting room and headmaster office is located on the fourth floor of the school. Each room has its own PC and printer, but the access point is placed only in the meeting room.

For the connection between devices, routers, and layer 2 switches are used in this topology. This network design contains a total of four routers with each router connecting to each floor of the building. All these routers are connected to each other using DCE cable. They are then connected to the respective switches of each floor. Each switch is also connected to the devices of its corresponding floor. Moreover, an access point is installed on each floor to provide WIFI networks connected to laptops, phones, and tablets.



Network Design for Tech Academy

Part B: Technologies Used

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to automatically assign the IP addresses to devices on a network. It provides reliable IP configuration, eliminating the need for manual configuration which can cause potential errors. Moreover, dynamically allocating addresses also helps in the efficient use of available IP addresses. It also reduces network administration as the administrators no longer need to assign the IP addresses manually. Besides, DHCP servers allow for centralized control, making the network more efficient, scalable, and easier to administer. In this design, each router is configured as a DHCP server to provide dynamic IP allocation.

VLAN

Virtual Local Area Network known as (VLAN) is a way to create separate, isolated networks within a larger physical network. Although the devices are in separate networks, VLAN allows them to communicate as if they're on the same network. Moreover, VLANs are used for many good reasons such as simplified network administration, security, and better performance. In this design, each department is grouped as a separate VLAN and there is a total of 9 VLANs for the whole building.

Floor	Department	VLAN	Network	Subnet Mask
1 st Floor	Reception	10	192.168.1.0	255.255.255.0
	Finance	20	192.168.2.0	255.255.255.0

2 nd Floor	Class1	30	192.168.3.0	255.255.255.0
	Lab Room	40	192.168.4.0	255.255.255.0
	Class2	50	192.168.5.0	255.255.255.0
3 rd Floor	IT	60	192.168.6.0	255.255.255.0
	Server Room	70	192.168.7.0	255.255.255.0
4 th Floor	Headmaster Office	80	192.168.8.0	255.255.255.0
	Meeting Room	90	192.168.9.0	255.255.255.0

Inter-VLAN Routing

Inter VLAN routing is a process that allows communication between different VLANs within a network. This routing technique forward traffic between different VLANs by implementing a router or layer 3 switch in the network. By default, devices within a VLAN can communicate with each other, but they cannot directly communicate with devices in other VLANs. Therefore, the Inter-VLAN Routing is used to enable the traffic flow between VLANs. There are several methods to achieve inter-VLAN routing such as Router on a stick, SVI interface or L3 interfaces. However, only router on a stick method is used in this type of network design. ROAS is a technique to connect a router with a single physical link to a switch and perform IP routing between VLANs. The router's interface is divided into sub-interfaces, which acts as a default gateway to their respective VLANs. The router then routes traffic between these VLANs.

OSPF

Open Shortes Path First known as OSPF is a link-state routing protocol used in computer networks. It is used to determine the best path for routing IP packets within an autonomous system. It is one of the Interior Gateway Protocols (IGPs) used for routing within an autonomous system. Due to the scalability, security, and efficiency, OSPF routing protocol is widely used nowadays, and our design also uses OSPF as the routing protocol to advertise routes.

SSH

Secure Shell or SSH is a cryptographic network protocol for operating network services securely over an unsecured network. It gives users, particularly system administrators, a secure way to access a computer over an unsecured network. The primary purpose of SSH is to provide a secure means of connecting to a remote system. It encrypts the data transmitted between the client and the server, making it much more difficult for unauthorized parties to intercept the communication. Moreover, SSH is used for a wide range of purposes, including remote system administration, secure file transfers, tunneling of network traffic, and even for secure access to web services. In this network design, SSH is configured in all the routers for remote login.

