



University of Bahrain
College of Information Technology
Department of Computer Engineering

ITCE416/ITNE241 COMPUTER NETWORKS II

ITCE416/ITNE241 Project:

Start-up Bank Branch Network

Submitted By:

Student Name: Omar Ahmed Eldanasoury
Student ID: 202005808 Section No. 02

Student Name: Hesham Ahmed Ghulam
Student ID: 202003472 Section. No. 02

Student Name: Mohamed Hesham Alammal
Student ID: 202009144 Section. No. 02

Submitted to: Dr. Reham Almesaeed.

Submitted on: 25th/Dec/2022

Content Table

Introduction:	3
Project Scope:	4
Network Diagram:	5
Network Address:	6
Interface configuration:	7
VLAN:	9
Inter-VLAN routing:	13
RIP routing protocol:	18
DHCP Server:	20
Web Server:	23
NTP Configuration:	25
Syslog Configuration:	29
SSH Configuration:	33
DNS Server	36
FTP Server:	39
Test the Connectivity	42
Conclusion:	45
Team Worksheet	46

Objectives:

1. Develop self-learning skills
2. Expand learner knowledge in the Network configuration in Cisco tracer.
3. Applied the skills and knowledge learned in the course to design and configure the institutional network.
4. Practicing the Cisco tracer tool.

Introduction:

The design of networks is crucial to computing. To manage data flow through technological devices, many businesses and organizations use this crucial skill. These companies and organizations can organize and plan transfer data between various locations thanks to network design.

Cisco created the Cisco packet tracer tool to simulate a real network using Cisco hardware and configurations. With the aid of this tool, companies and organizations can efficiently plan out their networks while testing the effectiveness of their network designs prior to implementation.

This project is a commission from a small start-up bank to build a network in packet tracer to help in communication between the 4 departments of Finance, Information Technology (IT), Human Resources (HR), and Reception. The network design must be efficient and secure, capable of handling the data flow from all four departments, and after the completion of the design it will be physically implemented.

Project Scope:

The scope of this project is to build an enterprise network for a small start-up bank. The network should contain sub-networks (aka. subnets) for 4 departments: IT Department, Human Resources (HR) Department, Finance Department, and Reception Department. Each subnet will have essential devices and desktop devices for the employees to complete their work. As a result, each department contains 5 devices and a shared printer. Moreover, Network services have their own subnet. These services help employees to increase their productivity. The services are put in the network and configured properly. The services include:

- 1- NTP: synchronize the clock of all the network devices.
- 2- Syslog: to make centralized storage for all the events and logs so IT employees find it easier to troubleshoot problems.
- 3- SSH: to make it easier for IT employees to troubleshoot and configure routers and switch on the network remotely.
- 4- FTP: to make it easier for employees to share files.
- 5- DNS: to support the Webserver.
- 6- Webserver: to host an essential website that employees use internally in the company to create requests, tickets, ... etc.

Many technologies - that writers used during the lab and their self-learning time – are used, including DHCP, VLANs, Inter-VLANs, and Dynamic Routing using RIP.

Network Diagram:

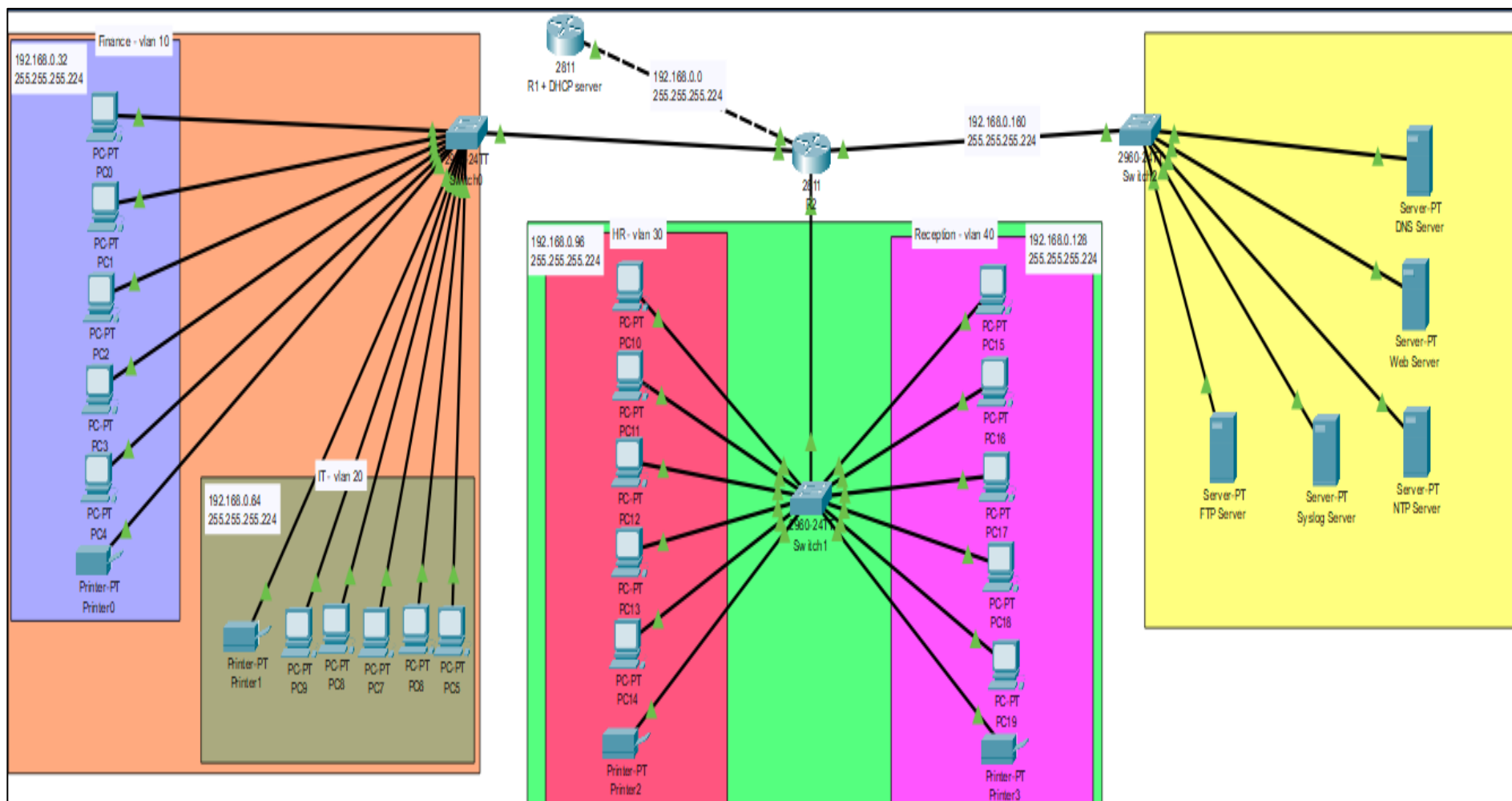


Figure 1

Network Address:

DEPARTMENT	SUBNET MASK	NETWORK ADDRESS	DEFAULT GATEWAY
FINANCE	255.255.255.224	192.168.0.0 - 192.168.0.31	192.168.0.1
IT	255.255.255.224	192.168.0.32 – 192.168.0.63	192.168.0.33
HR	255.255.255.224	192.168.0.64 – 192.168.0.95	192.168.0.65
RECEPTION	255.255.255.224	192.168.0.96 - 192.168.0.127	192.168.0.97

Interface configuration:

- Router 2

After the subnetting. Configuration of the router interfaces should be done with the IP addresses; the table below represents interfaces from R2 with IP addresses:

Interface	IP address	VLAN
Fa 0/0	192.168.0.1	No
Fa 0/1		Yes
Fa 1/0		Yes
Fa 1/1	192.168.0.161	No

To configure the interfaces with IPv4 addresses some commands have been used and you can see the commands in the figures below:

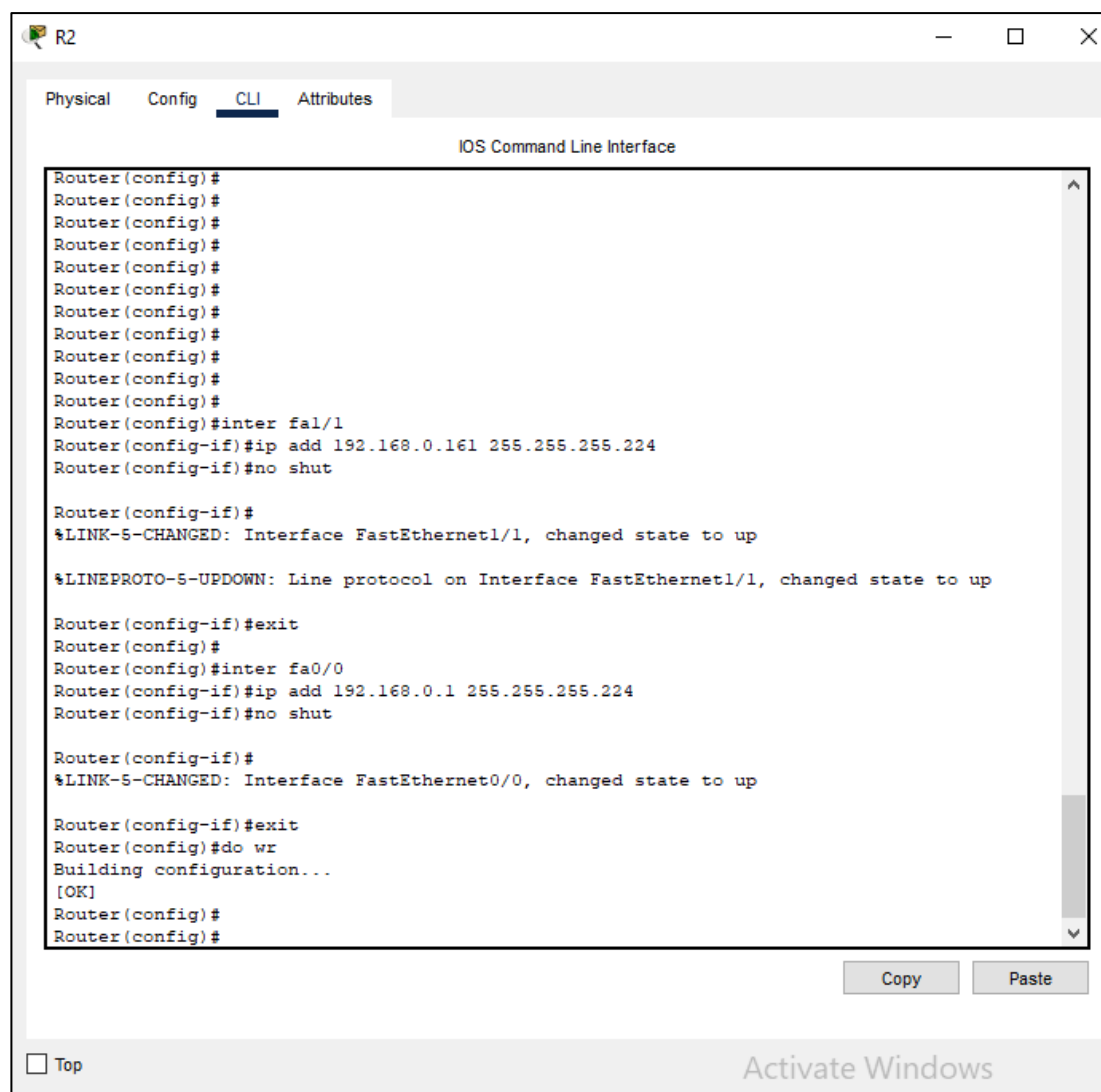


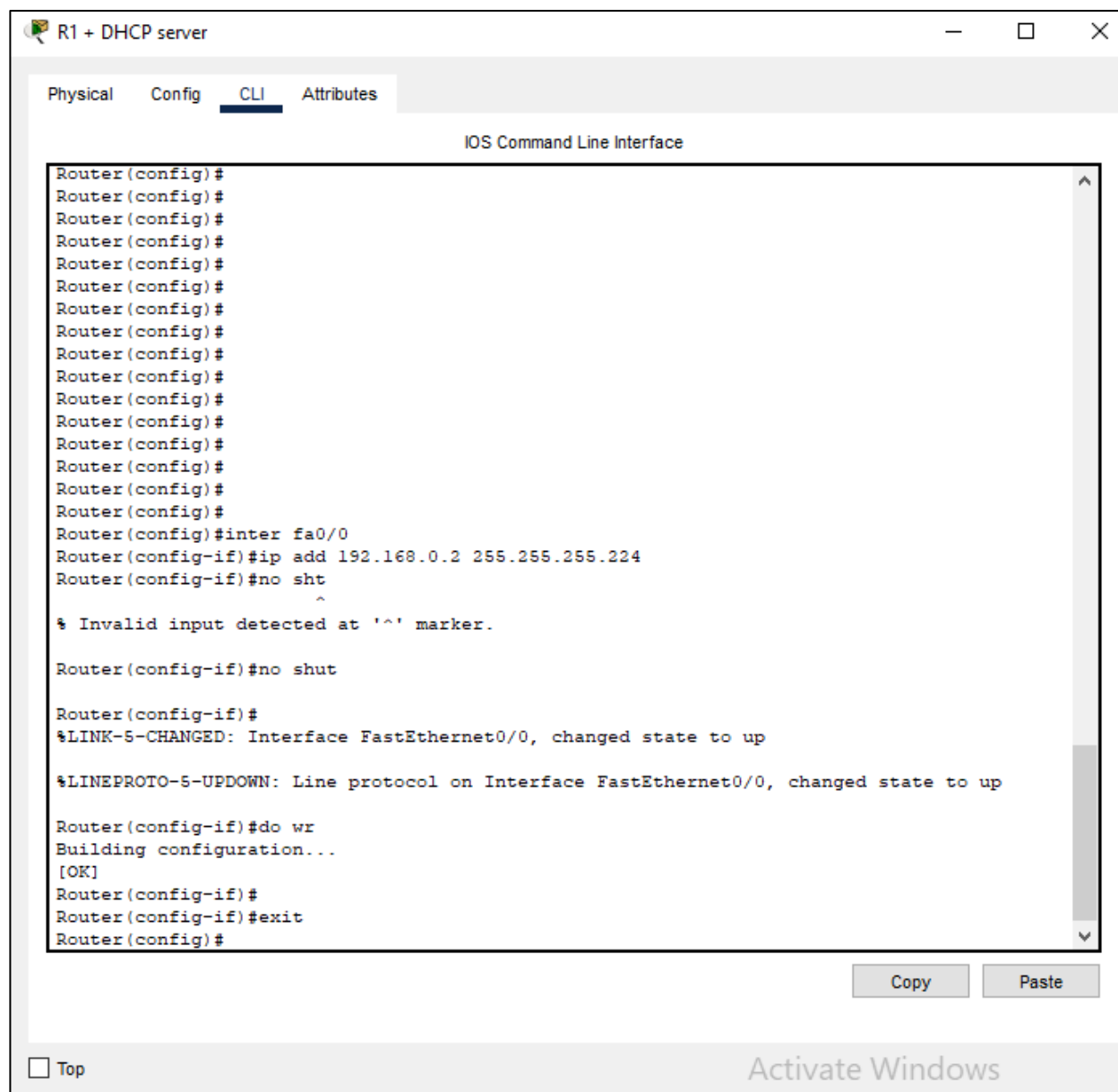
Figure 2: Interface configuration on R2

- Router 1

After the subnetting. Configuration of the router interfaces should be done with the IP addresses; the table below represents interfaces from R1 with IP addresses:

interface	IP address	VLAN
Fa 0/0	192.168.0.2	No

To configure the interfaces with IPv4 addresses some commands have been used and you can see the commands in the figures below:



```

R1 + DHCP server
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#inter fa0/0
Router(config-if)#ip add 192.168.0.2 255.255.255.224
Router(config-if)#no sht
^
% Invalid input detected at '^' marker.
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#do wr
Building configuration...
[OK]
Router(config-if)#
Router(config-if)#exit
Router(config)#
  
```

Figure 3: Interface configuration on R1

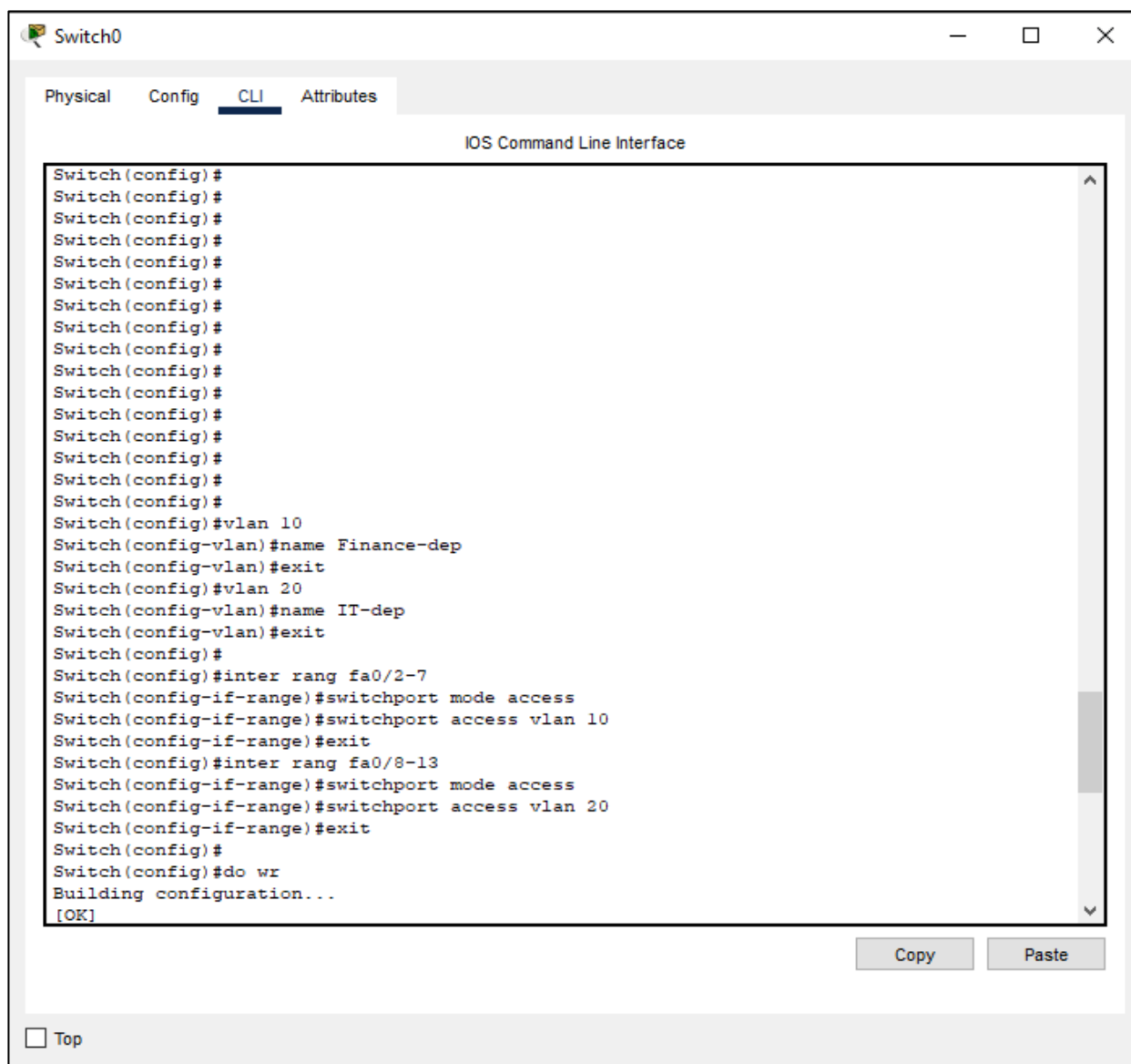
VLAN:

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN.

Here is the configuration of the VLAN on (Switch0). We applied VLANs on (switch0) for 2 departments (Finance and IT), so we can have 2 VLANs on (switch0): VLAN 10 (interface rang Fa0/2-7), VLAN 20 (interface rang Fa0/8-13).

- Switch0

To configure VLAN we used such commands, and you can see the commands in the figure below:



```
Switch0
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name Finance-dep
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name IT-dep
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#inter rang fa0/2-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#inter rang fa0/8-13
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do wr
Building configuration...
[OK]
```

Figure 4: VLAN10 & VLAN20 configuration on S0

This figure will show the VLANs we create, and the following command has been used: **show vlan**.

