University of Bahrain
College of Information Technology
Department of Computer Engineering

Network Infrastructure Design and Implementation for Infinx Electronics Company

Prepared By:
Zahid Saleh Muthanna Muhammed

Table of Contents

1.1 Abstract……..4
2.1 Introduction……4
3.1 Objectives……4
4.1 Description……5
5.1 Requirements……6
6.1 Used Devices……7
7.1 Cables Used……7
7.2 Passwords……7
8.1 Infinx Electronics Network Topology ……8
9.1 Subnetting and IP Addressing……9
10.1 Configuration of hostname, banner message, password, domain lookup, and password encryption on layer2 switches, layer3 switches, and layer3 routers. ……10
11.1 VLANs……12
11.1.1 Overview of VLAN ……12
11.1.2 Advantages of VLANs ……12
11.1.3 Step#1 VLANs on Access Layer Switches……12
11.1.3 Step#2 VLANs and Inter-VLANS on Layer 3 Switches……13
12.1 IP Addresses Assignments……14
12.1.1 Layer 3 Switch Interfaces to Core routers Interfaces ……14
12.1.2 Core Router's Interfaces to Layer 3 Switch Interfaces ……15
12.1.3 Core Router's Interfaces to ISPs Router's Interfaces ……16
12.1.4 ISPs Router's Interfaces to Core Router's Interfaces ……17
13.1 Secure Shell (SSH) Configuration……18
13.1.1 Overview about SSH ……18
13.1.2 Key points about SSH:……18
13.1.3 SSH Configuration on Multilayer Switch ……18
13.1.4 SSH configuration on Layer 3 Routers……19
14.1 OSPF Configuration ……20
14.1.1 Overview about OSPF ……20
14.1.2 Key points about OSPF:……20
14.1.3 OSPF Configuration on Multilayer Switches ……20
14.1.4 OSPF Configuration on Layer3 Routers ……21
14.1.5 OSPF Configuration on ISPs Routers……21
14.1.6 OSPF, NAT Overload, RIP, ACL Show Results……22

15.1 Servers Infrastructure and configuration 23
15.1.1 DHCP Server 23
15.1.2 DNS Server 24
15.1.3 Web Server 25
15.1.4 FTP Server 26
15.1.5 Email Server 27
16.1 Wireless Configuration 28
17.1 IOT Door Configuration 30
19.1 Testing and verifying the connectivity 32
20.1 Conclusion 34

1.1 Abstract

This project involves designing a computer network topology using Cisco Packet Tracer for Infinix Electronics (a global mobile electronics company). Computer networks are crucial in today's business world due to the increasing number of electronic devices. Cisco Packet Tracer is a simulation software that allows for network design, configuration, and troubleshooting without affecting real networks. It provides a powerful tool for learning network design principles and allows visualization of network behavior and connectivity. With Packet Tracer, designers can create network topologies, test connectivity, and simulate the behavior of different network devices, such as routers, switches, servers, and access points.

2.1 Introduction

In today's world, computer networks have become an essential aspect of every business. With the increasing number of electronic devices, the demand for effective and efficient networks has increased as well. In this project, we are designing a network for a mobile electronics company called Infinix Electronics, which operates globally. The network will be designed using Cisco Packet Tracer, a simulation software that allows us to design, configure and troubleshoot networks.

Packet Tracer is a powerful tool that enables network designers to simulate network configurations and test them without disrupting real networks. It is an essential tool for learning about network design and allows network administrators to visualize network behavior and connectivity. With Packet Tracer, network designers can create network topologies, test connectivity, and simulate the behavior of network devices. The software includes a variety of networking devices, such as routers, switches, servers, and access points, which can be easily configured to simulate real-world scenarios.

The proposed network for Infinix Electronics will encompass four floors, and we will highlight the components and relevant connectivity in this report. We will implement VLANs and configure IP routing, DHCP, inter-VLAN-related configuration, etc. In this report, we will discuss the design and implementation of the network using Cisco Packet Tracer, focusing on the relevant configurations, the challenges faced, and their solutions.

3.1 Objectives

- Develop self-learning skills.
- Expand learner knowledge in the Network configuration in Cisco tracer.
- Apply the skills and knowledge learned in the course to design and configure institutional networks.
- Practicing Cisco tracer tool.