Switchport Security

Switchport security is a part of the security measures to prevent unauthorized access to a network. This type of security helps to secure the physical ports on the

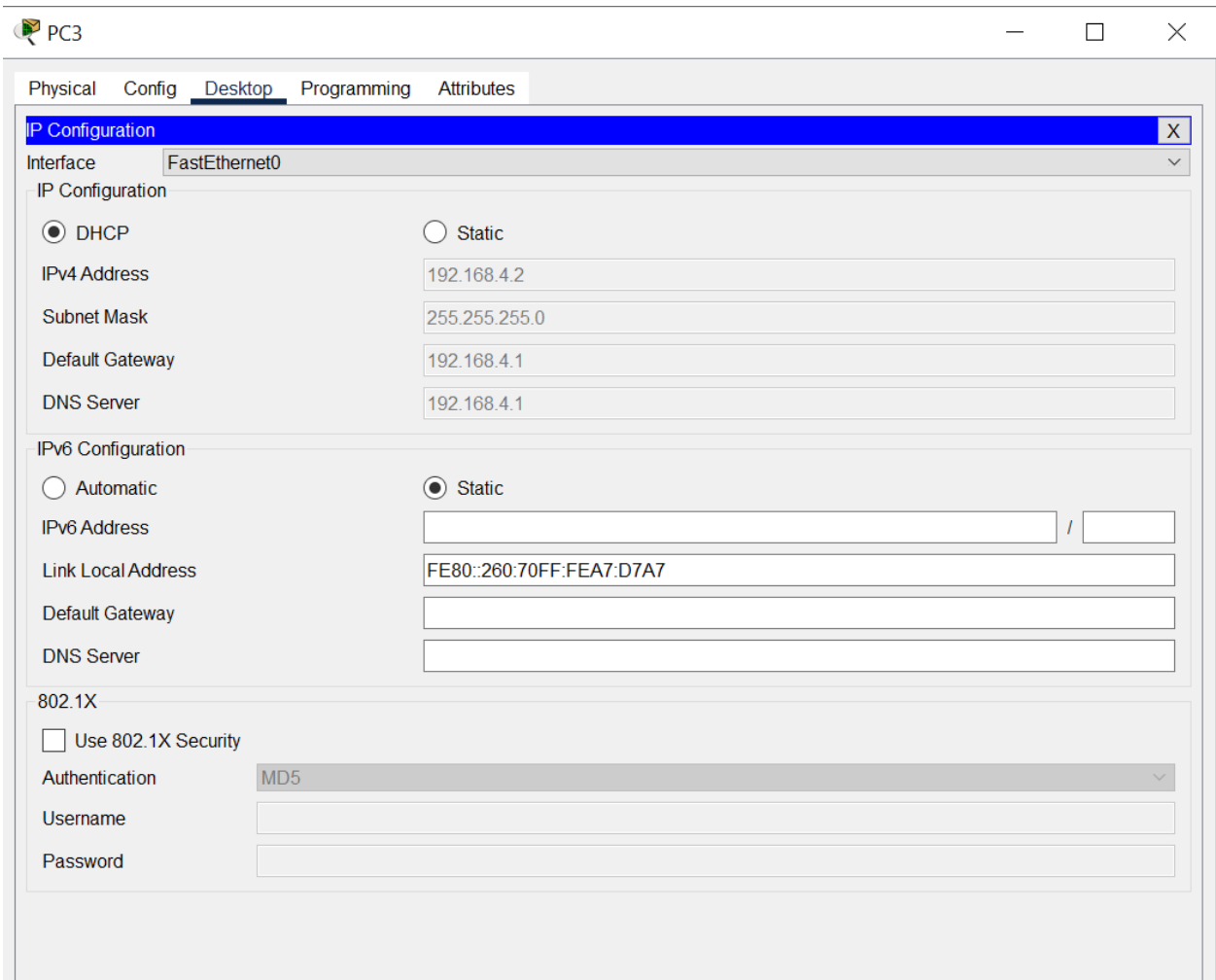
switch by controlling which devices are allowed to connect to them. Switchport security feature offers the ability to configure a switchport so that traffic can be limited to only a specific configured MAC address or list of MAC addresses. There are several methods to obtain port security on the switches such as static secure MAC addresses, dynamic secure MAC addresses, sticky secure MAC addresses etc.....

- Static secure MAC addresses—This type of secure MAC address is statically configured on a switchport and is stored in an address table and in the running configuration.
- Dynamic secure MAC addresses—This type of secure MAC address is learned dynamically from the traffic that is sent through the switchport. These types of addresses are kept only in an address table and not in the running configuration.
- Sticky secure MAC addresses—This type of secure MAC address can be manually configured or dynamically learned. These types of addresses are kept in an address table and in the running configuration.