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config)#do show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	Finance-dep	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7
20	IT-dep	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

☐ Top

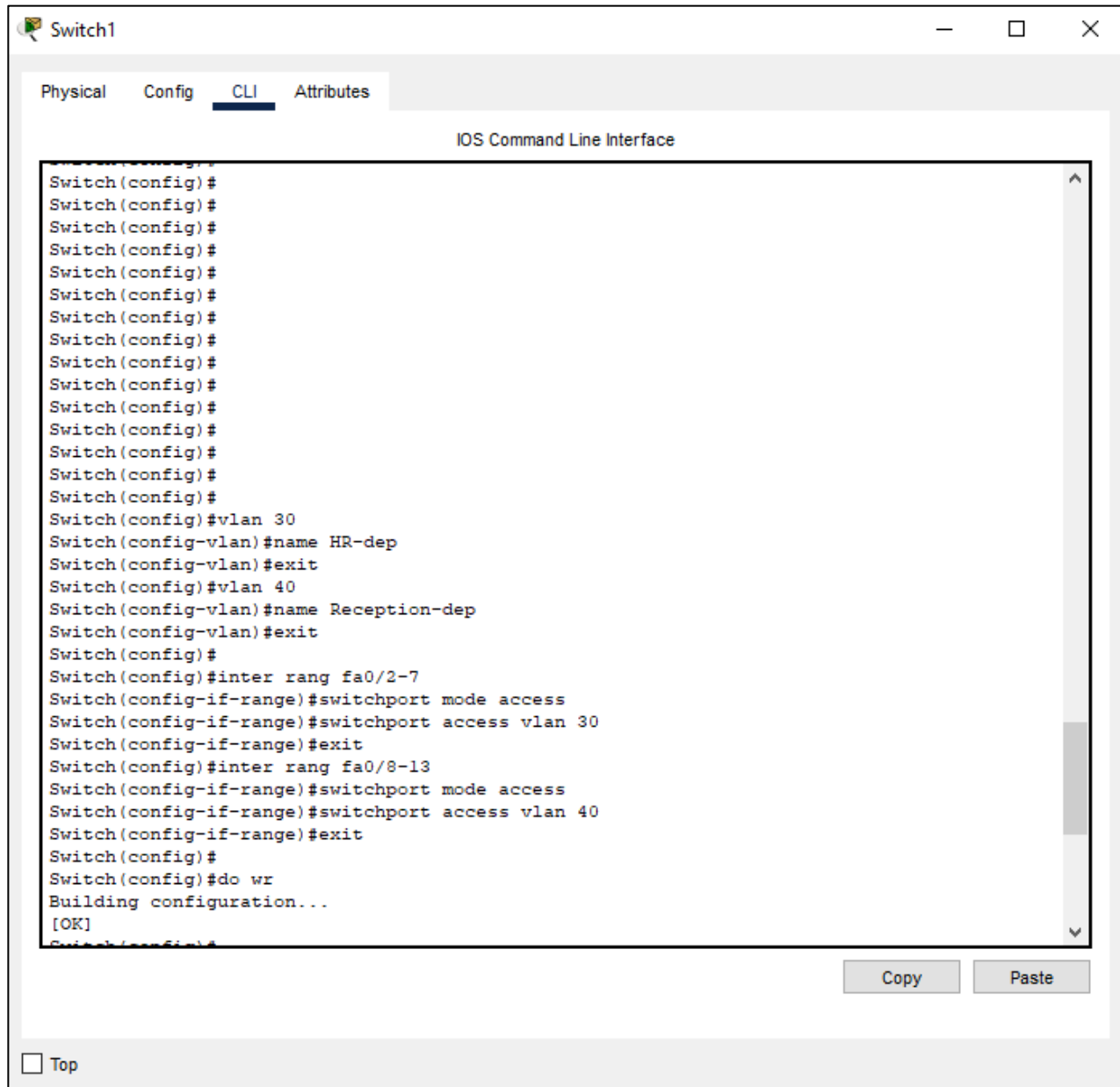
Copy Paste

Figure 5: VLAN10 & VLAN20 verification on R0

- Switch1

Also, we applied VLANs on (switch1) for 2 departments (HR and Reception), so we can have 2 VLANs on (switch1): VLAN 30 (interface rang Fa0/2-7), VLAN 40 (interface rang Fa0/8-13).

To configure VLAN we used such commands, and you can see the commands in the figure below:



The screenshot shows a window titled "Switch1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration commands entered are as follows:

```
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 30
Switch(config-vlan)#name HR-dep
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name Reception-dep
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#inter rang fa0/2-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#inter rang fa0/8-13
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do wr
Building configuration...
[OK]
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" button with a checkbox.

Figure 6: VLAN30 & VLAN40 configuration on R1

This figure will show the VLANs we create, and the following command has been used: **show vlan**.

Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config)#
Switch(config)#do show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
30	HR-dep	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7
40	Reception-dep	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

Copy Paste

☐ Top

Figure 7: VLAN30 & VLAN40 verification on S1

Inter-VLAN routing:

Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

- **Legacy Inter-VLAN routing:** This is a legacy solution. It does not scale well.
- **Router-on-a-Stick (ROAS):** This is an acceptable solution for a small- to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs):** This is the most scalable solution for medium to large organizations.

However, in our case, we will use Router-on-a-stick (ROAS). It requires only one physical Ethernet interface to route traffic between multiple VLANs on a network.

A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using subinterfaces to identify routable VLANs.

The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.

- Switch0

First, we should configure port Fa0/1 as a trunk port so that multiple VLANs can pass through this port:

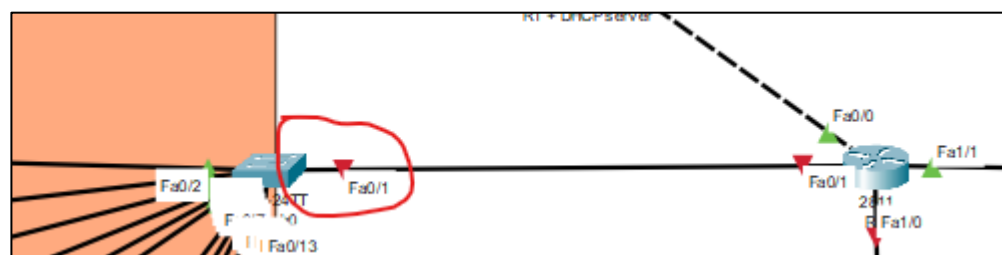
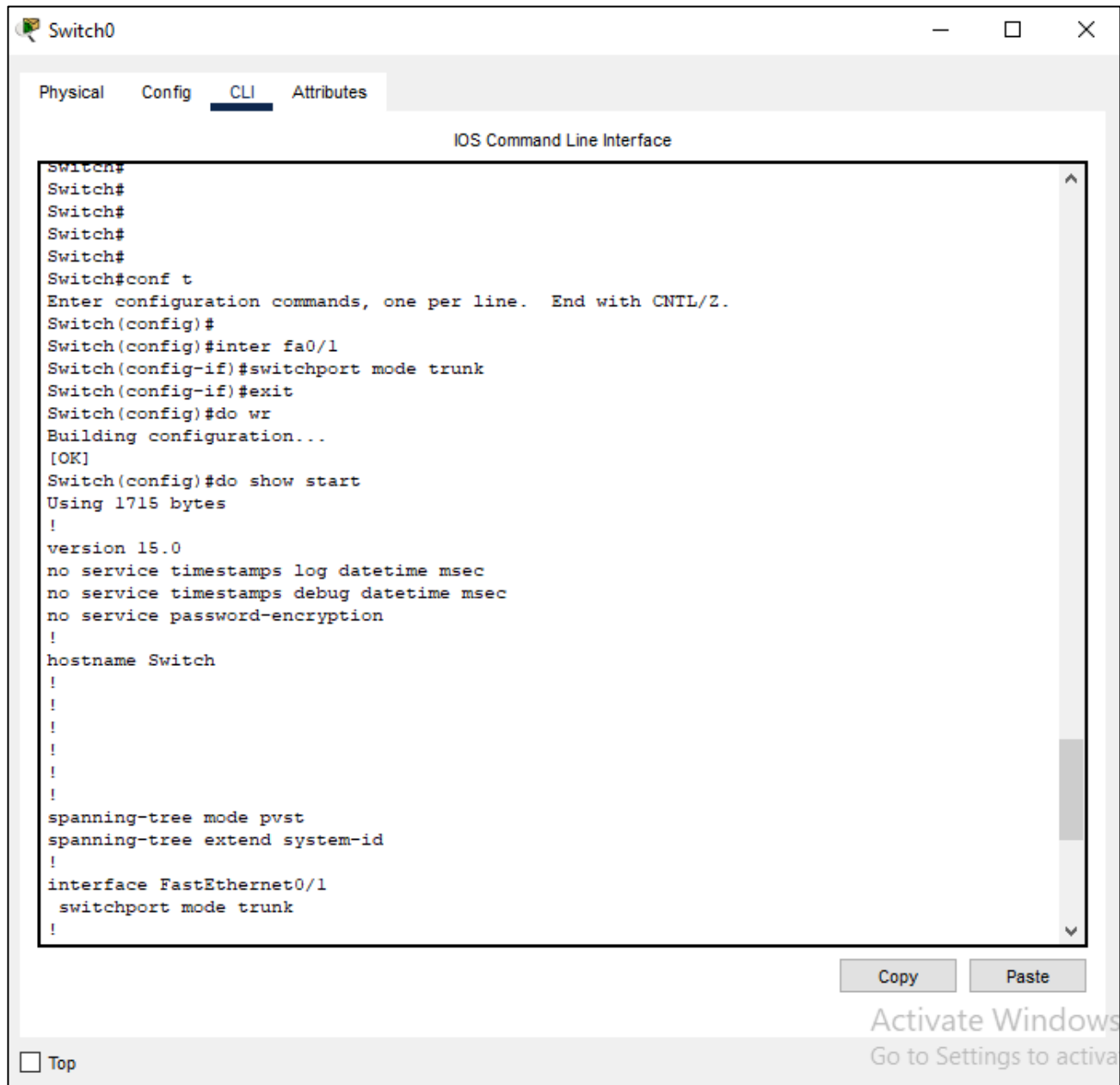


Figure 8: Trunk port (Fa0/1) on S0

The configuration of the trunk port has been done by using the following commands and you can see that the port has been configured properly at the last of this figure (**show startup configuration**) command used:



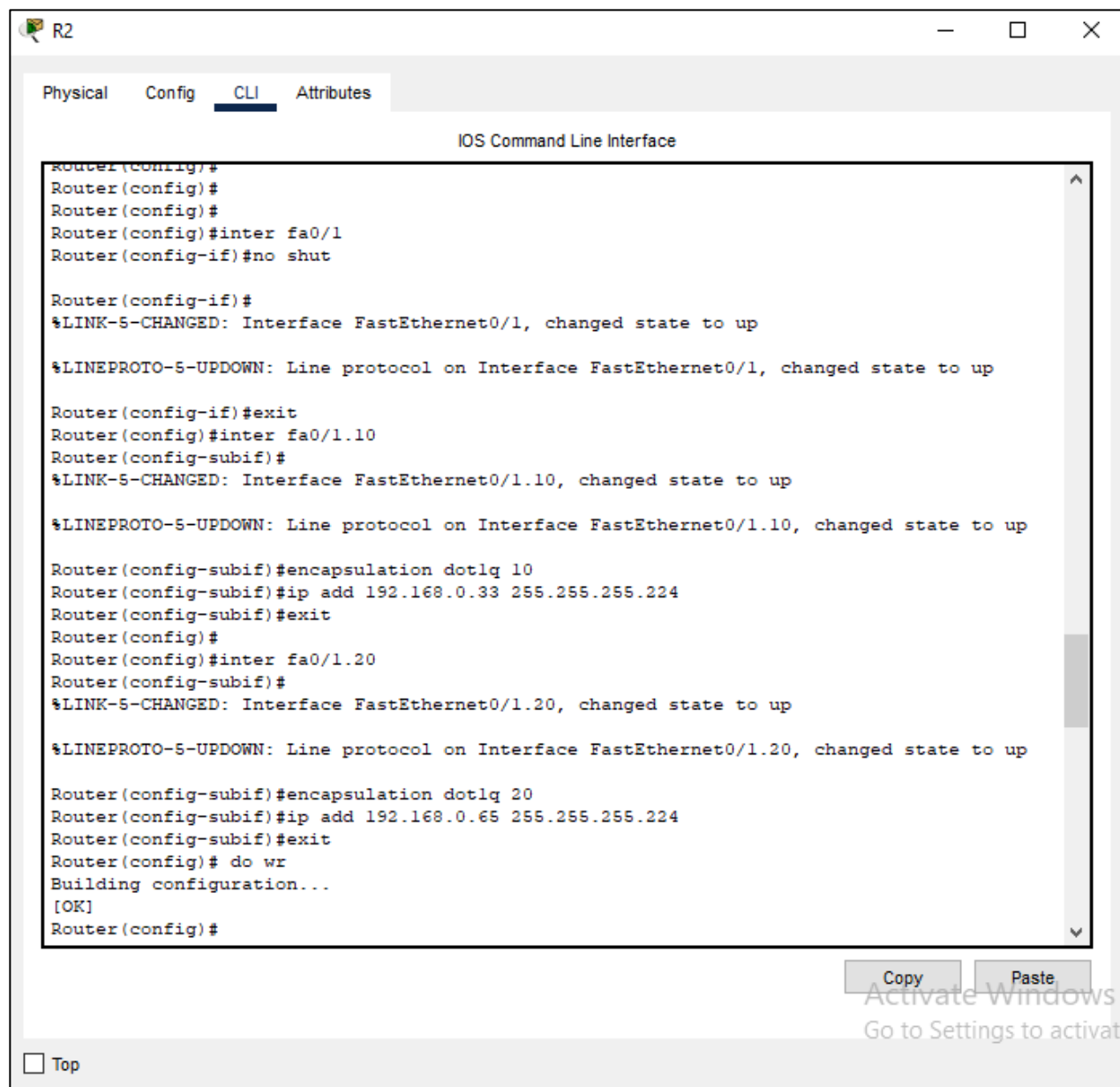
The screenshot shows a network switch window titled "Switch0" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and their results:

```
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#inter fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#do show start
Using 1715 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport mode trunk
!
```

At the bottom of the window, there are "Copy" and "Paste" buttons, a "Top" button, and a watermark for "Activate Windows".

Figure 9: Trunk port configuration & verification on S0

Then, we configured virtual sub-interfaces from a real physical interface Fa0/1. The following figures represent such commands used to do the configuration:



The screenshot shows a network simulator window titled 'R2' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The configuration commands entered are as follows:

```
Router(config)#
Router(config)#
Router(config)#inter fa0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#inter fa0/1.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.10, changed state to up

Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 192.168.0.33 255.255.255.224
Router(config-subif)#exit
Router(config)#
Router(config)#inter fa0/1.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.20, changed state to up

Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 192.168.0.65 255.255.255.224
Router(config-subif)#exit
Router(config)# do wr
Building configuration...
[OK]
Router(config)#
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. A watermark for 'Activate Windows' is visible in the background.

Figure 10: Sub-Interface configuration on R2

- Switch1

Again, we will do the same thing on (switch1), at (R2) we configured port Fa0/1 as a trunk port so that multiple VLANs can pass through this port:

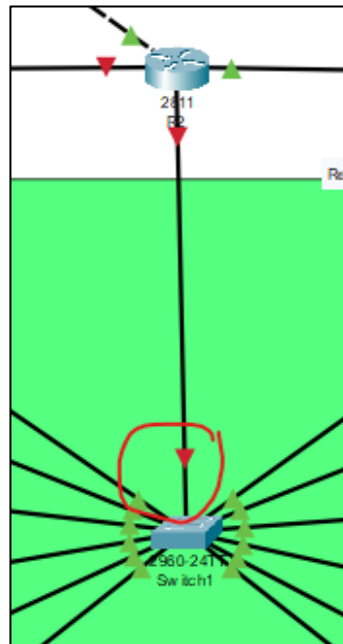


Figure 11: Trunk port (Fa0/1) on S1

The configuration of the trunk port has been done by using the following commands and you can see that the port has been configured properly at the last of this figure (**show startup configuration**) command used:

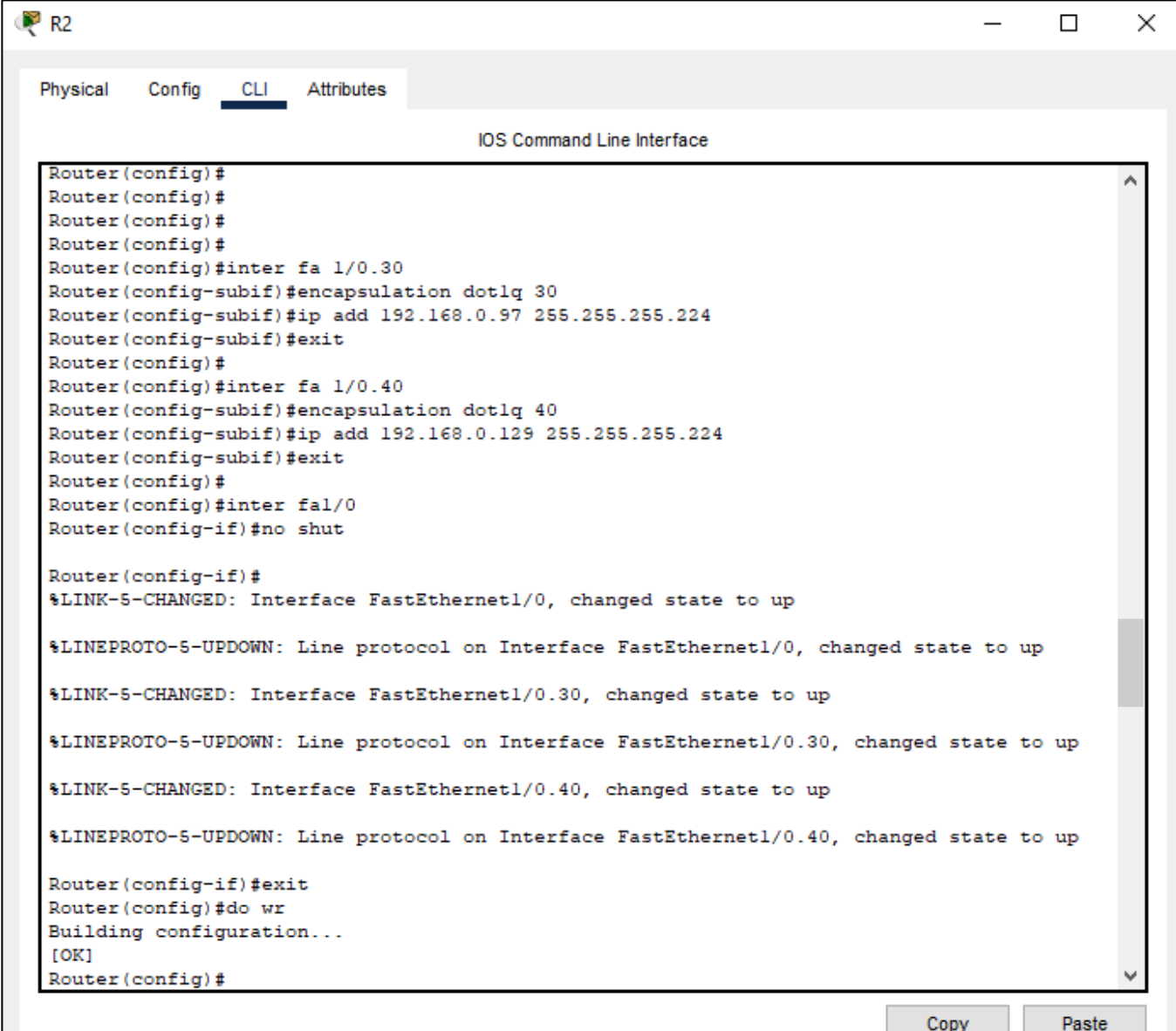
```

Switch1
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#inter fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#do show start
Using 1715 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!