4.1 Description

Infinix Electronics, a global mobile electronics company, is currently expanding and in the process of relocating to a new building. However, the chosen building lacks an existing network infrastructure. Therefore, before the company can proceed with the move, it is essential to design and implement a new network system for the building. This network implementation project aims to provide seamless connectivity and communication throughout the building.

The new building will consist of four floors, each accommodating two departments:

- The first floor will house the Production and Customer Services departments.
- The second floor will accommodate Sales and Marketing.
- The third floor will be allocated to the Acc/Finance and HR departments.
- The fourth floor will serve as the IT department and house the room servers.
- Furthermore, it is recommended to establish a dedicated wireless network for the break area of the staff.

To ensure a smooth transition, Infinix Electronics hired us as a network engineers team. Our responsibility will be to design and implement a reliable, redundant network system that caters to the specific needs of each department and facilitates efficient communication and collaboration. By successfully completing this project, Infinix Electronics aims to establish a robust network infrastructure that supports its expanding operations and promotes seamless connectivity among its various departments in the new building.

5.1 Requirements

To ensure that the new network for Infenix Electronics meets the current business requirements and remains adaptable for future needs, we need to focus on logical design. The logical design encompasses the following requirements that will be implemented:

1. We'll implement a topology with a redundant connection at every layer for fault tolerance using two routers (*Core-R1, Core-R2*), two multilayer switches, and two routers' ISPs. *Note:* (*we'll use an AC Power Supply module in each multilayer switch to provide electrical power to the device*)
2. For each department, we'll allocate an access layer switch.
3. In order to achieve high performance, reliability, scalability, and simplified troubleshooting, we will use suitable cables for connecting routers, routers to multilayer switches, and switches to end systems.
4. In order for the routers to be connected with each other using DTE Serial connection, we will use HWIC-2T module inside each router (*The HWIC-2T is a Cisco 2-Port Serial High-Speed WAN Interface Card, providing 2 serial ports*).
5. We'll assign a wireless network to each department for users' connectivity using Wireless Access Point (WAP). *Note:* (*we will assign a password authentication for each WAP in each department to enhance security, control access, and better management for organization's wireless network*).
6. We'll allocate different VLANs and subnets for each department with considering access ports and trunk ports on layer2 and layer3 switches.
7. For the access layer switches, multilayer switches, and core routers basic device settings, including hostnames, service password encryption, enable passwords, banner messages, and disable IP domain lookup should be implemented.
8. For efficient address allocation, network segmentation, efficient routing, and effective IP address management, we will perform a proper subnetting and IP addressing.
9. We will enable inter-VLAN routing on both layer3 switches to facilitate communication between departments.
10. For the devices on the room server, we will assign IP addresses statically. Also, we'll assign IP addresses to the multilayer switches for routing and switching functionality.
11. We'll use a dedicated DHCP server that is located in the server room to dynamically allocate IP addresses to devices in the network.
12. To provide a path for network traffic when there is no specific route available for a destination, we'll configure the default route in layer 3 switches and core routers.
13. We'll configure OSPF as the routing protocol to advertise routes on routers and layer3 switches and SSH on routers and layer3 switches for secure remote login,
14. For efficient address utilization, enabling multiple devices to share a single public IP address, providing internet access for private networks, we'll configure the NAT overload. In addition, we will configure standard and extended ACL.
15. After implementing the necessary technologies, we'll test the connectivity between departments to ensure proper configuration and functionality of all devices.

6.1 Used Devices

Device Name	Model	Quantity
Router	*2811*	*2*
Router	*2911*	*2*
Multilayer Switch	*3652-2PS*	*2*
Access Layer Switch	*2960-24TT*	*2*
Access Point	*AP-PT*	*8*
PCs	*-*	*43*
Smartphone	*-*	*11*
Tablets	*-*	*11*
Printer	*-*	*7*
IoT Door	*-*	*7*
Server	*-*	*5*