This campus network design uses sticky MAC addresses method to control and manage access to network ports on a switch, preventing unauthorized users to access the LAN.

Part C: Experiments

DHCP



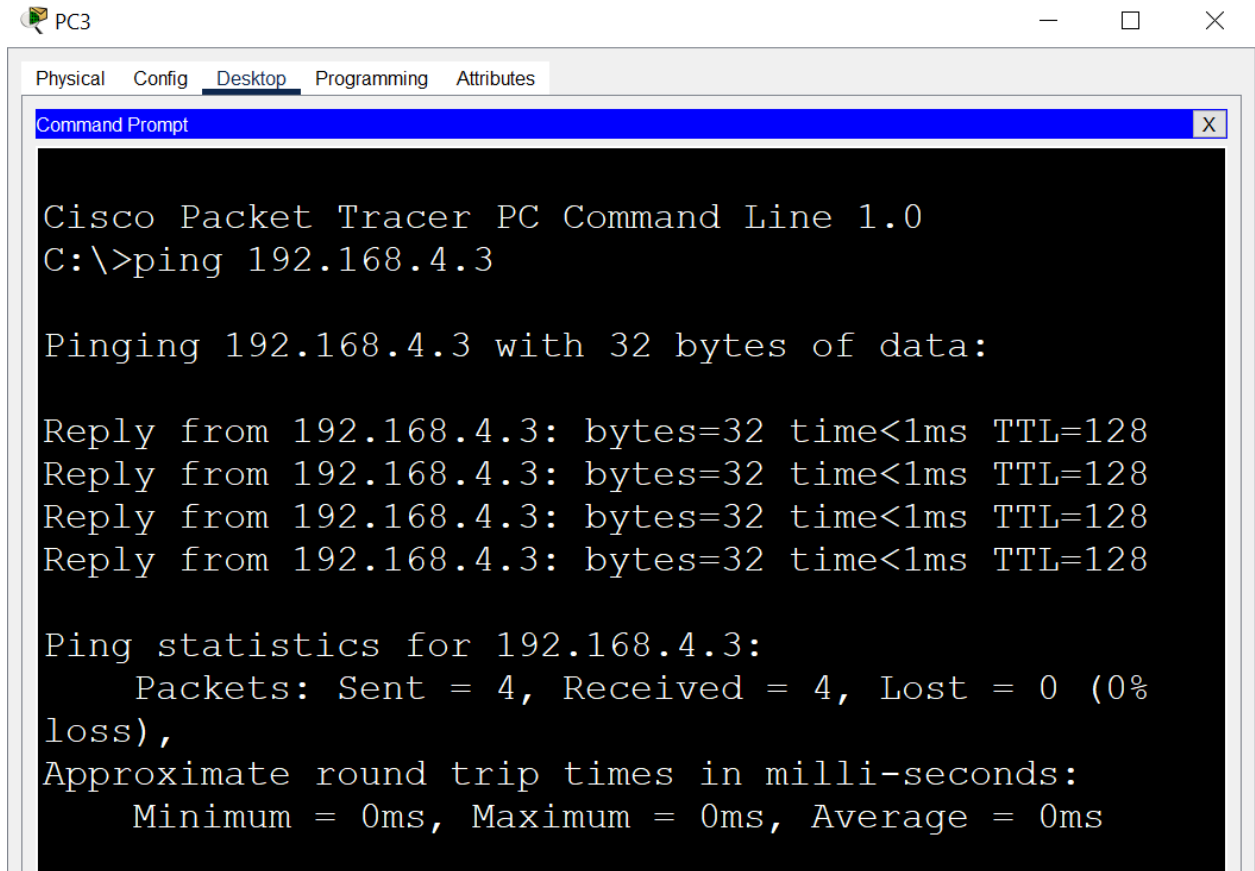
The screenshot shows a configuration window for PC3 with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying the IP Configuration for the FastEthernet0 interface. The IP Configuration section has two radio buttons: DHCP (selected) and Static. Below these are input fields for IPv4 Address (192.168.4.2), Subnet Mask (255.255.255.0), Default Gateway (192.168.4.1), and DNS Server (192.168.4.1). The IPv6 Configuration section has two radio buttons: Automatic and Static (selected). Below these are input fields for IPv6 Address (empty), Link Local Address (FE80::260:70FF:FEA7:D7A7), Default Gateway (empty), and DNS Server (empty). The 802.1X section has a checkbox for Use 802.1X Security (unchecked), a dropdown for Authentication (MD5), and input fields for Username and Password (both empty).