```

Figure 12: Trunk port configuration & verification

Then, we configured virtual subinterfaces from a real physical interface Fa1/0. The following figures represent such commands used to do the configuration:



The screenshot shows a window titled 'R2' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#inter fa 1/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip add 192.168.0.97 255.255.255.224
Router(config-subif)#exit
Router(config)#
Router(config)#inter fa 1/0.40
Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip add 192.168.0.129 255.255.255.224
Router(config-subif)#exit
Router(config)#
Router(config)#inter fa1/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.30, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.40, changed state to up

Router(config-if)#exit
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

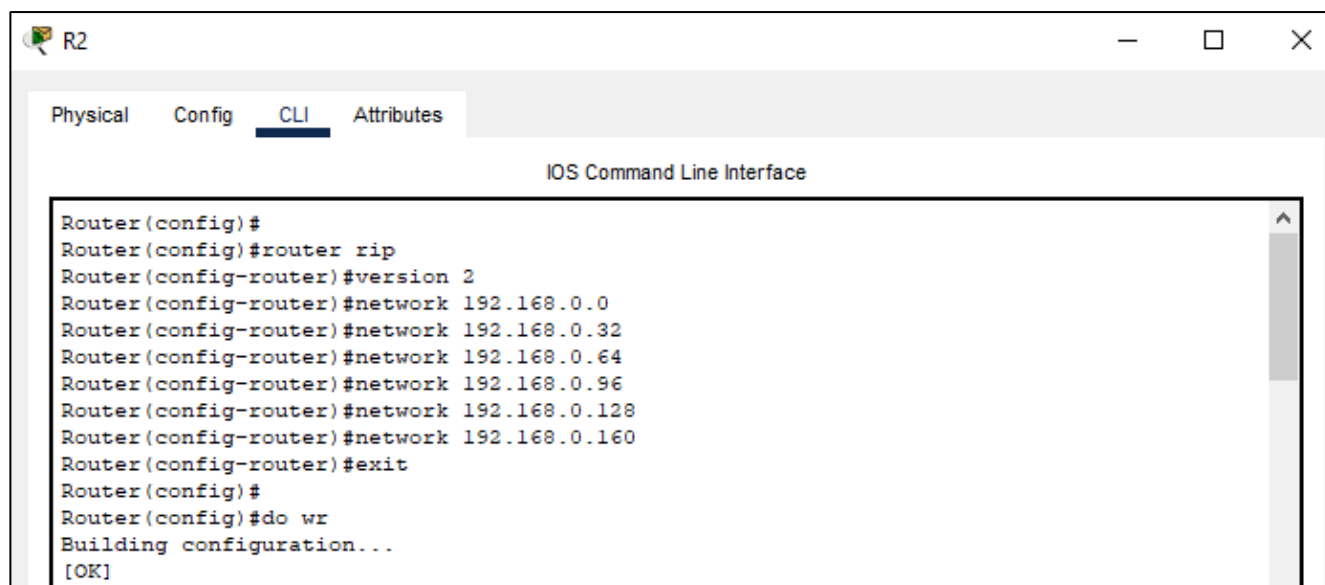
At the bottom of the window, there are 'Copy' and 'Paste' buttons.

Figure 13: Sub-Interface configuration on R2

RIP routing protocol:

Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

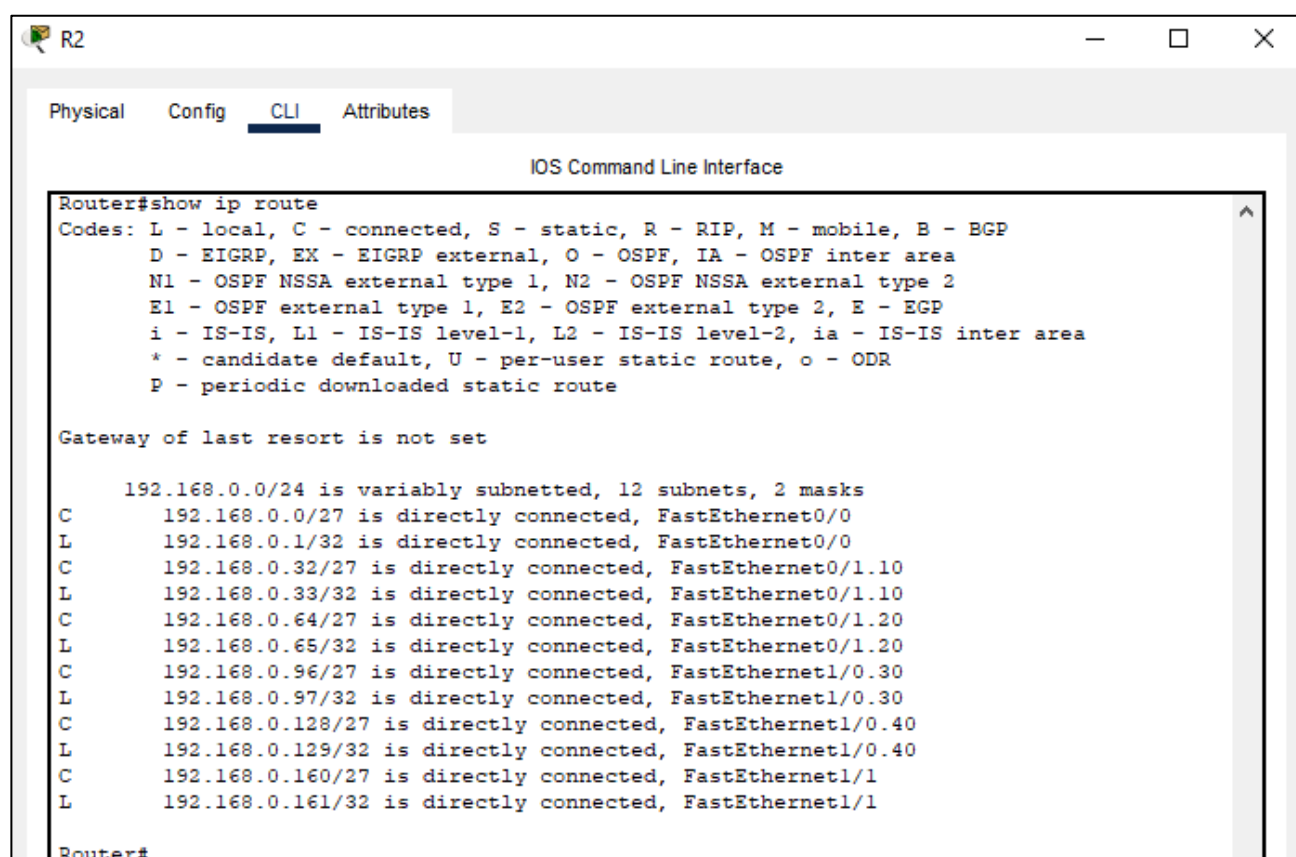
At (R2) we configured the RIPv2 routing protocol. The figure below shows the command used to do the configuration:



```
Router(config)#
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.0.32
Router(config-router)#network 192.168.0.64
Router(config-router)#network 192.168.0.96
Router(config-router)#network 192.168.0.128
Router(config-router)#network 192.168.0.160
Router(config-router)#exit
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
```

Figure 14: RIPv2 configuration on R2

The routing table of (R2):



```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.0.0/24 is variably subnetted, 12 subnets, 2 masks
C       192.168.0.0/27 is directly connected, FastEthernet0/0
L       192.168.0.1/32 is directly connected, FastEthernet0/0
C       192.168.0.32/27 is directly connected, FastEthernet0/1.10
L       192.168.0.33/32 is directly connected, FastEthernet0/1.10
C       192.168.0.64/27 is directly connected, FastEthernet0/1.20
L       192.168.0.65/32 is directly connected, FastEthernet0/1.20
C       192.168.0.96/27 is directly connected, FastEthernet1/0.30
L       192.168.0.97/32 is directly connected, FastEthernet1/0.30
C       192.168.0.128/27 is directly connected, FastEthernet1/0.40
L       192.168.0.129/32 is directly connected, FastEthernet1/0.40
C       192.168.0.160/27 is directly connected, FastEthernet1/1
L       192.168.0.161/32 is directly connected, FastEthernet1/1
Router#
```

Figure 15: RIPv2 verification

At (R1) we configured the RIPv2 routing protocol. The figure below shows the command used to do the configuration and at the same time you can see the routing table of (R1):

R1 + DHCP server

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router(config)#
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.0.0
Router(config-router)#exit
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.0.0/24 is variably subnetted, 7 subnets, 2 masks
C       192.168.0.0/27 is directly connected, FastEthernet0/0
L       192.168.0.2/32 is directly connected, FastEthernet0/0
R       192.168.0.32/27 [120/1] via 192.168.0.1, 00:00:24, FastEthernet0/0
R       192.168.0.64/27 [120/1] via 192.168.0.1, 00:00:24, FastEthernet0/0
R       192.168.0.96/27 [120/1] via 192.168.0.1, 00:00:24, FastEthernet0/0
R       192.168.0.128/27 [120/1] via 192.168.0.1, 00:00:24, FastEthernet0/0
R       192.168.0.160/27 [120/1] via 192.168.0.1, 00:00:24, FastEthernet0/0

Router#
```

Copy Paste

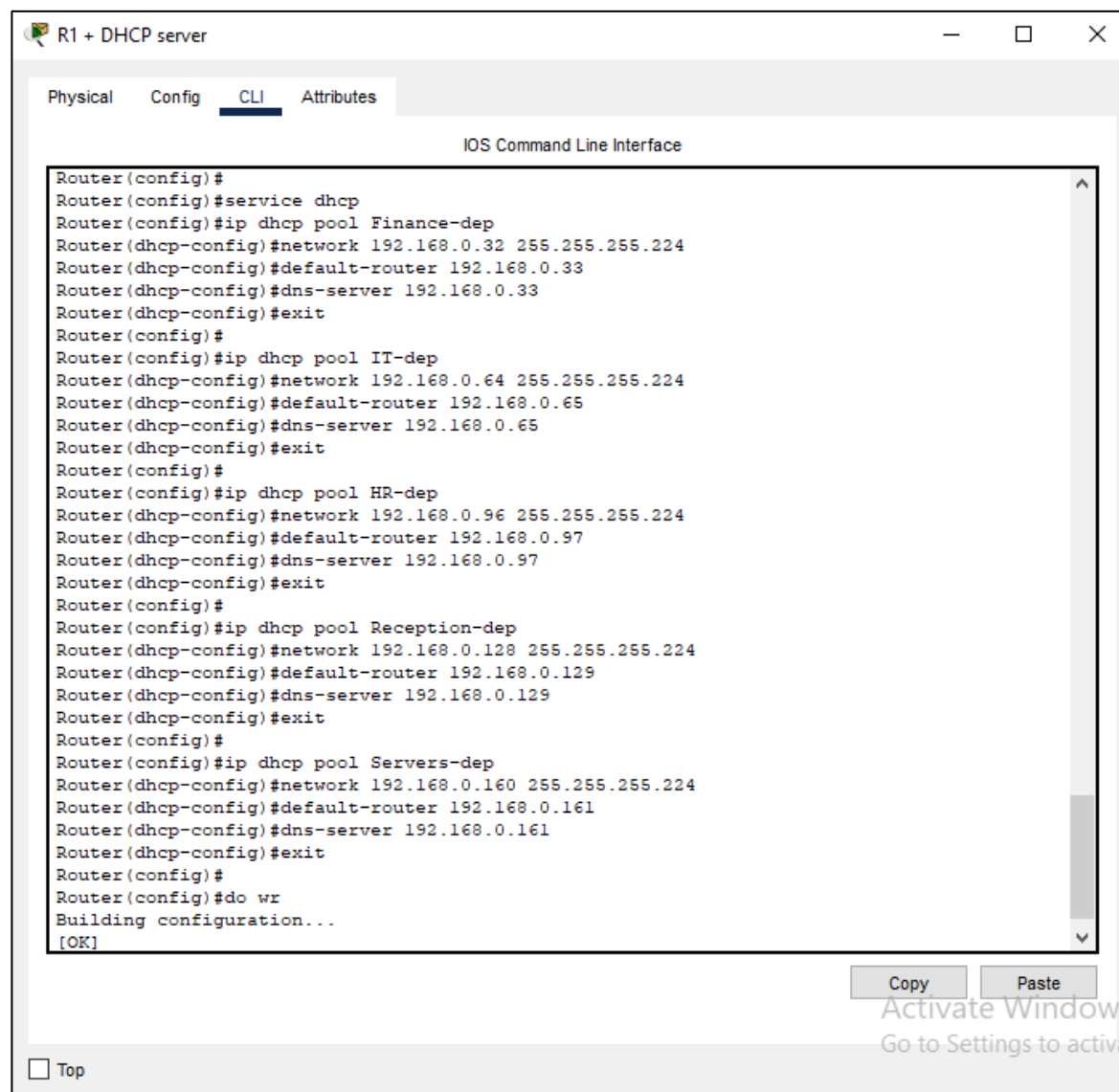
☐ Top

Figure 16: RIPv2 configuration & verification on R1

DHCP Server:

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

At (R1) we configured the DHCP server. The pools are created for each network and the commands used to configure (R1) as a DHCP server appears in the figure below:



```
Router(config)#
Router(config)#service dhcp
Router(config)#ip dhcp pool Finance-dep
Router(dhcp-config)#network 192.168.0.32 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.33
Router(dhcp-config)#dns-server 192.168.0.33
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool IT-dep
Router(dhcp-config)#network 192.168.0.64 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.65
Router(dhcp-config)#dns-server 192.168.0.65
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool HR-dep
Router(dhcp-config)#network 192.168.0.96 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.97
Router(dhcp-config)#dns-server 192.168.0.97
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool Reception-dep
Router(dhcp-config)#network 192.168.0.128 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.129
Router(dhcp-config)#dns-server 192.168.0.129
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp pool Servers-dep
Router(dhcp-config)#network 192.168.0.160 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.161
Router(dhcp-config)#dns-server 192.168.0.161
Router(dhcp-config)#exit
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
```

Figure 17: DHCP configuration on R1

This figure will show that the DHCP server configuration is properly done **show startup configuration** command used:

```
Router(config)#  
Router(config)#do show start  
Using 1245 bytes  
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Router  
!  
!  
!  
!  
!  
ip dhcp pool Finance-dep  
network 192.168.0.32 255.255.255.224  
default-router 192.168.0.33  
dns-server 192.168.0.33  
ip dhcp pool IT-dep  
network 192.168.0.64 255.255.255.224  
default-router 192.168.0.65  
dns-server 192.168.0.65  
ip dhcp pool HR-dep  
network 192.168.0.96 255.255.255.224  
default-router 192.168.0.97  
dns-server 192.168.0.97  
ip dhcp pool Reception-dep  
network 192.168.0.128 255.255.255.224  
default-router 192.168.0.129  
dns-server 192.168.0.129  
ip dhcp pool Servers-dep  
network 192.168.0.160 255.255.255.224  
default-router 192.168.0.161  
dns-server 192.168.0.161
```

Figure 18: DHCP verification on R1

After configuring the DHCP server on (R1) we need to do the configuration of the IP helper address on (R2). The figure below represents the command used to do the configuration:

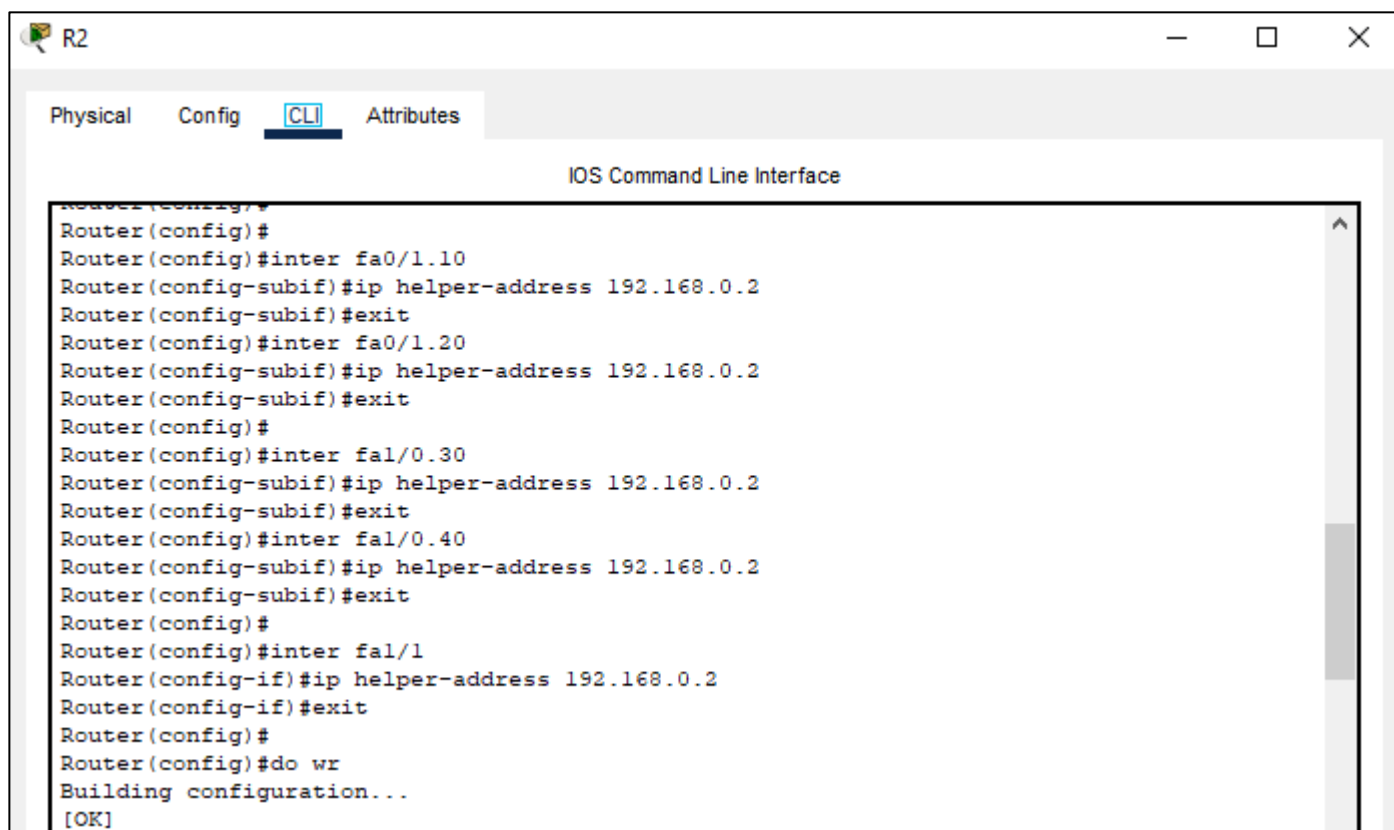


Figure 19: IP-helper configuration on R2

Finally, after finishing everything related to DHCP server configuration we must go to each host in our networks and configure hosts to DHCP as you can see in the figure:

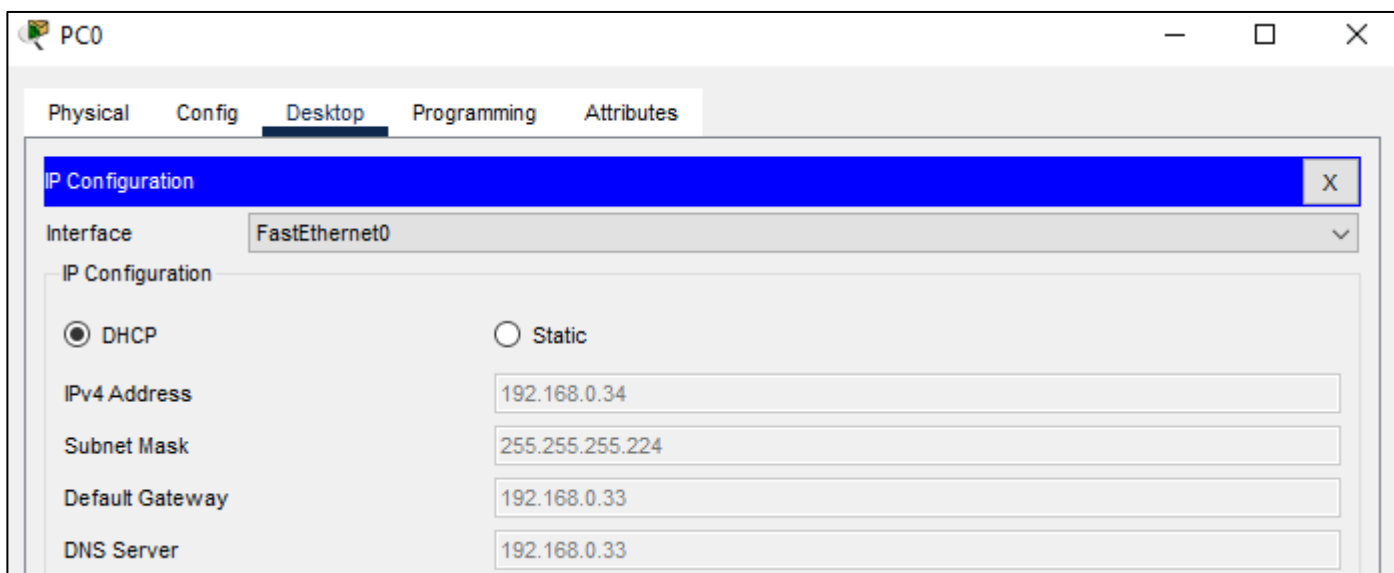


Figure 20: IP configuration on host

PC0 – Finance department

Web Server:

In simple terms, a web server is a computer that stores, processes, and delivers website files to web browsers.

Web servers consist of hardware and software that use Hypertext Transfer Protocol (HTTP) to respond to web users' requests made via the World Wide Web.

Through this process, web servers load and deliver the requested page to the user's browser – Google Chrome, for example.

Here in this figure below you can see that we configured the web server IP address statically:

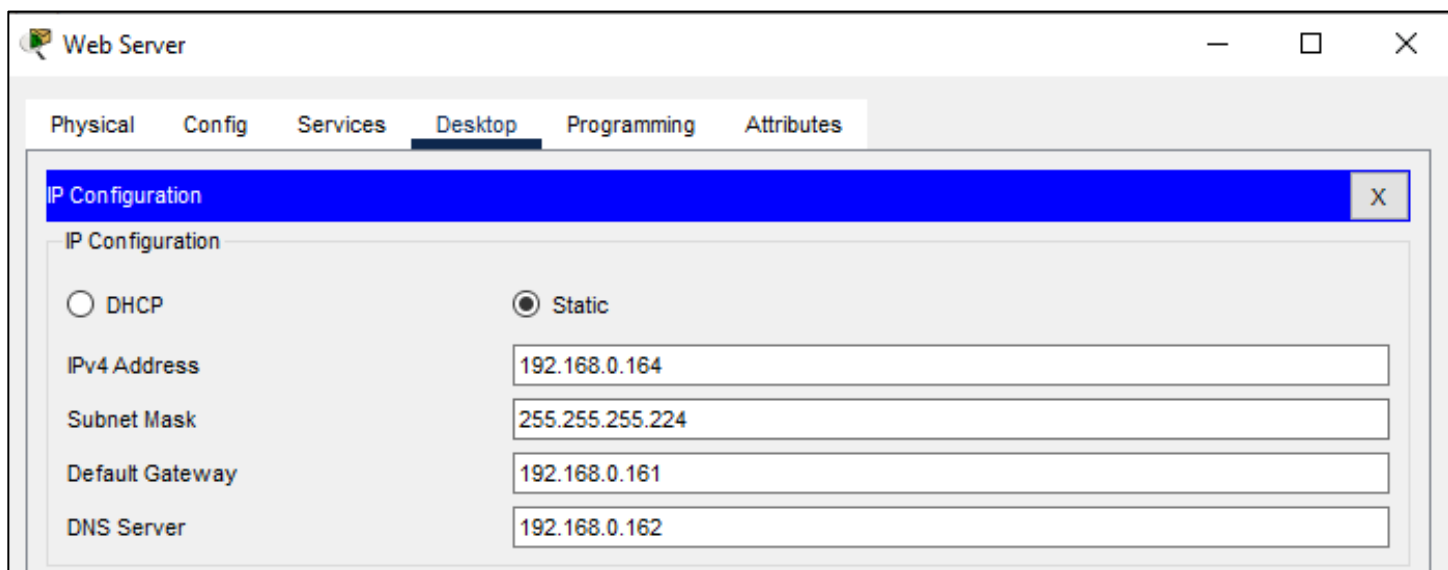


Figure 21: Configuring web server IP address statically

In this figure, you can see the website of the web server which is opened from one of the hosts in the topology using its IP:

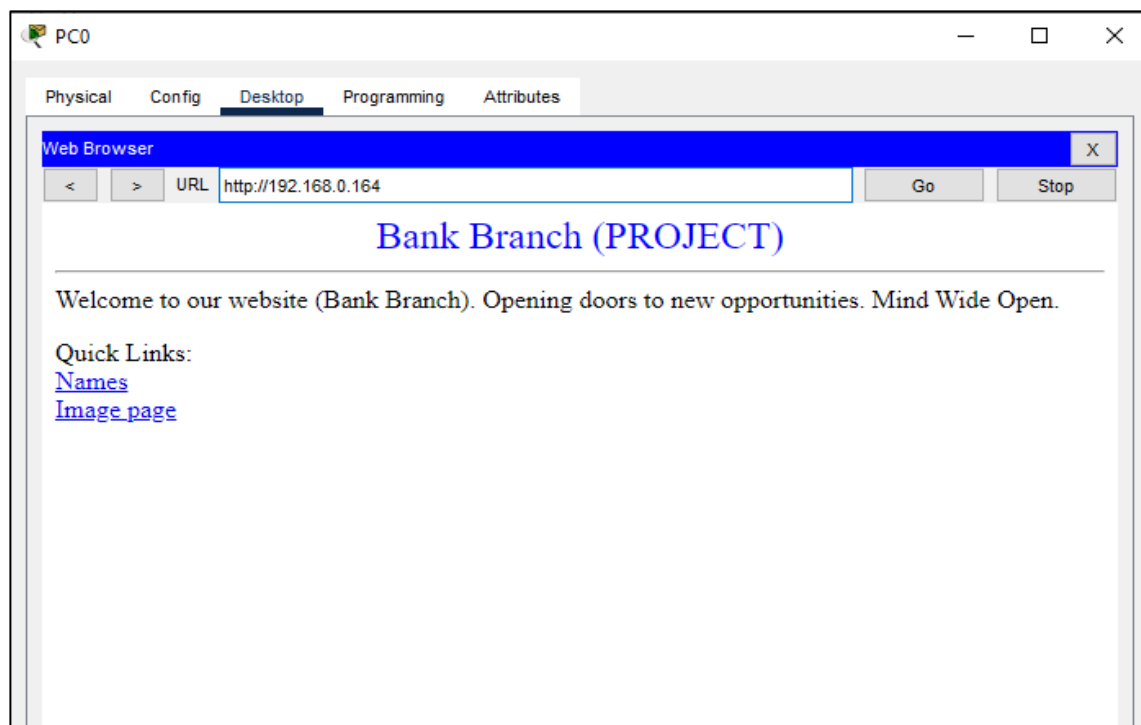


Figure 22: Web server verification using IP address

In this figure, you can see the website of the web server which is opened from one of the hosts in the topology using its domain name:

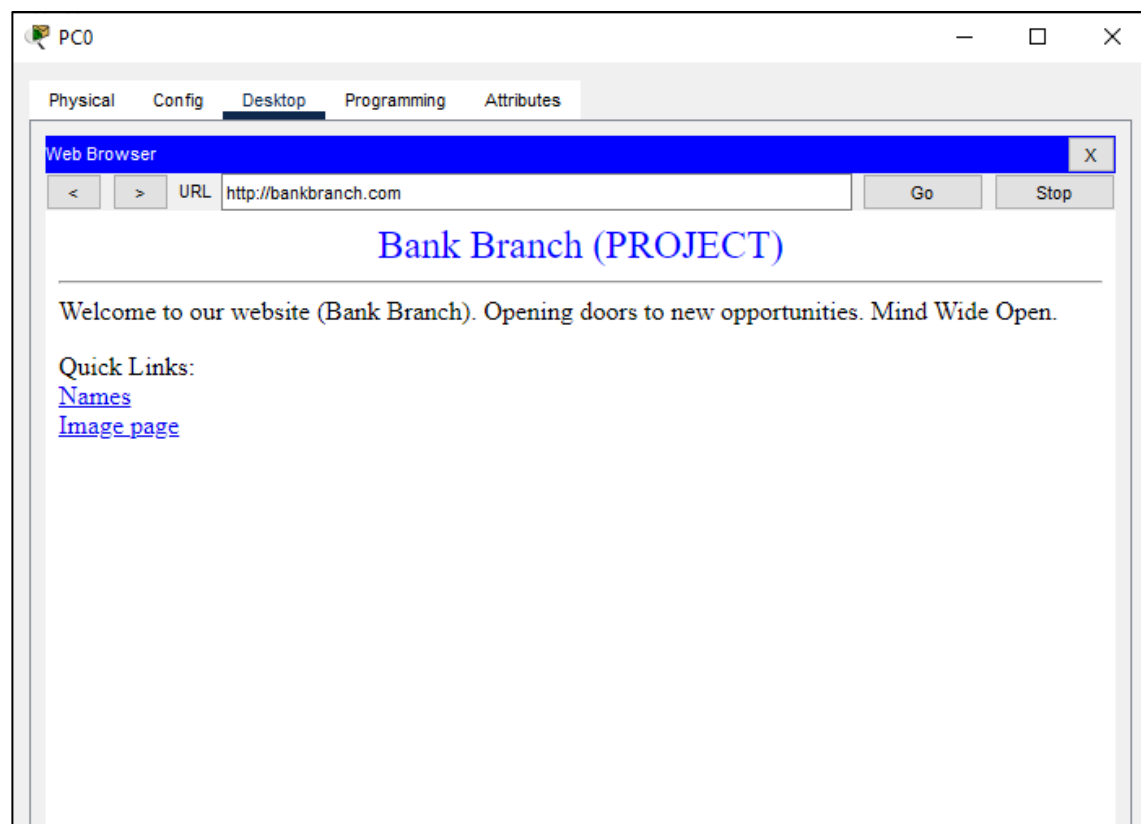


Figure 23: Web server verification using DNS

NTP Configuration:

NTP service is important to the network to synchronize the device's clocks and to make it easier to troubleshoot and solve problems that may happen.

First, the NTP service is toggled to be “on” in the server, then the appropriate date and time are set in the server as shown.

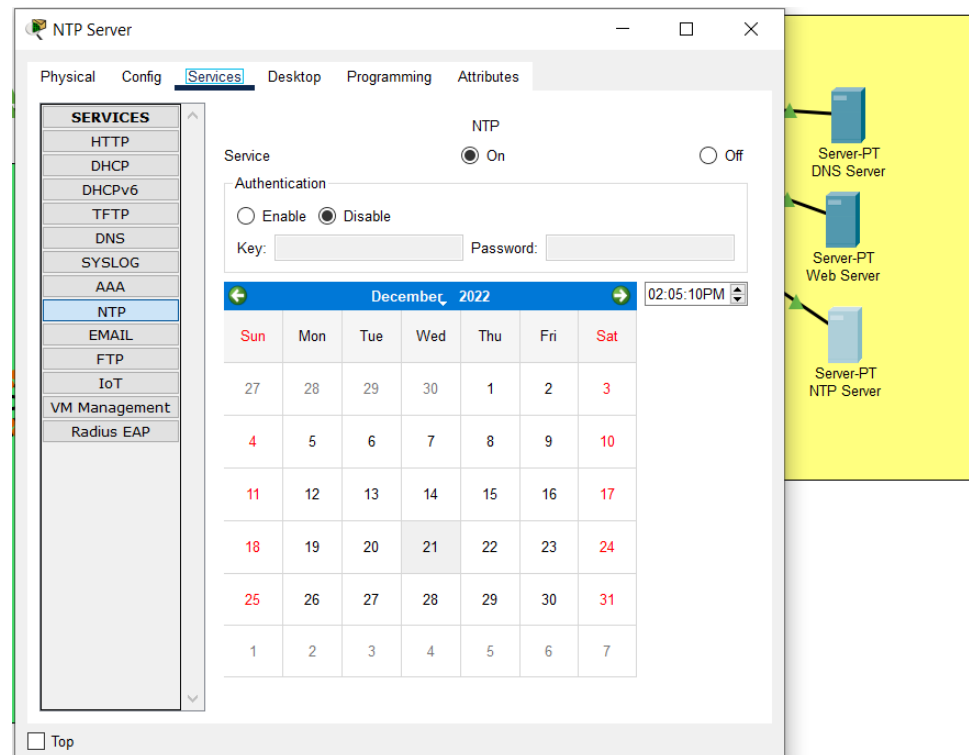


Figure 24: Enabling NTP in the NTP server.

As in the screenshot, the NTP Server is set to use DHCP, and its IP address is 192.168.0.163.

After that, Routers and switches are configured to use the NTP server in the network instead of the time of the hardware calendar. If R2 is checked for the time it uses, it shows the time in the year 1993 as it is assigned to that by the hardware calendar. “show clock” and “show clock detail” commands are used as shown.

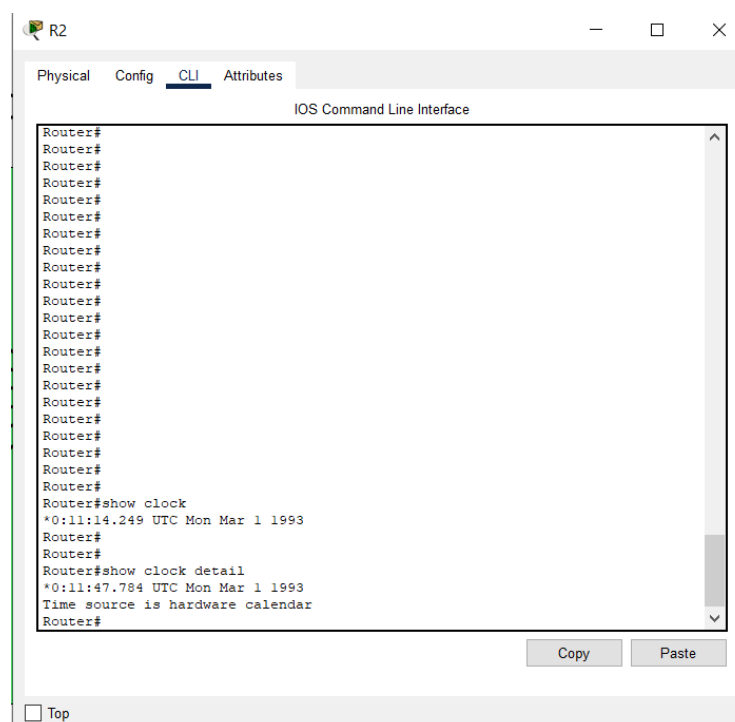
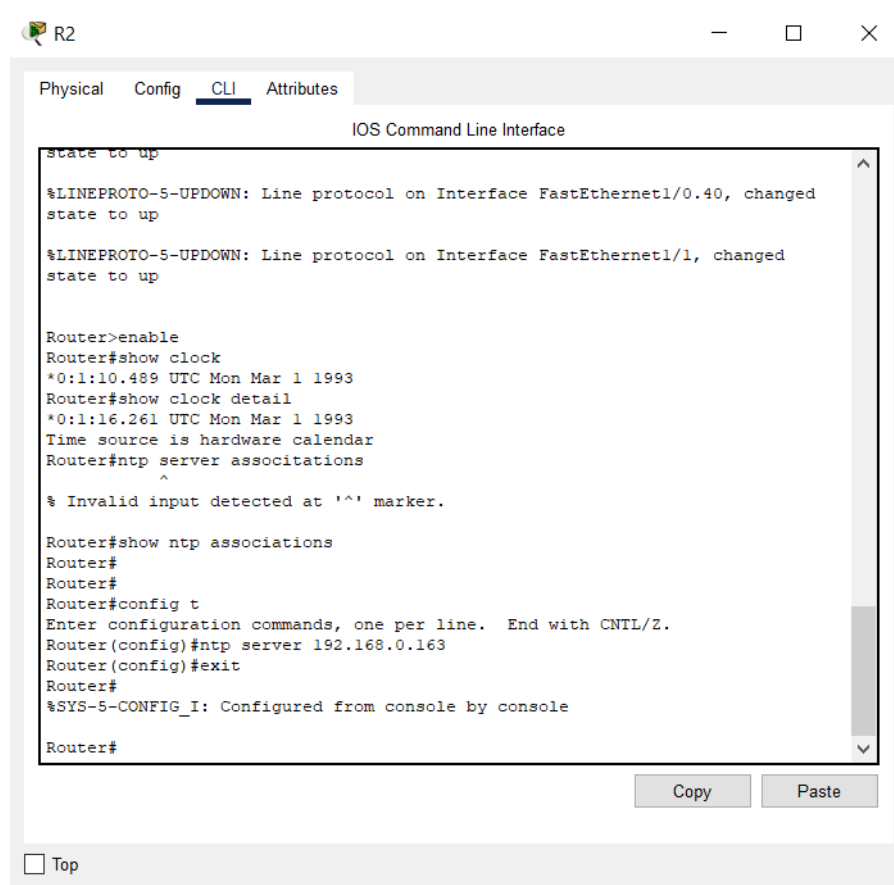


Figure 25: Clock Information in R2 Router before implementing NTP.

Then R2 and other routers and switches are configured to use the NTP Server. The command “ntp server [NTP Server IP address]” is used as shown in the following screenshots:



The screenshot shows the CLI window for Router 2. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "R2". The main area is titled "IOS Command Line Interface". The text in the window is as follows:

```
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.40, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed
state to up

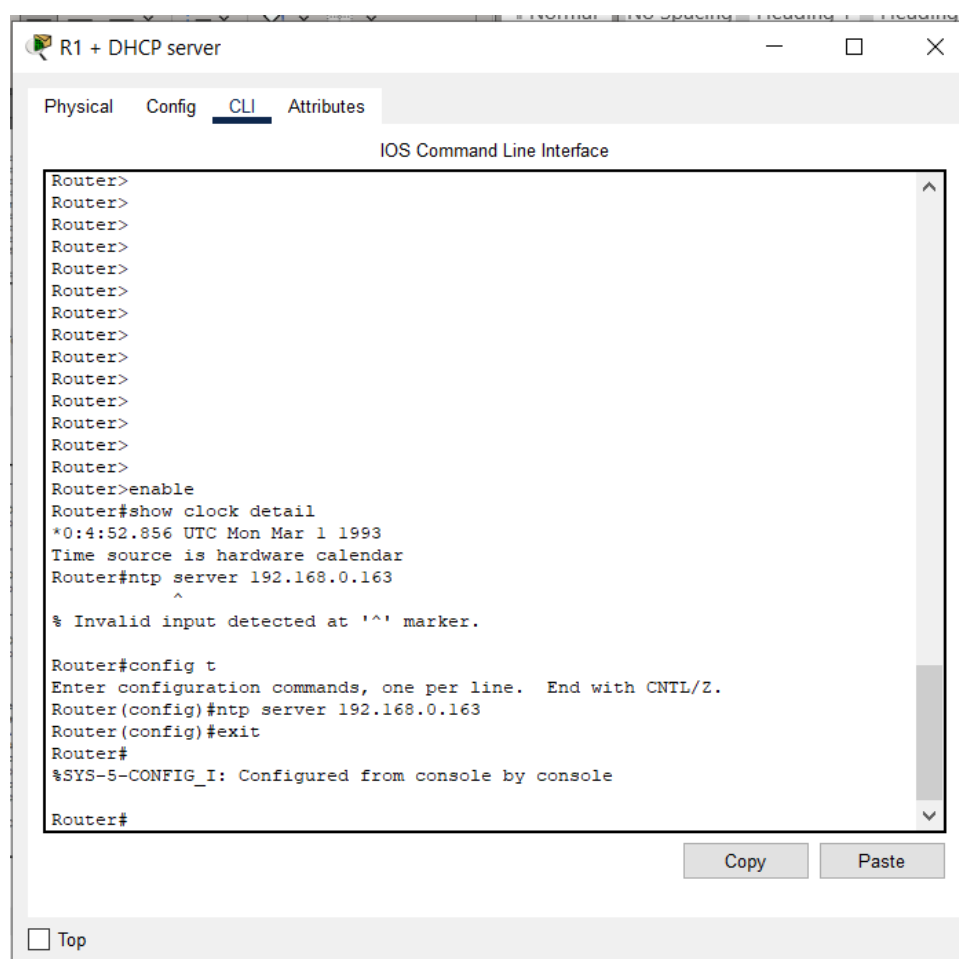
Router>enable
Router#show clock
*0:1:10.489 UTC Mon Mar 1 1993
Router#show clock detail
*0:1:16.261 UTC Mon Mar 1 1993
Time source is hardware calendar
Router#ntp server associations
^
% Invalid input detected at '^' marker.

Router#show ntp associations
Router#
Router#
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.0.163
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

At the bottom right of the window are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Figure 26: NTP Configuration on Router 2.