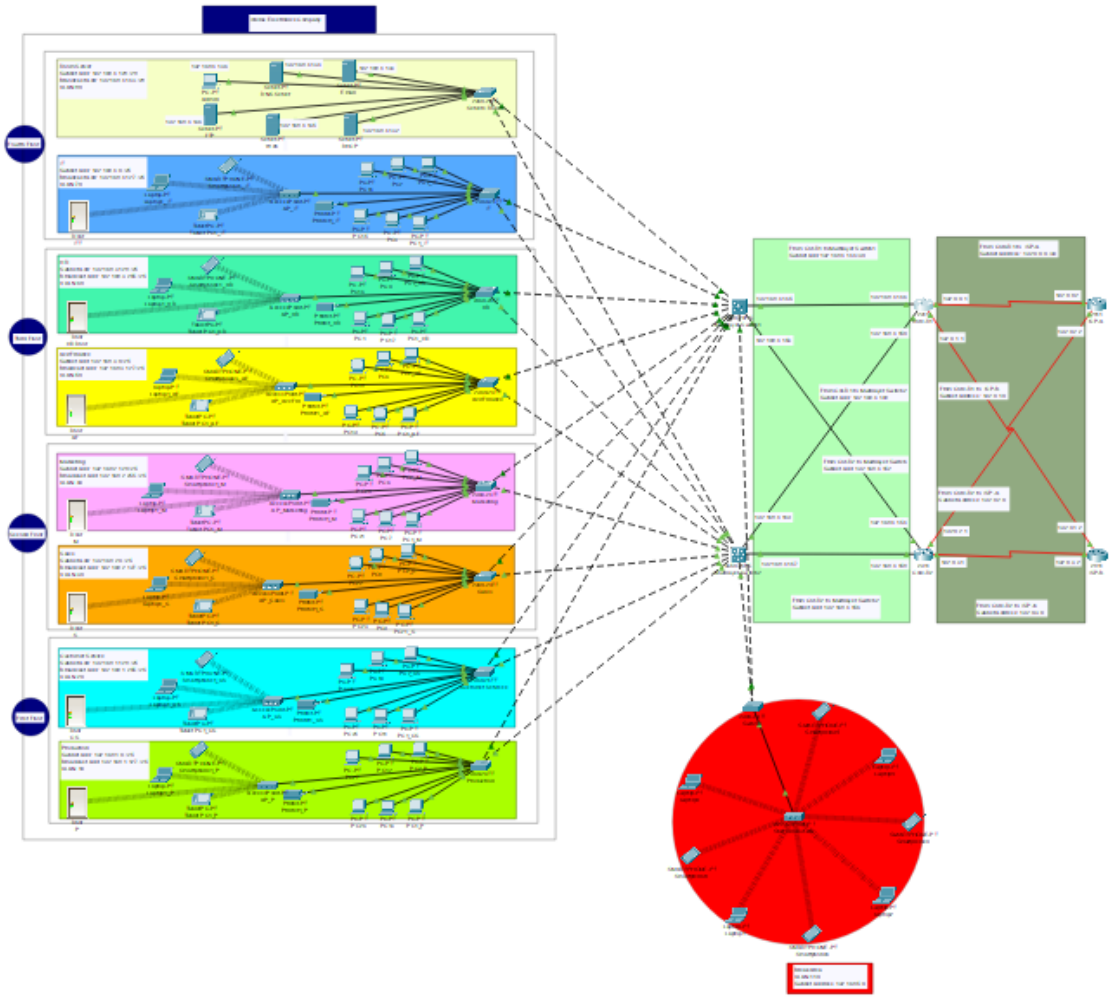
7.1 Cables Used

Location	Type
Between Routers	*Serial connection (DTE)*
Routers' to multilayer switches	*Straight-through connection*
Multilayer switches to access layer switches	*Cross-over connection*
Access layer switches to end systems	*Straight-through connection*

7.2 Passwords

Device	Password
Production-Switch	*production123*
Customer Service Switch	*cs1234*
Acc/Finance Switch	*acc/fin1234*
Marketing-Switch	*m1234*
HR-Switch	*hr1234*
IT-Switch	*it1234*
Sales-Switch	*s1234*
Main Multilayer Switch1	*mmls1*
Main Multilayer Switch2	*mmls2*
Core-R1	*corer1*
Core-R2	*corer2*

8.1 Infinx Electronics Network Topology



9.1 Subnetting and IP Addressing

- *Four Floors (Each Two Departments)*

Subnet Name	Subnet Address	First Usable Host	Last Usable Host	Broadcast Address	Subnet Mask
Production	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127	255.255.255.128/25
Customer Service	192.168.1.128	192.168.1.129	192.168.1.254	192.168.1.255	
Sales	192.168.2.0	192.168.2.1	192.168.2.126	192.168.2.127	
Marketing	192.168.2.128	192.168.2.129	192.168.2.254	192.168.2.255	
Acc/Finance	192.168.3.0	192.168.3.1	192.168.3.126	192.168.3.127	
HR	192.168.3.128	192.168.3.129	192.168.3.254	192.168.3.255	
IT	192.168.4.0	192.168.4.1	192.168.4.126	192.168.4.127	
Server Room	192.168.4.128	192.168.4.129	192.168.4.142	192.168.4.143	255.255.255.240/28