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.4.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	192.168.4.1
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::260:70FF:FEA7:D7A7
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

DHCP IP Configuration on PC3

DHCP (Dynamic Host Configuration Protocol) (DHCP) is used to automatically assign the IP addresses to devices on a network. Our network design is designed to use each router as a DHCP server to allocate the IP address dynamically.

Connection within VLAN



The screenshot shows a Cisco Packet Tracer PC Command Line interface for PC3. The interface has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.3

Pinging 192.168.4.3 with 32 bytes of data:

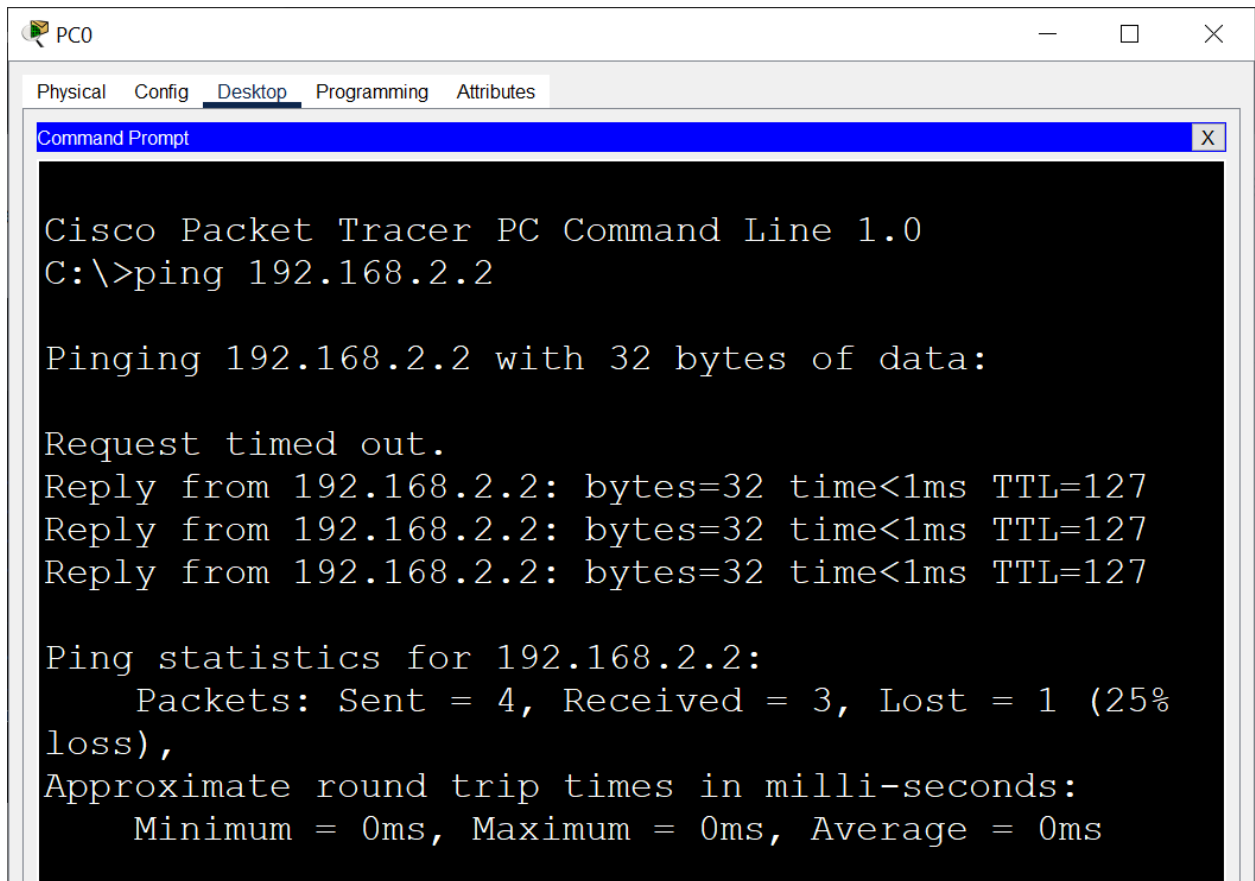
Reply from 192.168.4.3: bytes=32 time<1ms TTL=128
Reply from 192.168.4.3: bytes=32 time<1ms TTL=128
Reply from 192.168.4.3: bytes=32 time<1ms TTL=128
Reply from 192.168.4.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.4.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging successfully from PC3 to PC4 of lab room within VLAN 40