The screenshot shows the CLI window for Router 1. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "R1 + DHCP server". The main area is titled "IOS Command Line Interface". The text in the window is as follows:

```
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>enable
Router#show clock detail
*0:4:52.856 UTC Mon Mar 1 1993
Time source is hardware calendar
Router#ntp server 192.168.0.163
^
% Invalid input detected at '^' marker.

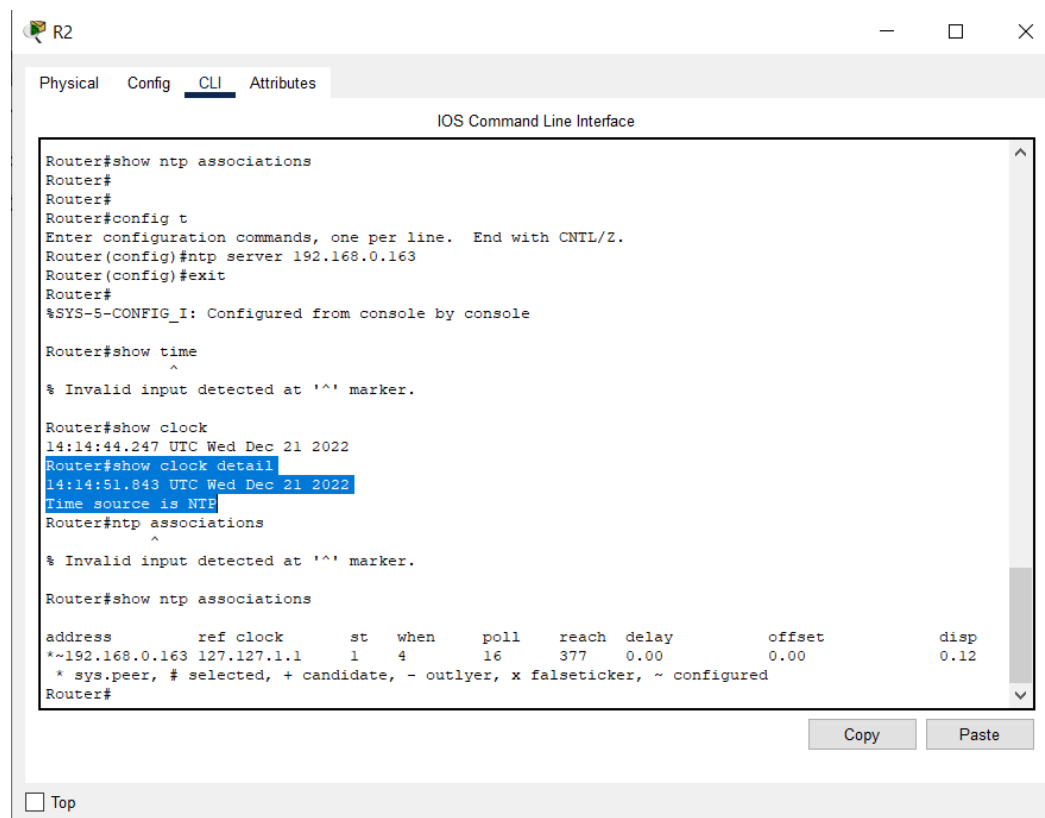
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.0.163
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

At the bottom right of the window are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Figure 27: NTP Configuration on Router 1.

After that, the verification is implemented in the routers using “show clock”, “show clock detail”, and “show ntp associations” commands. The commands are run on R2 as an example:



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Router#show ntp associations
Router#
Router#
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.0.163
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show time
^
% Invalid input detected at '^' marker.

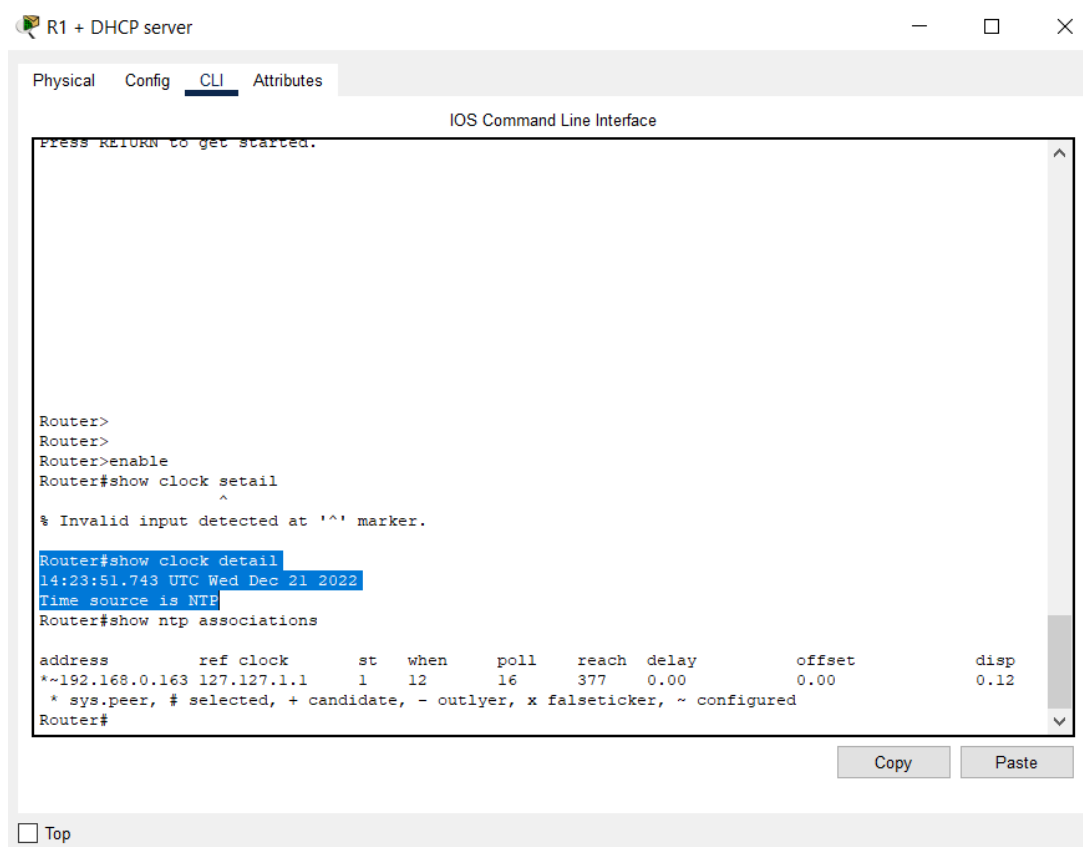
Router#show clock
14:14:44.247 UTC Wed Dec 21 2022
Router#show clock detail
14:14:51.843 UTC Wed Dec 21 2022
Time source is NTP
Router#ntp associations
^
% Invalid input detected at '^' marker.

Router#show ntp associations

address      ref clock      st  when    poll  reach  delay    offset    disp
*~192.168.0.163 127.127.1.1    1   4       16    377    0.00     0.00     0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
Copy Paste
Top

```

Figure 28: Verifying NTP Implementation on R2.



```

R1 + DHCP server
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

Router>
Router>
Router>enable
Router#show clock detail
^
% Invalid input detected at '^' marker.

Router#show clock detail
14:23:51.743 UTC Wed Dec 21 2022
Time source is NTP
Router#show ntp associations

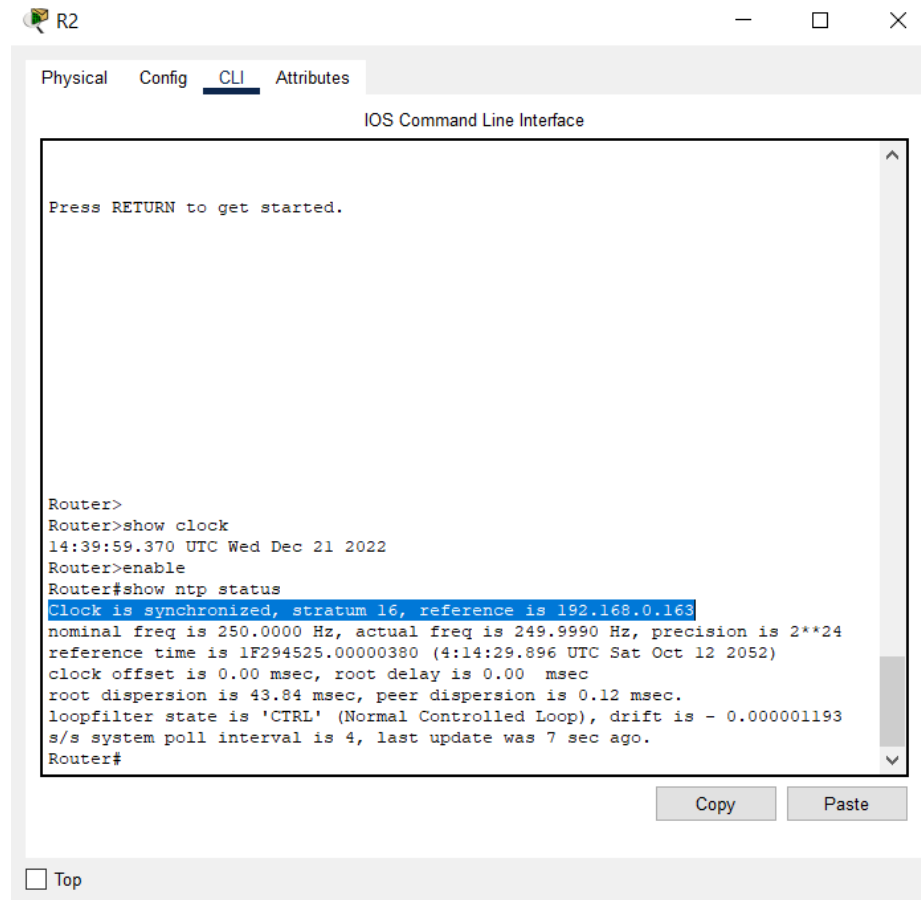
address      ref clock      st  when    poll  reach  delay    offset    disp
*~192.168.0.163 127.127.1.1    1   12      16    377    0.00     0.00     0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
Copy Paste
Top

```

Figure 29: Verifying NTP Implementation on R1.

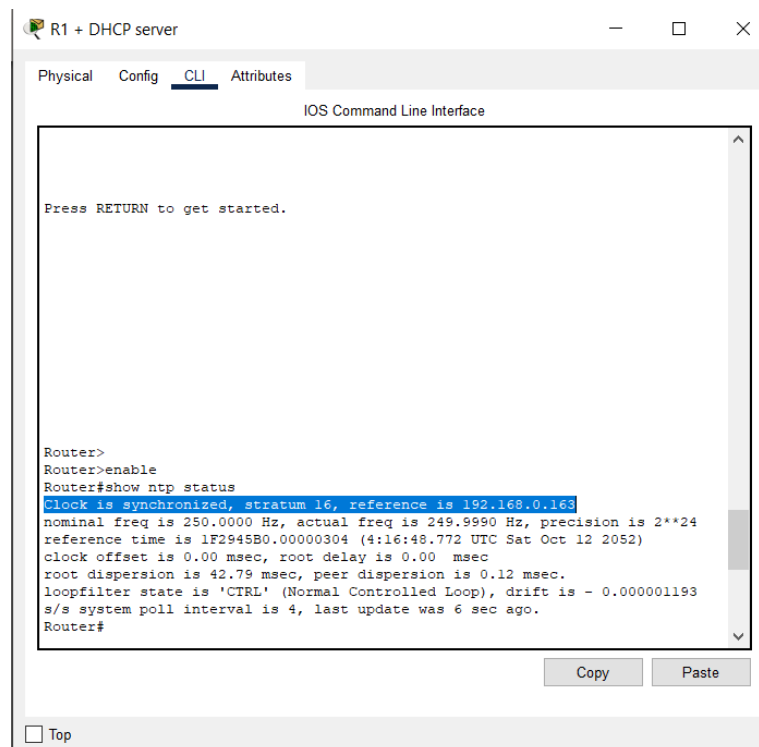
As in the screenshots, the output is showing the time as the actual time that writers were in when they configured the device. Moreover, the output specifies that the “Time source is NTP”.

Moreover, we can verify the NTP service using “show ntp status” command to verify the ntp service is running correctly.

A screenshot of a network device's CLI interface for R2. The window has tabs for Physical, Config, CLI (selected), and Attributes. The CLI window shows the command sequence: Router> show clock (output: 14:39:59.370 UTC Wed Dec 21 2022), Router> enable, and Router# show ntp status. The output of the last command is highlighted in blue. At the bottom of the CLI window are 'Copy' and 'Paste' buttons, and a 'Top' button is at the bottom left of the main window.

```
Router>
Router>show clock
14:39:59.370 UTC Wed Dec 21 2022
Router>enable
Router#show ntp status
Clock is synchronized, stratum 16, reference is 192.168.0.163
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 1F294525.00000380 (4:14:29.896 UTC Sat Oct 12 2052)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 43.84 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193
s/s system poll interval is 4, last update was 7 sec ago.
Router#
```

Figure 30: “show ntp status” command on R2.

A screenshot of a network device's CLI interface for R1 + DHCP server. The window has tabs for Physical, Config, CLI (selected), and Attributes. The CLI window shows the command sequence: Router> enable, Router# show ntp status. The output of the last command is highlighted in blue. At the bottom of the CLI window are 'Copy' and 'Paste' buttons, and a 'Top' button is at the bottom left of the main window.

```
Router>
Router>enable
Router#show ntp status
Clock is synchronized, stratum 16, reference is 192.168.0.163
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 1F2945B0.00000304 (4:16:48.772 UTC Sat Oct 12 2052)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 42.79 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193
s/s system poll interval is 4, last update was 6 sec ago.
Router#
```

Figure 31: show ntp status command on R2.

As seen, the clock is synchronized and the NTP server is running correctly across the network.

Syslog Configuration:

Syslog is a network service that is configured to collect log messages with date and timestamps from the devices across the network. These data and logs are used later in case any troubleshooting is needed to understand the cause of an incident in a network. Therefore, Syslog is an essential tool and service for every network administrator inside any enterprise.

NTP and Syslog are closely related. As mentioned before, Syslog does label the logs with timestamps; therefore, all the device clocks in the network must be synchronized together to give the accurate time of logs and incidents.

The Syslog service is configured in the start-up bank network to help network administrators access the routers and switches in order to troubleshoot them or do any remote configuration in case it is needed.

First, we inspect the IP address of the Syslog server and insure connectivity through a ping from a device from the network.

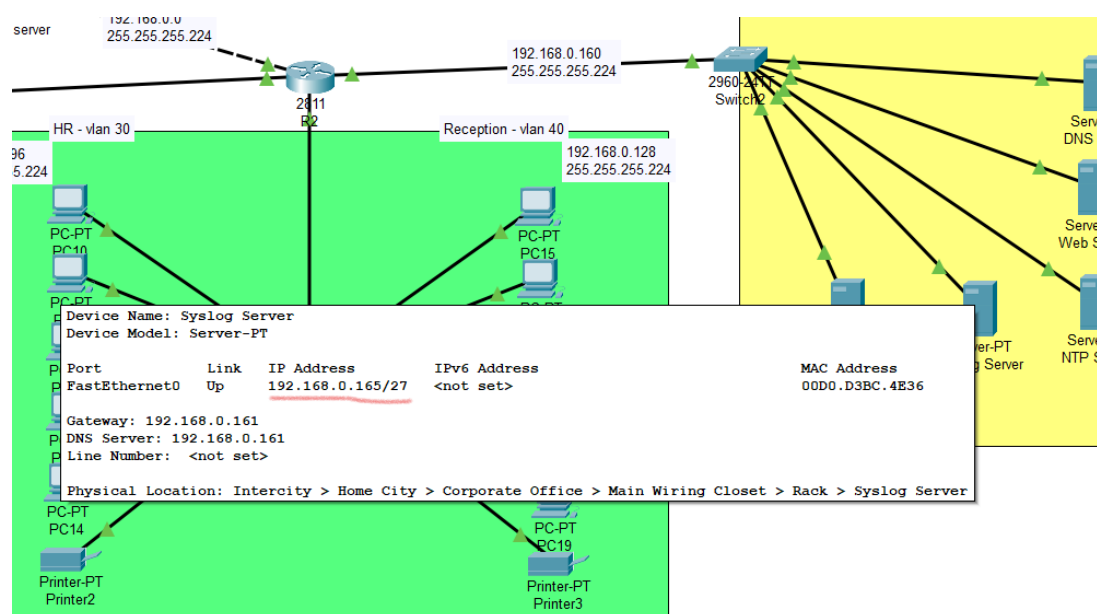


Figure 32: IP Information of Syslog Server.

Then we ping the IP 193.168.0.165 as below; to verify the connectivity.

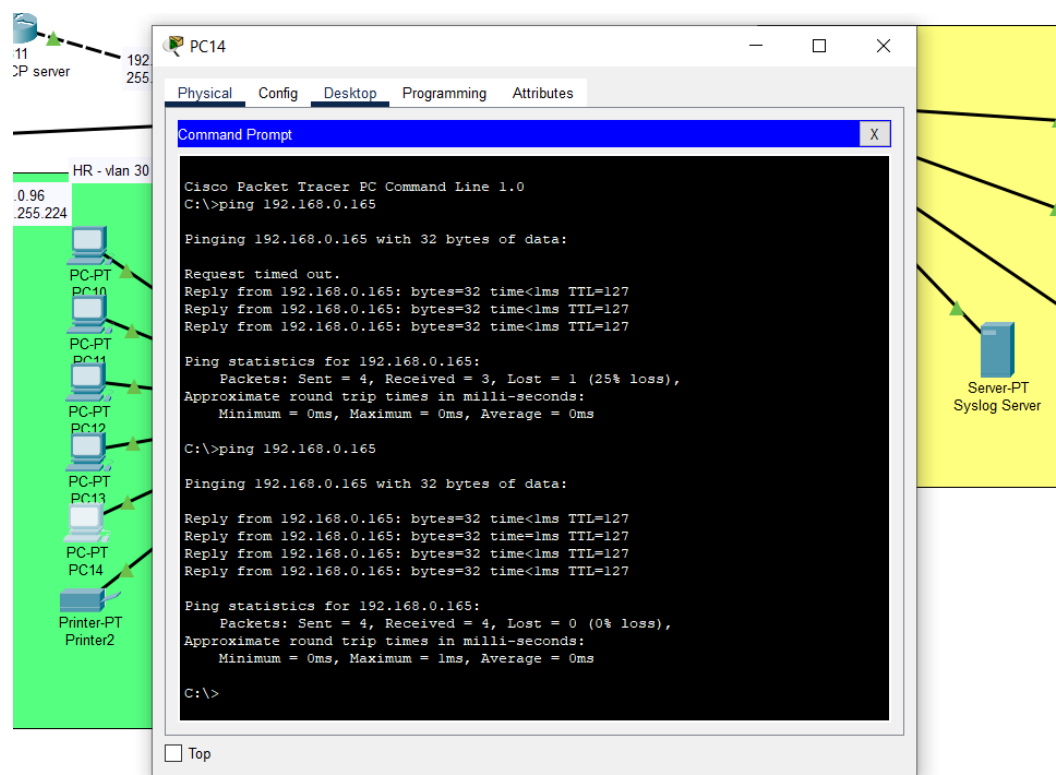


Figure 33: Pinging the Syslog Server.

As the image shows, the ping is successful to the syslog server.

Now the syslog service should be enabled in the syslog server.

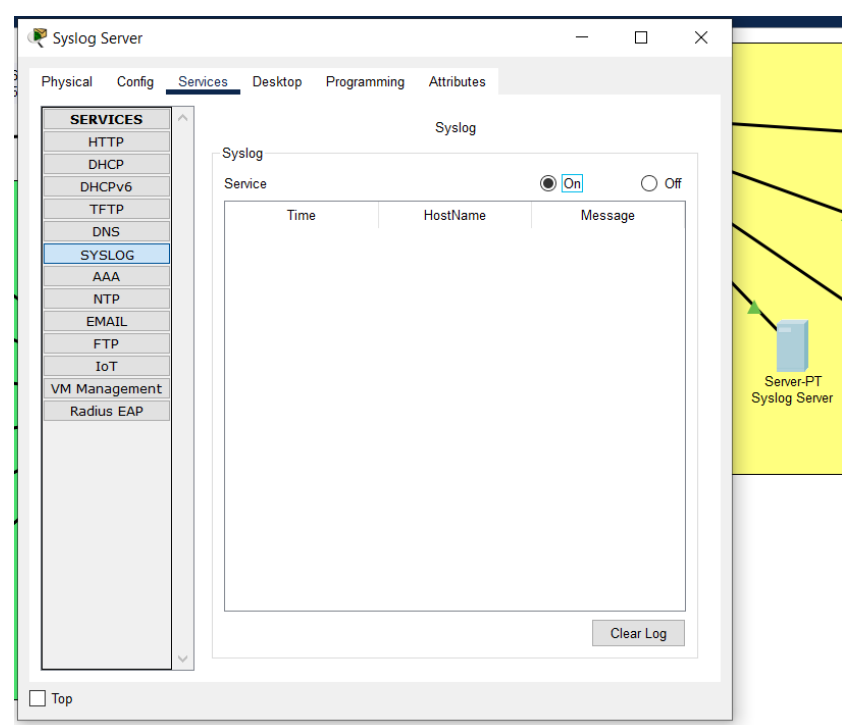


Figure 34: enabling syslog service on the server.

Moreover, the routers should be configured to pass all the logging information to the syslog server. First, we enter the privilege and configuration mode. Then we set the timestamp to be in milliseconds, and we use the command “logging host [IP Address]” – in our case, the IP is 192.168.0.165 which is the IP of the syslog server – to specify the syslog server that R2 will use to forward all the logs to.

These commands are entered to R2. The same commands are applied to R1 so it can forward any event to the syslog server.

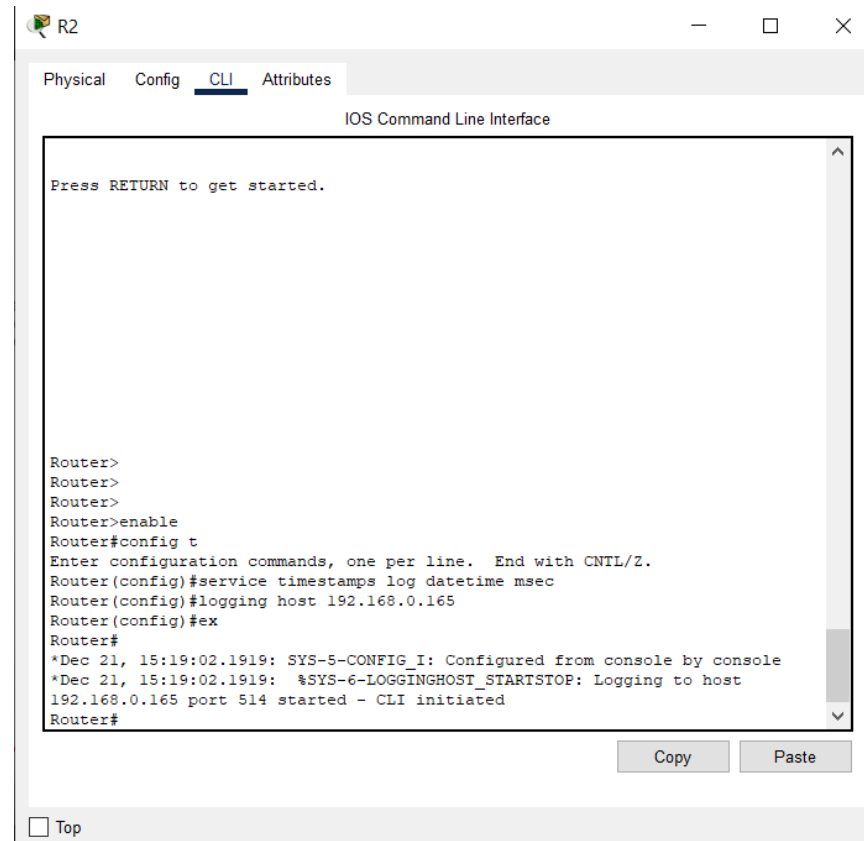


Figure 35: Syslog configuration in R2.