As shown in the figure, the connection between two PCs within the same VLAN (VLAN 40) is successful. Similarly, devices of other VLANs can also communicate with each other within its own VLAN.

Inter-VLAN Routing



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

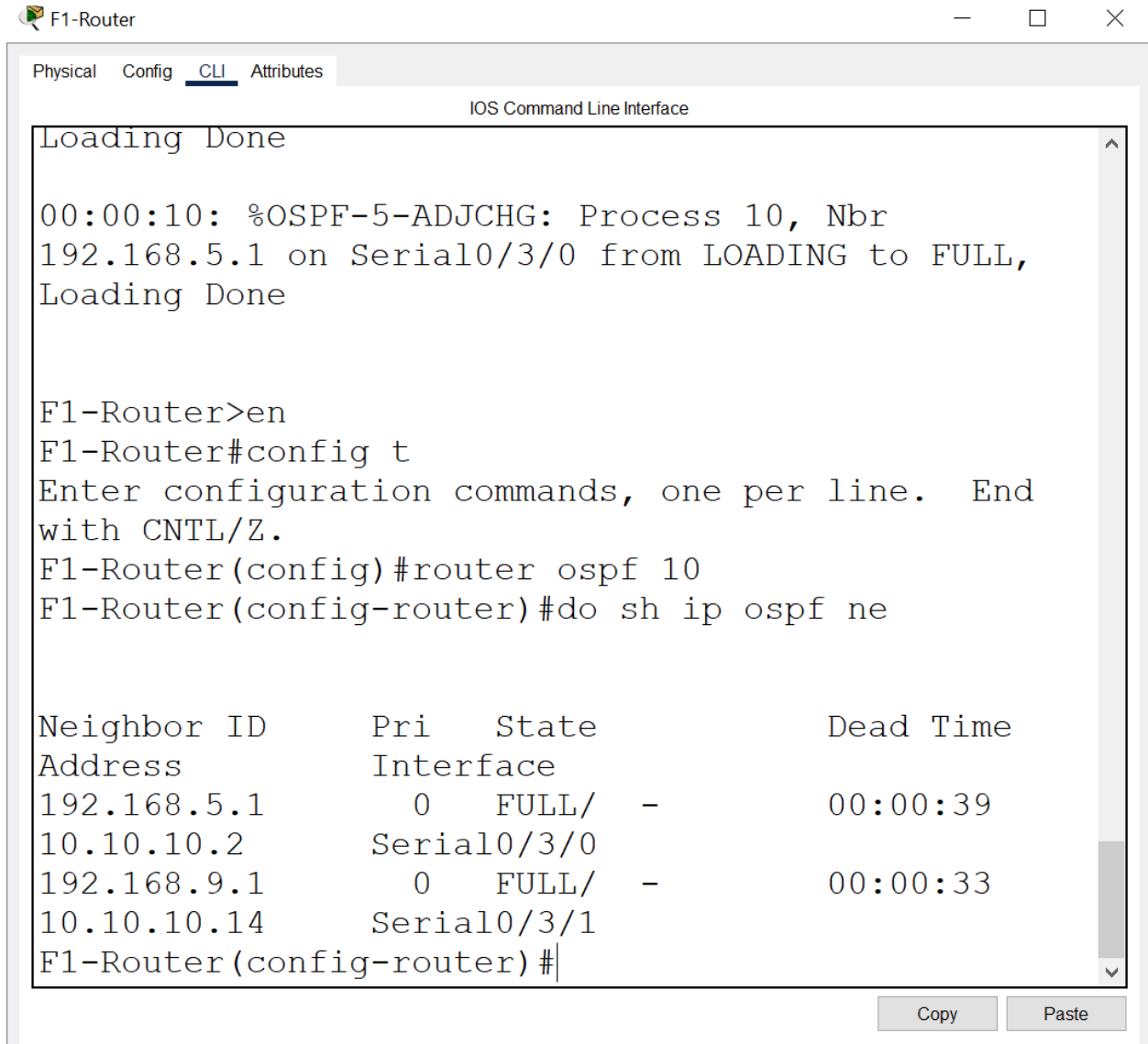
Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging successfully from PC0 of VLAN 10 to PC1 of VLAN 20