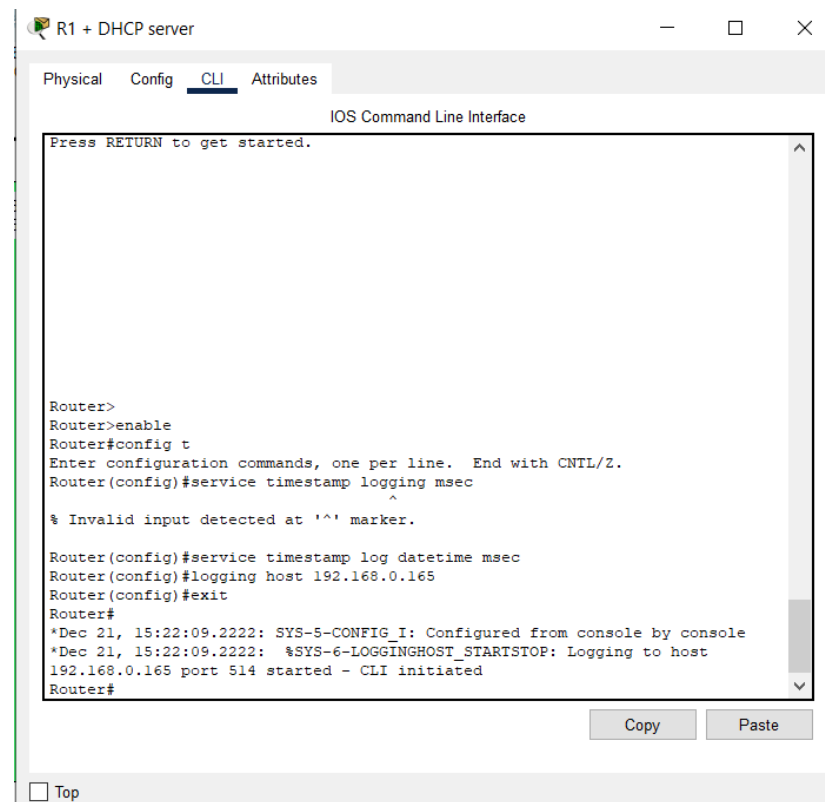


Figure 36: Syslog configuration in R1.

After that, we check the syslog server and we found that it collected 4 log messages (2 from each server). Moreover, the reader can notice and verify that the timestamp date and time as the syslog is dependent on the NTP service which we implemented in the network earlier. Even if the admin changed the configuration of an interface in the network this change will be reported to syslog service with its date and time.

The image shows two side-by-side windows. The left window is titled 'R2' and shows the 'IOS Command Line Interface' (CLI) with the following commands and output:

```

Router>
Router>
Router>
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#service timestamps log datetime msec
Router(config)#logging host 192.168.0.165
Router(config)#ex
Router#
*Dec 21, 15:19:02.1919: SYS-5-CONFIG_I: Configured from console by console
*Dec 21, 15:19:02.1919: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.0.165 port 514 started - CLI initiated
Router#interface fa 0/0
^
% Invalid input detected at '^' marker.
Router#interface fa0/0
^
% Invalid input detected at '^' marker.
Router#config t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#interface fa 0/0
Router(config-if)#exit
Router(config)#exit
Router#
*Dec 21, 15:27:26.2727: SYS-5-CONFIG_I: Configured from console by console
Router#
  
```

The right window is titled 'Syslog Server' and shows the 'Services' tab with 'SYSLOG' selected. The 'Syslog' service is set to 'On'. Below the service list is a table of log messages:

Service	Time	HostName	Message
1	12 21 2022 03:27:26.984 PM	192.168.0.161	%SYS-5-CONFIG_I: Configured from ...
2	12 21 2022 03:19:02.082 PM	192.168.0.161	%SYS-5-CONFIG_I: Configured from ...
3	12 21 2022 03:19:02.082 PM	192.168.0.161	: %SYS-6-LOGGINGHOST_ST...
4	12 21 2022 03:22:09.004 PM	192.168.0.2	%SYS-5-CONFIG_I: Configured from ...
5	12 21 2022 03:22:09.004 PM	192.168.0.2	: %SYS-6-LOGGINGHOST_ST...

At the bottom of the Syslog Server window, there is a 'Clear Log' button.

Figure 37: Testing the syslog service across the network.

SSH Configuration:

SSH is an acronym for “Secure Shell”. It is a communication protocol that uses encryption to provide secure communication between two parties. It is important because it prevents attackers from sniffing the communication to steal any credentials or sensitive data. Hence, it is important for any organization to implement and use SSH in its day-to-day tasks.

SSH is configured to help network admins troubleshoot problems in devices remotely. It works well in distant environments and where admins do have not to be closer to the equipment.

In general, and because this project is for self-learning and training purposes, the username and password used across all the devices are going to be “admin”. Of course, this is going to be changed into a stronger password and unique password for each device in real-world scenarios; in order to prevent brute-force attacks.

So, for each device, a hostname and a password are set, then the running configuration is going to be shown using the “show running-config” command, and saved using “copy running-config startup-config”.

For R2, we can see that the SSH service is disabled using the “show ip ssh” command.

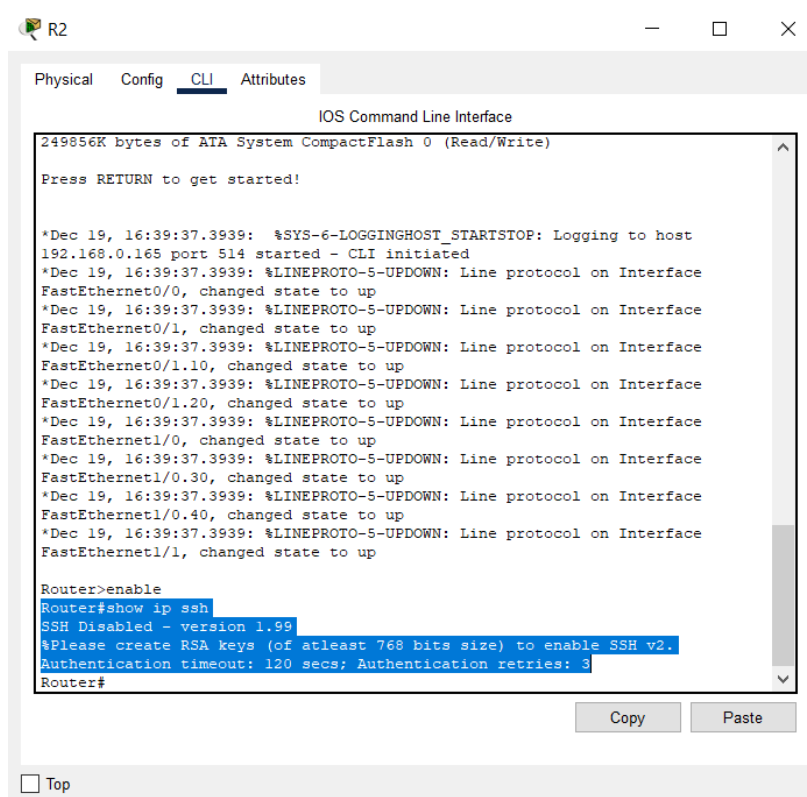


Figure 38: showing the status of SSH in R2.

Then, the name of the router is changed using “hostname [new name]”, and a domain name is created, as well as the encryption keys.

Encryption keys are generated using the RSA algorithm, and the key length is 2048 bits, which is the industrial standard. All that is done using the command: “crypto key generate rsa general-keys modulus 2048”.

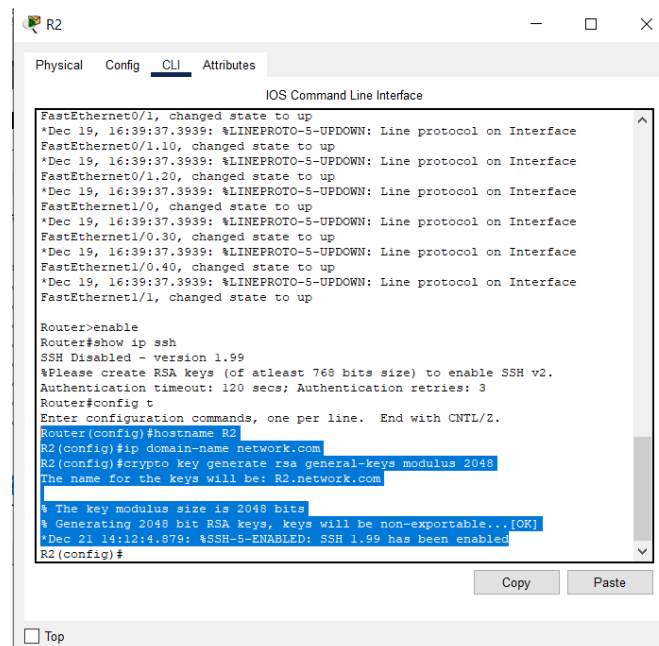


Figure 39: Changing the hostname in Router 2 and generating encryption keys.

Then we create the username and password and configure the SSH connection to R2 using the commands in the screenshot below. The configuration is using the “ssh” keyword (to distinguish it from other protocols such as telnet). Moreover, the login is configured to be locally, and the communication line is configured so that it is giving the user the privilege mode once they log in. After that, they can escalate to configuration mode using the “config t” command.

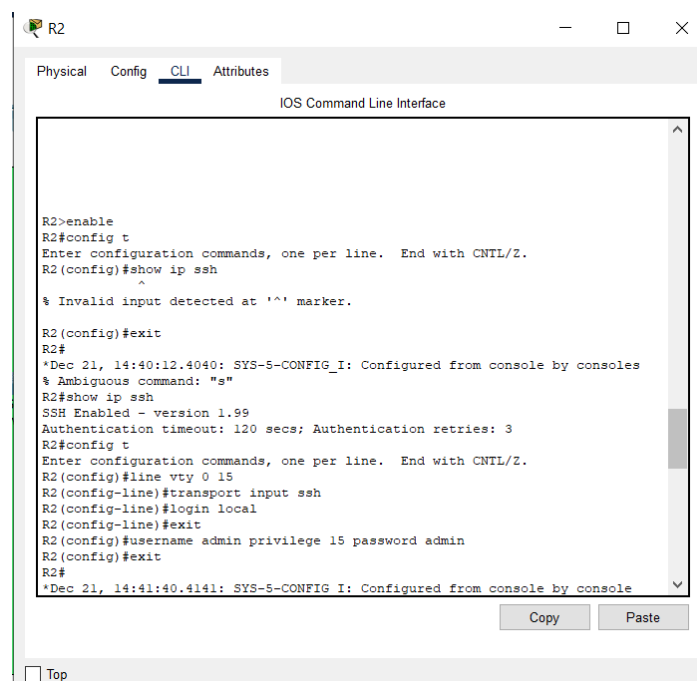


Figure 40: configuring and creating ssh user account and password.

After that, we verify the done configuration by logging from a computer (PC5) in the network using the username “admin” and password “admin” to one of the routers in the network. And as seen, the login was successful and configuration operations can be done remotely to the router using SSH.

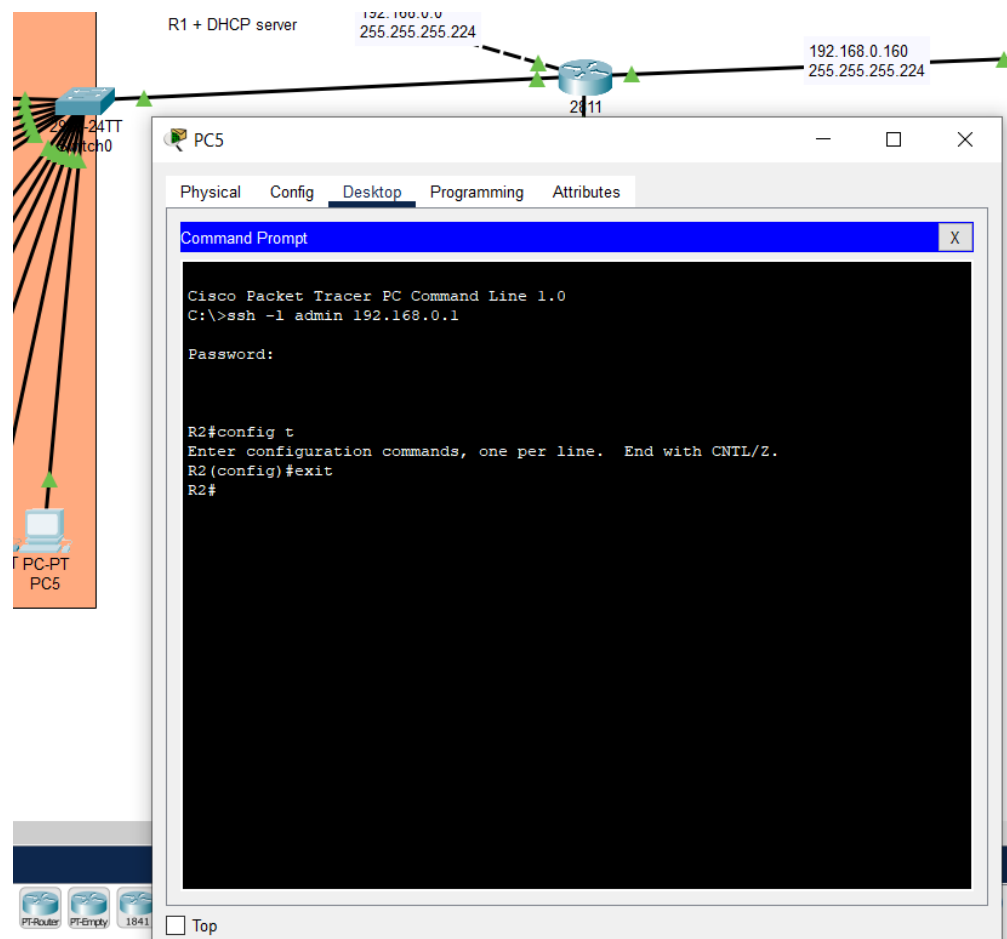


Figure 41: Successful SSH login from a device to the R2.

After that, the same steps are applied to R1 and all three switches in the network. And Network Administrators or other IT employees can access the routers and switches using SSH.

DNS Server

The DNS server is implemented to help facilitate communication between humans and computers, because computers communicate using IP addresses, while humans are more familiar with naming objects, so the DNS server allows the network to assign names to a given IP address for easier access from users.



Figure 43: DNS server connected to switch in topology

The DNS server is connected to Switch2 which controls all the servers in the network. This subnet of the network is using static IP instead of DHCP.

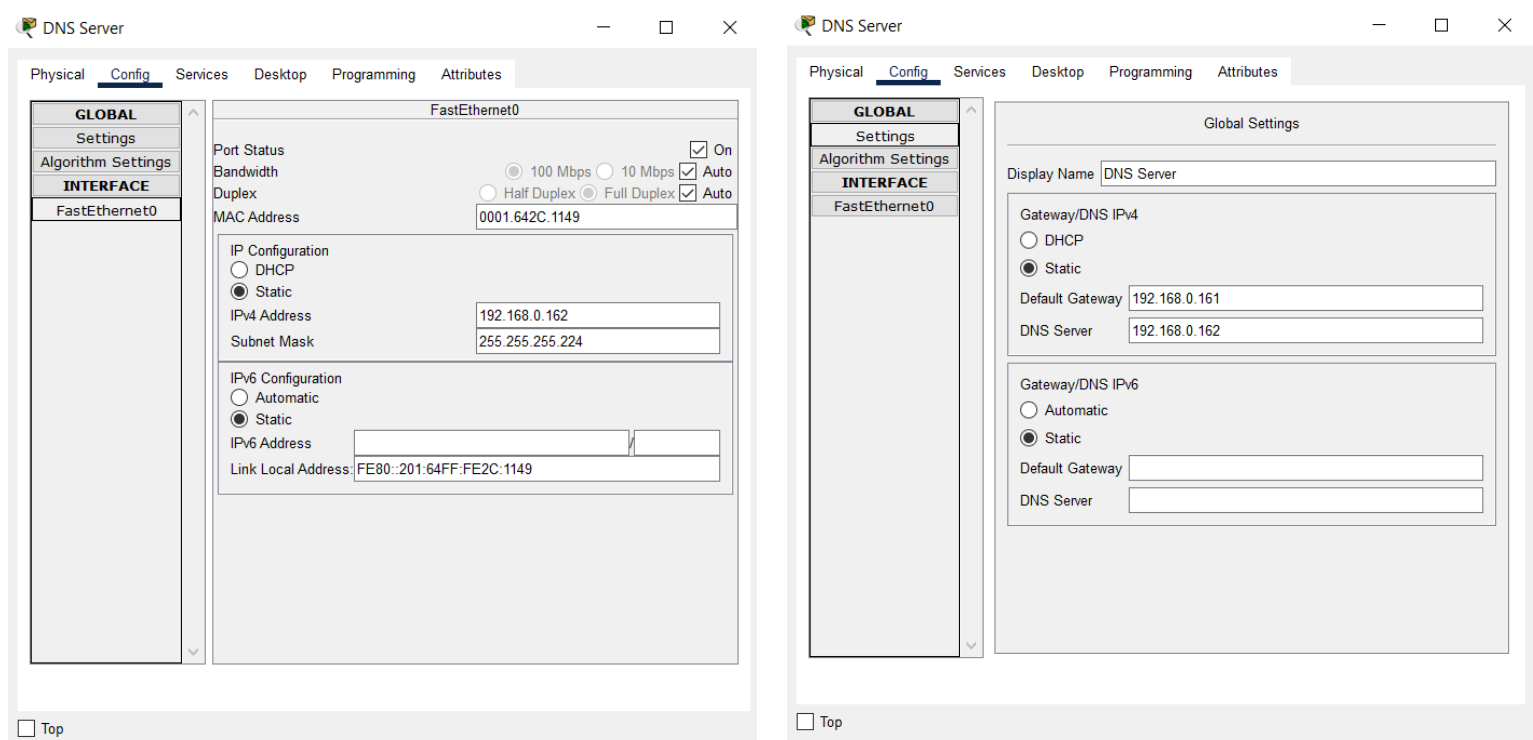


Figure 44: DNS server IP and settings configuration

The IP configuration for the DNS server is set as static, with the IP address 192.168.0.162/27. The server settings are configured with the default gateway 192.168.0.161, and DNS server 192.168.0.162. This DNS server IP is set in all static devices in the network, and for the devices connected by DHCP, it was added as shown in the figure below.

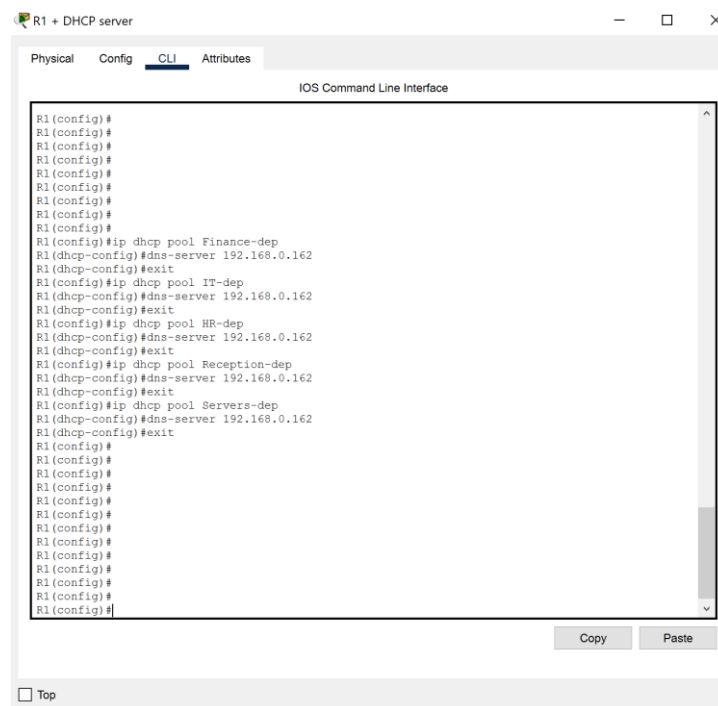


Figure 45: Adding the DNS server IP to DHCP pools

In R1 the DHCP server formerly created can add DNS server IP automatically to the devices. After entering the selected DHCP pool configuration the command (DNS-server {IP}) allocated the selected IP to all devices in the network, and in this case the IP is 192.168.0.162.