This picture shows an example of Inter-VLAN routing from Reception to Finance on floor 1. PC0 of Reception which is in VLAN 10 try to connect the PC1 of Finance Department in VLAN 20, and the connection is successful. Therefore, the communication of devices between different VLANs is achieved using Inter-VLAN routing.

OSPF



The screenshot shows the F1-Router CLI interface. The window title is 'F1-Router'. The tabs are 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The output shows the following commands and their results:

```
Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr
192.168.5.1 on Serial0/3/0 from LOADING to FULL,
Loading Done

F1-Router>en
F1-Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
F1-Router(config)#router ospf 10
F1-Router(config-router)#do sh ip ospf ne
```

Neighbor ID Address	Pri	State	Interface	Dead Time
192.168.5.1	0	FULL/	-	00:00:39
10.10.10.2			Serial0/3/0	
192.168.9.1	0	FULL/	-	00:00:33
10.10.10.14			Serial0/3/1	

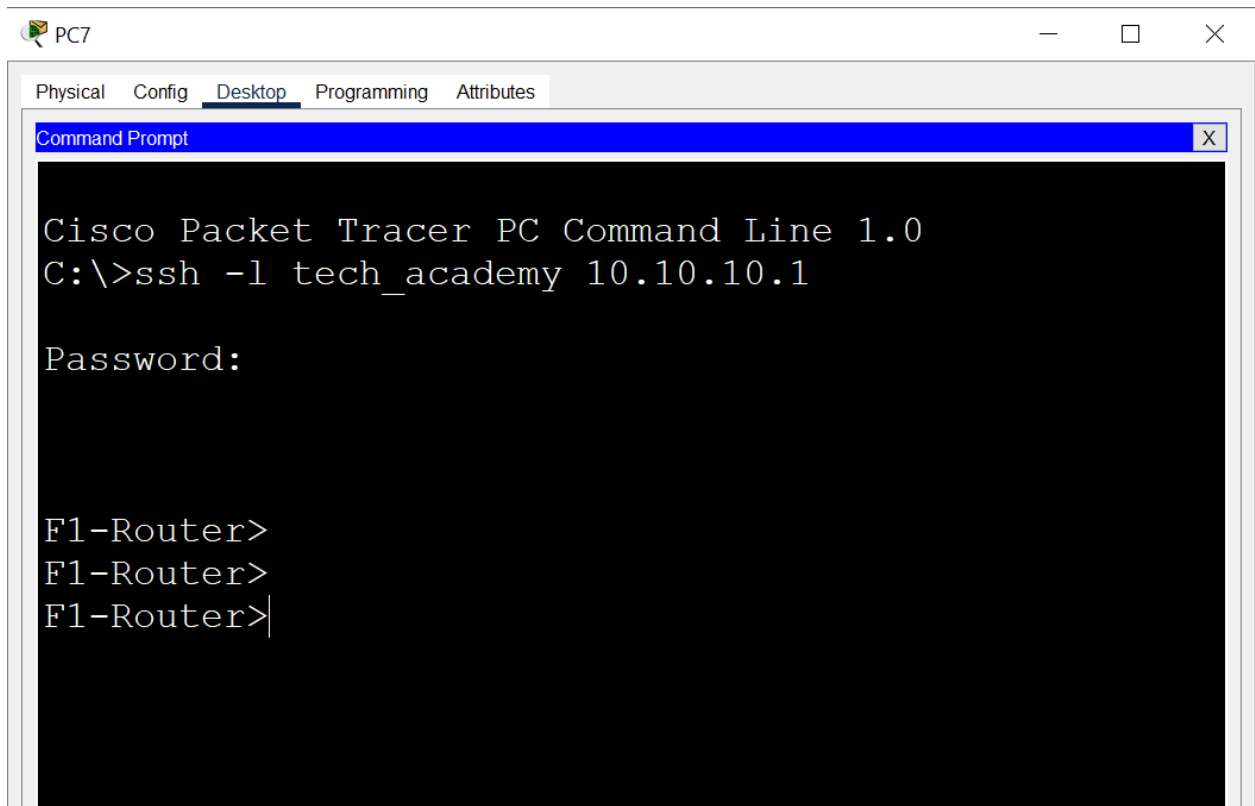
F1-Router(config-router)#

At the bottom right, there are 'Copy' and 'Paste' buttons.