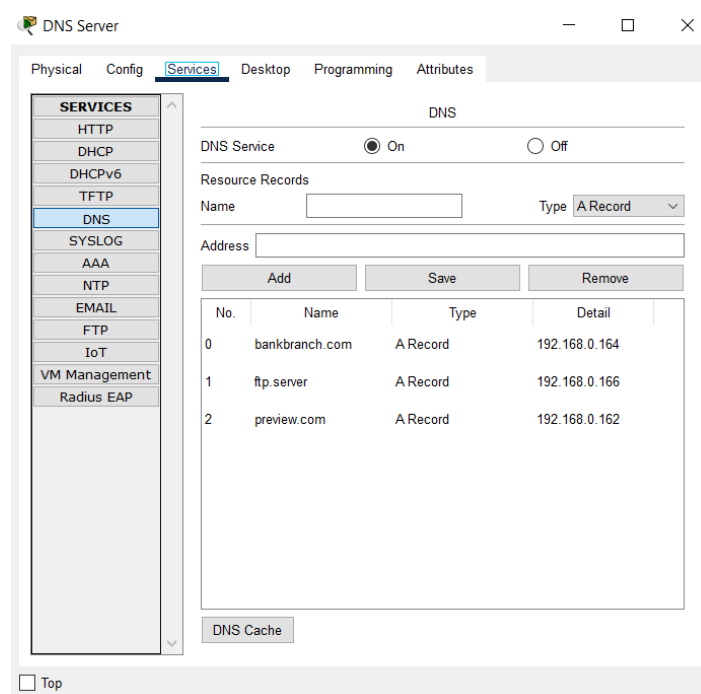


Figure 46: DNS service menu

After connecting the DNS IP to the network, the DNS service is turned on and configured according to the needs of the network users. For example, having a domain name for the FTP server allows user to log in to the server using the domain name instead of an IP address.

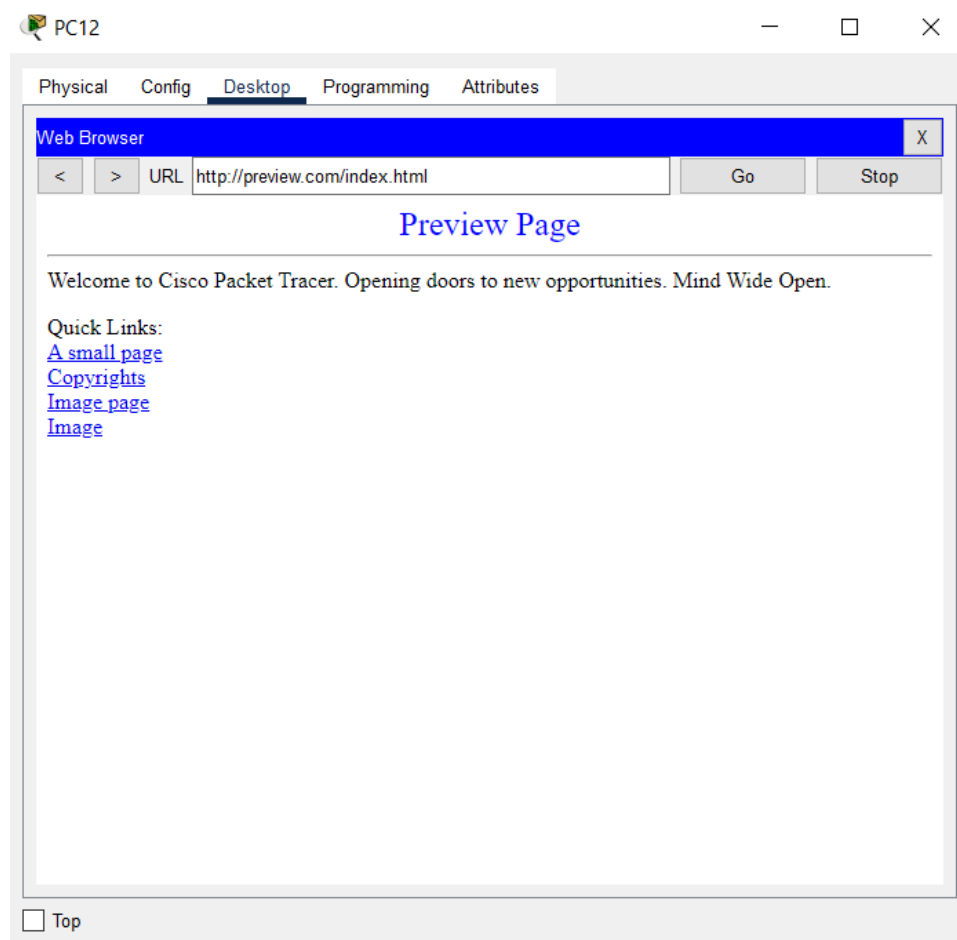


Figure 47: Accessing a website using a domain name

The figure above is a preview of the IP address 192.168.0.162 connected by the domain name preview.com. This shows the successful connection between PC12 which is in HR VLAN 192.168.0.96 connected using DHCP and the servers VLAN 192.168.0.160. The successful preview of a file in another server using a domain name proves the connection of the DNS server in the network.

FTP Server:

FTP is a service that provides users with the ability to send and receive files from a server that stores and controls all the data. This is an important service as many businesses have several people operate on documents, so a method sharing these documents is important.

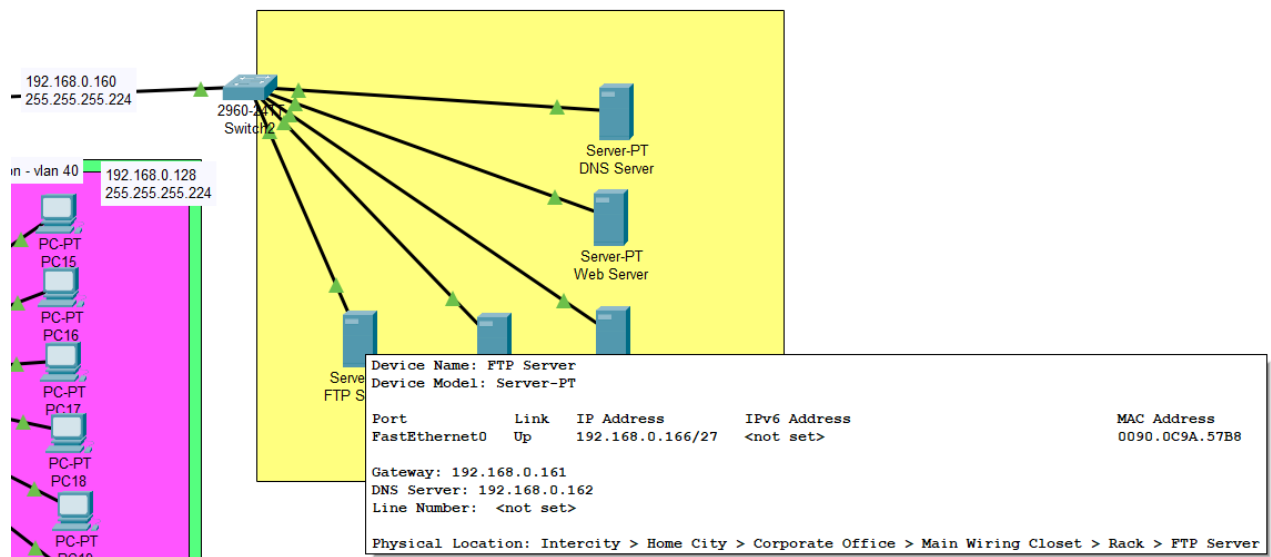


Figure 48: FTP server and IP in the topology

The FTP server is connected to Switch2 which controls all the servers in the network.

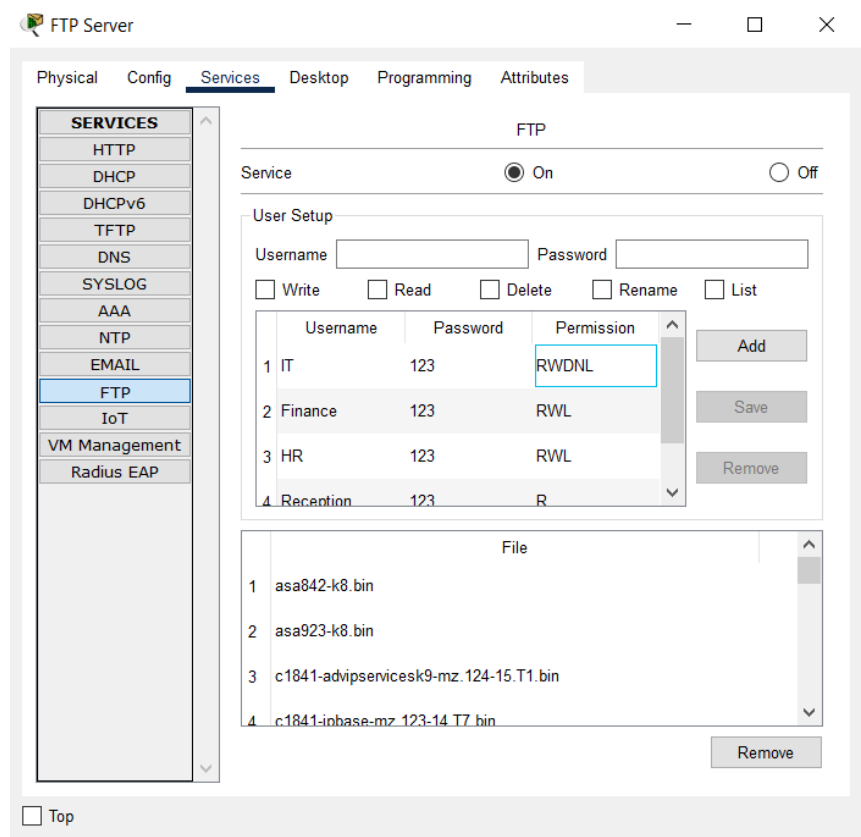


Figure 49: FTP service menu

The FTP server is configured from the FTP service tab, after enabling it gives the ability to add users and give them server permissions. In this network the user classification is split for each VLAN, IT with administration permissions with all functionalities. Finance and HR can upload and download files. Reception users are only given permission to read files from the server.

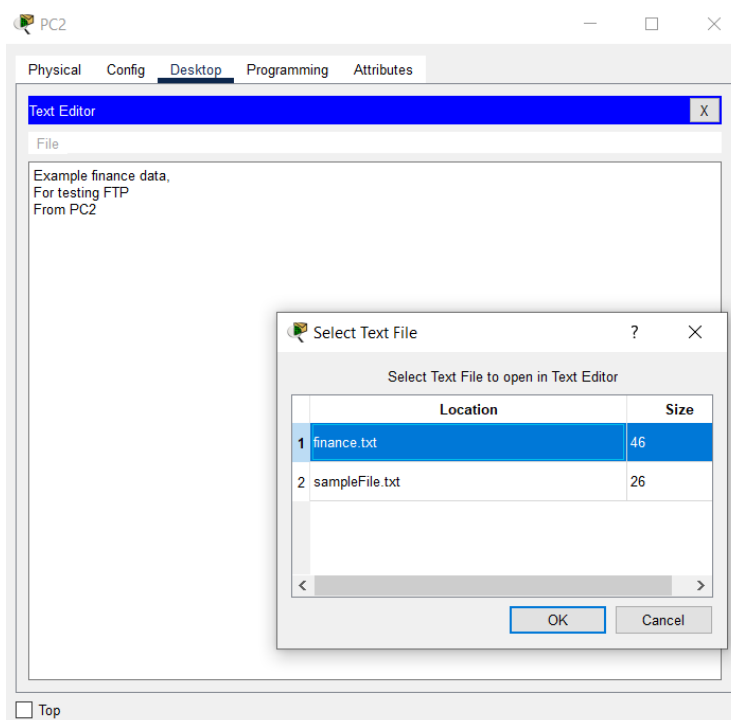


Figure 50: Creating the text file finance.txt in PC2

To test the FTP server, a text file with the name finance.txt is saved on device PC2. This will be the sample file to test the FTP service in the network.

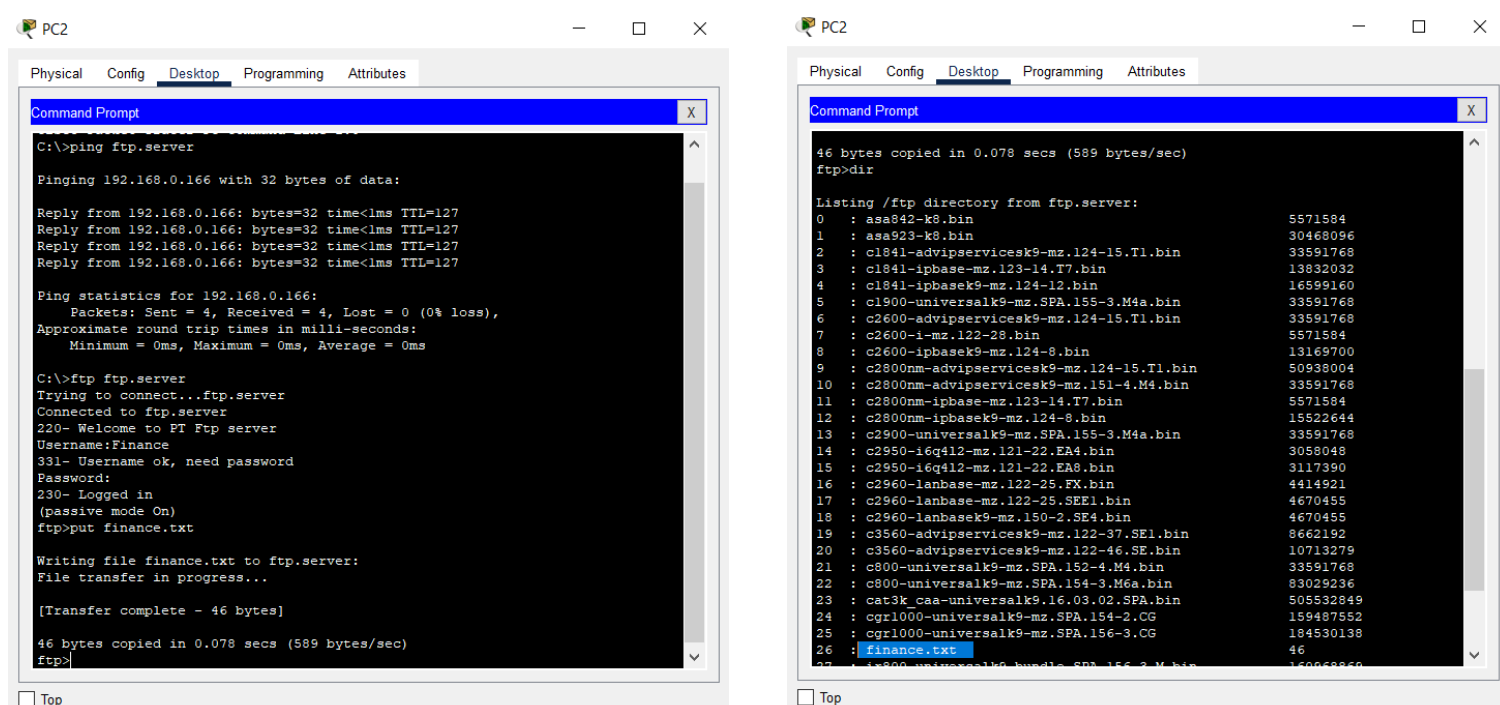


Figure 51: Sending text file finance.txt to FTP server

To send the file to the FTP server, a ping to the FTP server is sent using the domain name in the DNS server, it replied positively. Then the command (FTP {ip-address}) is used to form a connection with the FTP server, it will ask for the username and password and since this device is in the Finance VLAN it used the Finance user, after the login the command (put {file-name}) is used to transfer the file to the server. The server replied to the transfer positively and using the command (dir) the file finance.txt is shown to be in the FTP server files.

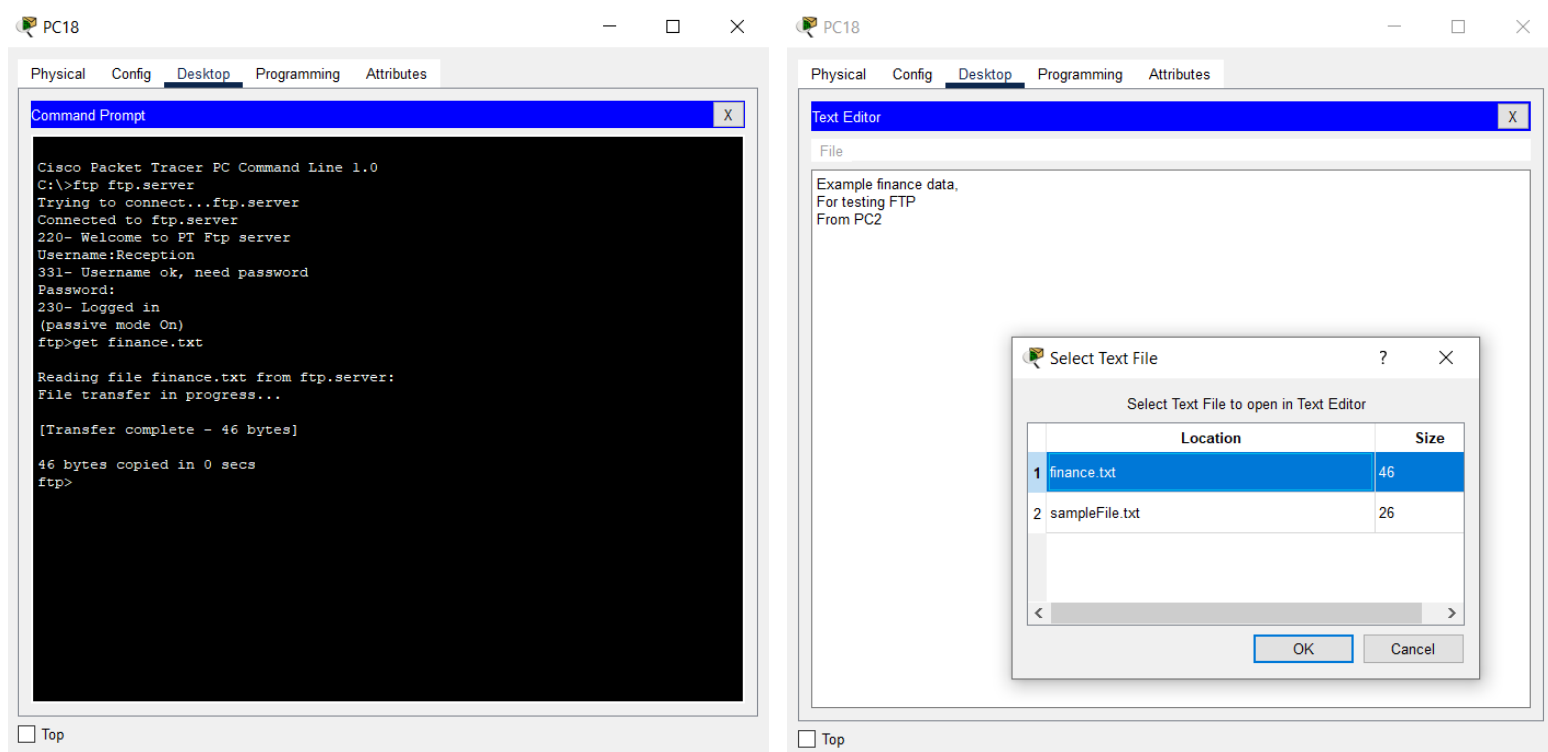
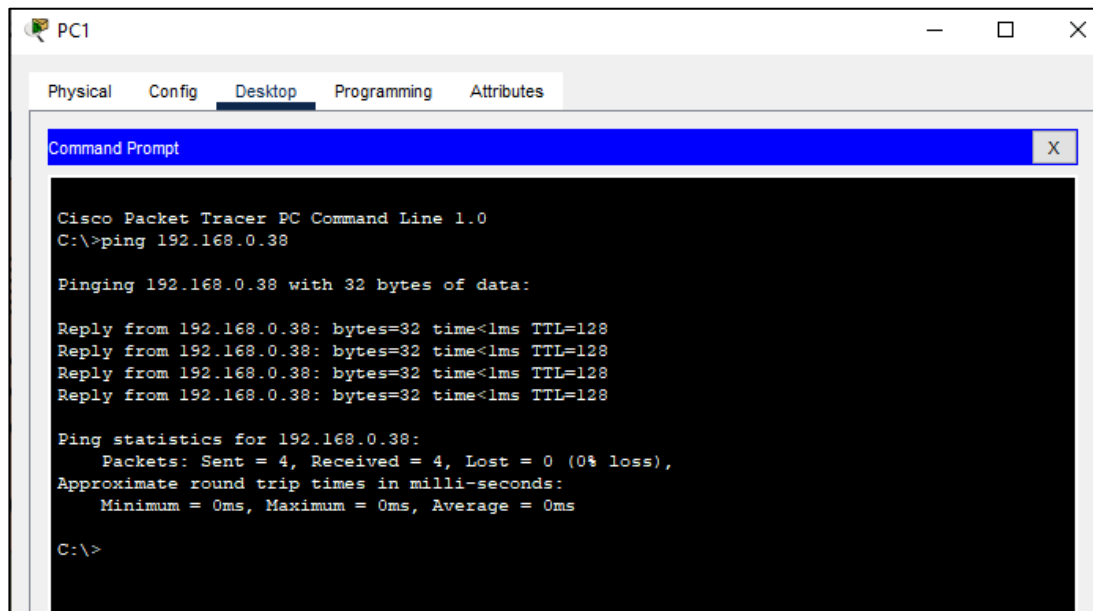


Figure 52: Retrieving finance.txt file from DNS server

On another device PC18 an attempt to download the file finance.txt is presented in the figure above, the device is part of the Reception VLAN, so it connected with its Reception user. To obtain the file the command (get {file-name}) is used. The transfer was complete and the file finance.txt is shown on the text editor of PC18. This process showcases the implementation of the FTP server in the network.