OSPF neighbors of F1 Router

This network topology use OSPF as the routing protocol to advertise routes. OSPF is configured on each router to choose the best routes and the configurations are successful.

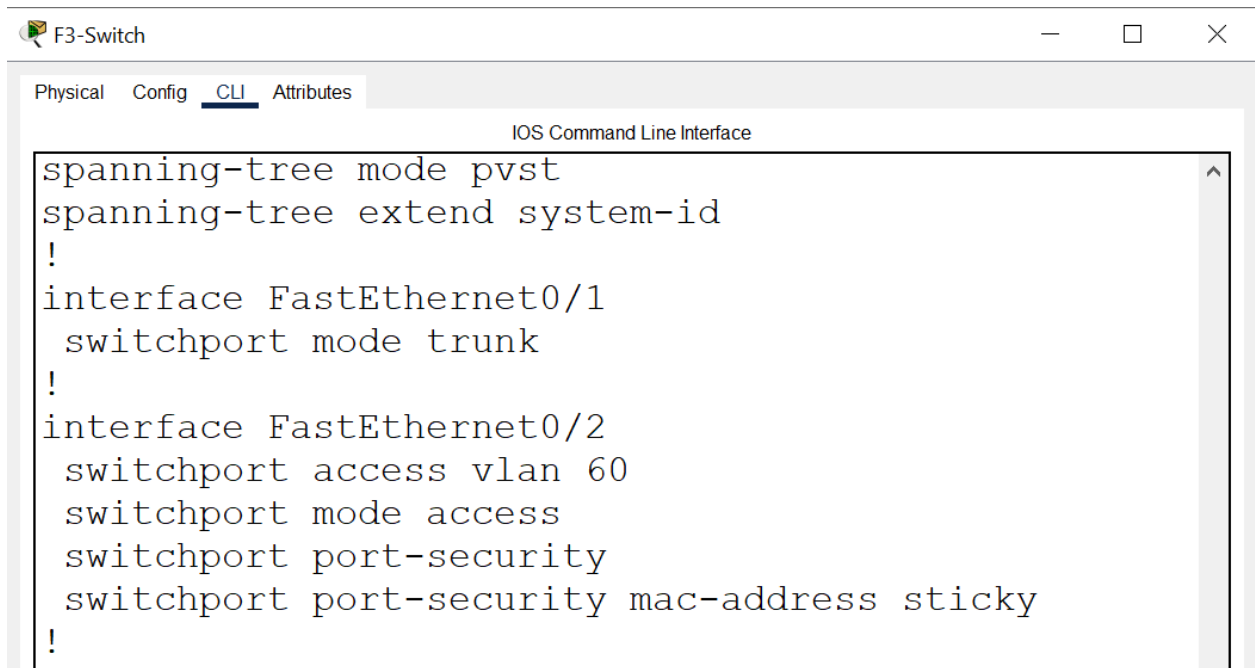
SSH remote login



SSH remote login

This is an example of SSH remote login from PC7 to F1-Router. SSH is used to encrypt the data transmitted between the client and the server, making it much more difficult for unauthorized parties to intercept the communication. And SSH is configured on every single router in this design.

Switchport Security



Switchport Security on F4-Switch

Switchport Security is configured on F4-Switch for a better and secure network and prevent unauthorized access to the network.

Conclusion

This is an individual project for designing and implementing a campus network design. The whole process of designing is completed through the use of networking simulation tool called Cisco Packet Tracer. Apart from the design process, doing this project helps me gain experience of carrying out an experiment. Moreover, practical experiment also allows me to better understand the subject. And also, working on this project made me realize how important and useful networking is in our real world.