Test the Connectivity

Pinging two hosts from the same VLAN:



The screenshot shows a Cisco Packet Tracer PC window for PC1. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt shows the execution of the command 'ping 192.168.0.38'. The output indicates that the ping was successful, with 4 packets sent and 4 received, resulting in 0% loss. The round trip times are all 0ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.38

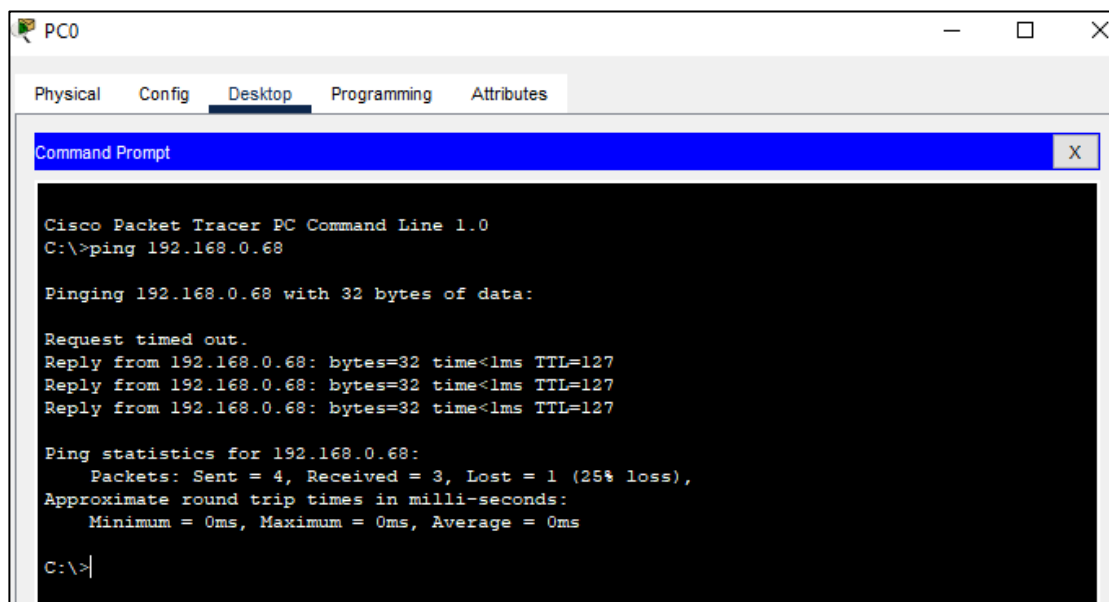
Pinging 192.168.0.38 with 32 bytes of data:

Reply from 192.168.0.38: bytes=32 time<1ms TTL=128
Reply from 192.168.0.38: bytes=32 time<1ms TTL=128
Reply from 192.168.0.38: bytes=32 time<1ms TTL=128
Reply from 192.168.0.38: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging two hosts from different VLANs:



The screenshot shows a Cisco Packet Tracer PC window for PC0. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt shows the execution of the command 'ping 192.168.0.68'. The output indicates that the ping failed, with 4 packets sent and 3 received, resulting in 25% loss. The round trip times are all 0ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.68

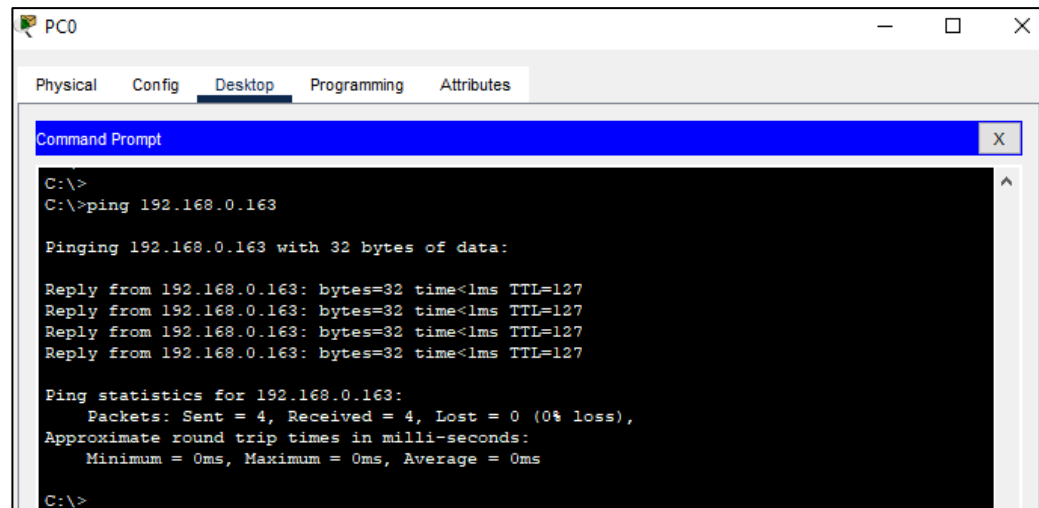
Pinging 192.168.0.68 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.68: bytes=32 time<1ms TTL=127
Reply from 192.168.0.68: bytes=32 time<1ms TTL=127
Reply from 192.168.0.68: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.68:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging the NTP Server from PC:



The screenshot shows a window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 192.168.0.163'. The output indicates a successful ping to the NTP server at 192.168.0.163, with four replies showing 32 bytes, time <1ms, and TTL=127. The statistics show 4 packets sent, 4 received, and 0% loss.

```
C:\>
C:\>ping 192.168.0.163

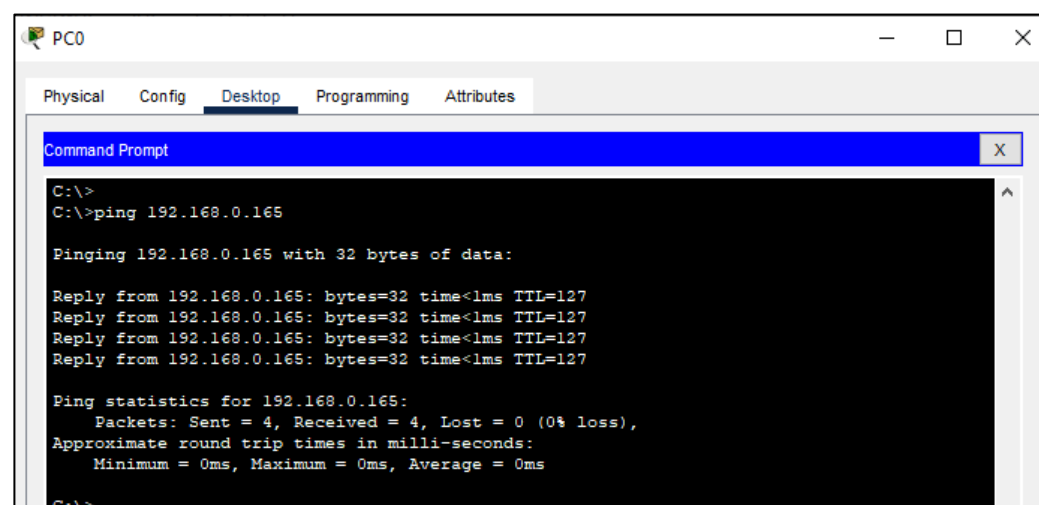
Pinging 192.168.0.163 with 32 bytes of data:

Reply from 192.168.0.163: bytes=32 time<1ms TTL=127
Reply from 192.168.0.163: bytes=32 time<1ms TTL=127
Reply from 192.168.0.163: bytes=32 time<1ms TTL=127
Reply from 192.168.0.163: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging the Syslog Server from PC:



The screenshot shows a window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 192.168.0.165'. The output indicates a successful ping to the Syslog server at 192.168.0.165, with four replies showing 32 bytes, time <1ms, and TTL=127. The statistics show 4 packets sent, 4 received, and 0% loss.

```
C:\>
C:\>ping 192.168.0.165

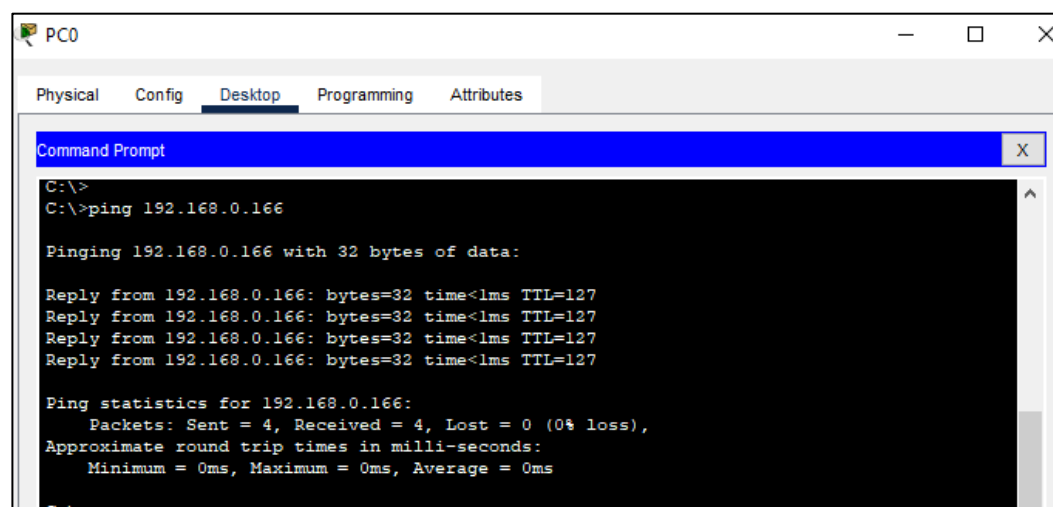
Pinging 192.168.0.165 with 32 bytes of data:

Reply from 192.168.0.165: bytes=32 time<1ms TTL=127
Reply from 192.168.0.165: bytes=32 time<1ms TTL=127
Reply from 192.168.0.165: bytes=32 time<1ms TTL=127
Reply from 192.168.0.165: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.165:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging FTP Server from PC:



The screenshot shows a window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 192.168.0.166'. The output indicates a successful ping to the FTP server at 192.168.0.166, with four replies showing 32 bytes, time <1ms, and TTL=127. The statistics show 4 packets sent, 4 received, and 0% loss.

```
C:\>
C:\>ping 192.168.0.166

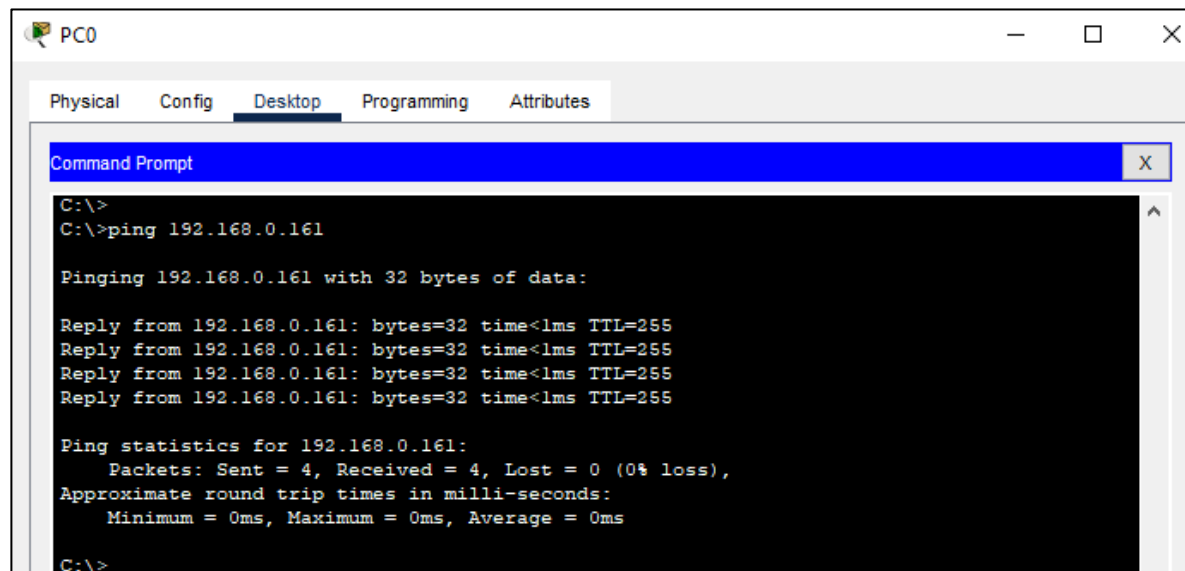
Pinging 192.168.0.166 with 32 bytes of data:

Reply from 192.168.0.166: bytes=32 time<1ms TTL=127
Reply from 192.168.0.166: bytes=32 time<1ms TTL=127
Reply from 192.168.0.166: bytes=32 time<1ms TTL=127
Reply from 192.168.0.166: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.166:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging the Web Server from PC:



The screenshot shows a window titled "PC0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the command "ping 192.168.0.161". The output indicates a successful ping to 192.168.0.161 with 32 bytes of data. The ping statistics show 4 packets sent, 4 received, and 0% loss.

```
C:\>
C:\>ping 192.168.0.161

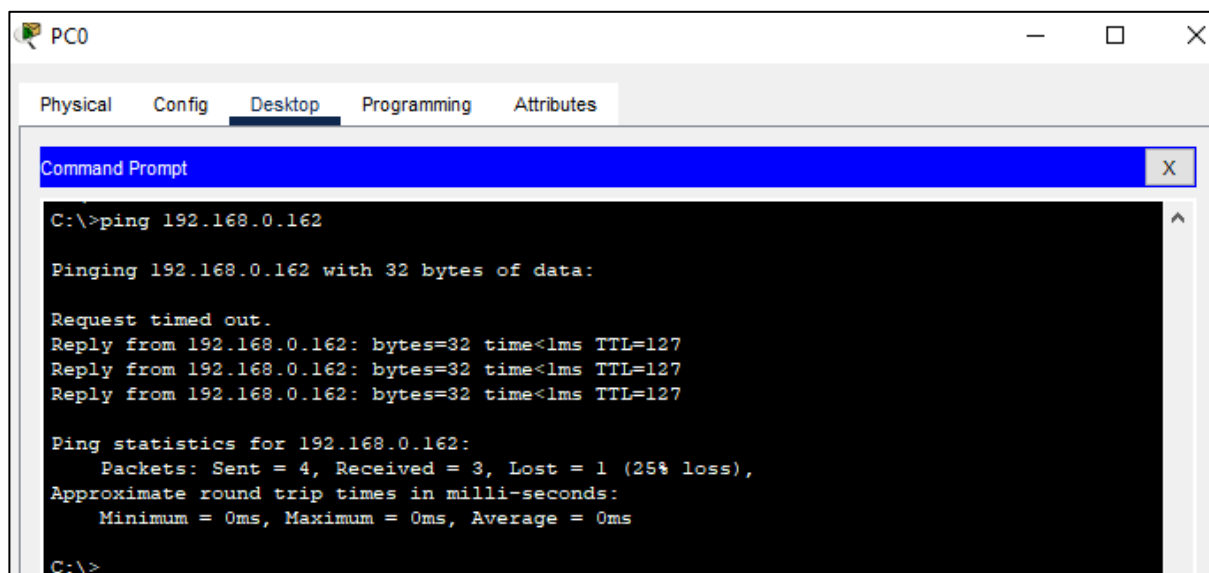
Pinging 192.168.0.161 with 32 bytes of data:

Reply from 192.168.0.161: bytes=32 time<1ms TTL=255
Reply from 192.168.0.161: bytes=32 time<1ms TTL=255
Reply from 192.168.0.161: bytes=32 time<1ms TTL=255
Reply from 192.168.0.161: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.161:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pinging the DNS Server from PC:



The screenshot shows a window titled "PC0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the command "ping 192.168.0.162". The output indicates a failed ping to 192.168.0.162 with 32 bytes of data. The ping statistics show 4 packets sent, 3 received, and 25% loss.

```
C:\>ping 192.168.0.162

Pinging 192.168.0.162 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.162: bytes=32 time<1ms TTL=127
Reply from 192.168.0.162: bytes=32 time<1ms TTL=127
Reply from 192.168.0.162: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.162:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Conclusion:

Several protocols allow routers and switches to connect with the network's devices. We explained the protocols and how to configure them on the devices in this report. In addition, we explained the features and characteristics of all the technologies and protocols we used in the network. Additionally, by working on this project, we improved our self-learning abilities and expanded our knowledge of network configuration in Cisco packet tracer, where we put the skills and knowledge, we have already learned in the course to use. It was a great project where we faced a variety of problems that pushed us to put in attempt and improve our research and problem-solving skills.

References:

- 1- infoblox. What is a DHCP Server? [online]. Available: <https://www.infoblox.com/glossary/dhcp-server/>
- 2- ciscopress. Inter-VLAN Routing [online]. Available: <https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4>
- 3- hostinger. What Is a Web Server? How It Works and More [online]. Available: <https://www.hostinger.com/tutorials/what-is-a-web-server>
- 4- study-ccna. What is VLAN? [online]. Available: <https://study-ccna.com/what-is-a-vlan/>
- 5- geeksforgeeks. Routing Information Protocol (RIP) [online]. Available: <https://www.geeksforgeeks.org/routing-information-protocol-rip/>
- 6- YouTube: Cisco Packet Tracer Labs Channel, 2021. " 10 3 4 Packet Tracer - Configure and Verify NTP," September 25th, 2021. [<https://www.youtube.com/watch?v=FI-BuvahfOU>].<https://www.youtube.com/watch?v=FI-BuvahfOU>].
- 7- YouTube: David Dalton Channel, 2021. " Configuring Syslog and NTP," May 27th, 2020. [<https://www.youtube.com/watch?v=3lxH2nwLi-4>].
- 8- YouTube: Titas Sarker Channel, 2021. " How to configure NTP server in Cisco router?," March 15th, 2018. [<https://www.youtube.com/watch?v=ahLANvMSIJs>].
- 9- YouTube: Cisco Packet Tracer Labs Channel, 2021. " [CCNA Bridging] Packet Tracer 2.3.1.5 Configure and verify NTP," February 14th, 2017. [<https://www.youtube.com/watch?v=Ti37u6oO5ns>].
- 10- YouTube: Unique Rifat Channel, 2029. " dns server in cisco packet tracer||how to configure a dns server," August 1st, 2020. [https://www.youtube.com/watch?v=yZFBNJLz1z0&ab_channel=UniqueRifat].
- 11- YouTube: Easy Learning Tutorials Channel, 2021. " FTP Server Using CISCO Packet Tracer || CCNA videos easy learning tutorials," April 27th, 2021. [https://www.youtube.com/watch?v=Mk5WUsHOK0Y&ab_channel=EasyLearningTutorials].

Team Worksheet

MEMBER	TASK
OMAR AHMED ELDANASOURY ITCE416 – SEC 02 202005808	1- PLANNING 2- TOPOLOGY DESIGN 3- PROJECT SCOPE 4- NTP 5- SSH 6- SYSLOG 7- TEST CONNECTIVITY 8- DOCUMENT FORMAT
HESHAM AHMED GHULAM ITNE241 – SEC02 202003472	1- TOPOLOGY DESIGN 2- SUBNETTING & INTERFACE CONFIG 3- VLANS 4- INTER-VLAN (ROAS) 5- RIPV2 ROUTING PROTOCOL 6- DHCP SERVER 7- WEB SERVER 8- TEST CONNECTIVITY 9- TABLE OF CONTENTS 10- CONCLUSION
MOHAMED HESHAM ALAMMAL ITCE416 – SEC02 202009144	1- PLANNING 2- TOPOLOGY DESIGN 3- INTRODUCTION 4- DNS SERVER 5- FTP SERVER 6- TEST CONNECTIVITY