- *Between Core Routers' and Layer3 Switches*

Router and Multilayer Switch Names	Subnet Address	First Usable Host	Last Usable Host	Broadcast Address	Subnet Mask
Core-R1 to Multilayer Switch1	192.168.4.144	192.168.4.145	192.168.4.146	192.168.4.147	255.255.255.252/30
Core-R1 to Multilayer Switch1	192.168.4.148	192.168.4.149	192.168.4.150	192.168.4.151	
Core-R2 to Multilayer Switch1	192.168.4.152	192.168.4.153	192.168.4.154	192.168.4.155	
Core-R2 to Multilayer Switch1	192.168.4.156	192.168.4.157	192.168.4.158	192.168.4.159	

- *Between Core Routers and ISPs*

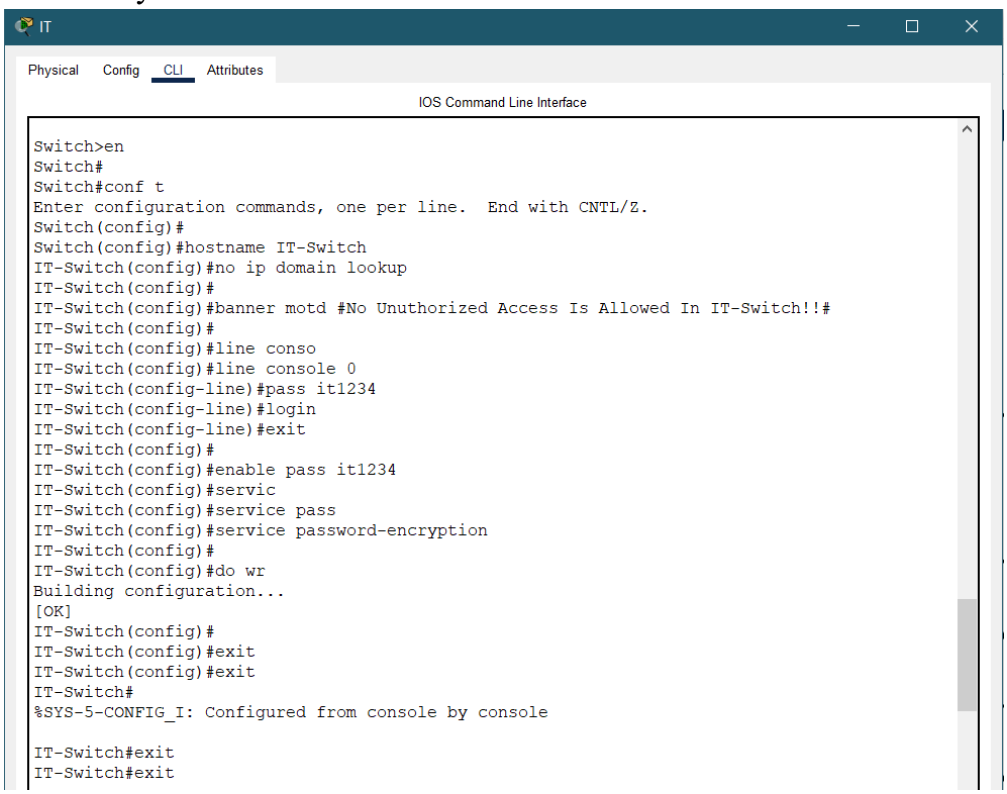
Router and ISP Names	Subnet Address	First Usable Host	Last Usable Host	Broadcast Address	Subnet Mask
Core-R1 to ISP1	192.0.0.0	192.0.0.1	192.0.0.2	192.0.0.3	255.255.255.252/30
Core-R1 to ISP2	192.0.1.0	192.0.1.1	192.0.1.2	192.0.1.3	
Core-R2 to ISP1	192.0.2.0	192.0.2.1	192.0.2.2	192.0.2.3	
Core-R2 to ISP2	192.0.3.0	192.0.3.1	192.0.3.2	192.0.3.3	

- *Wireless Subnet for Staff Break Area*

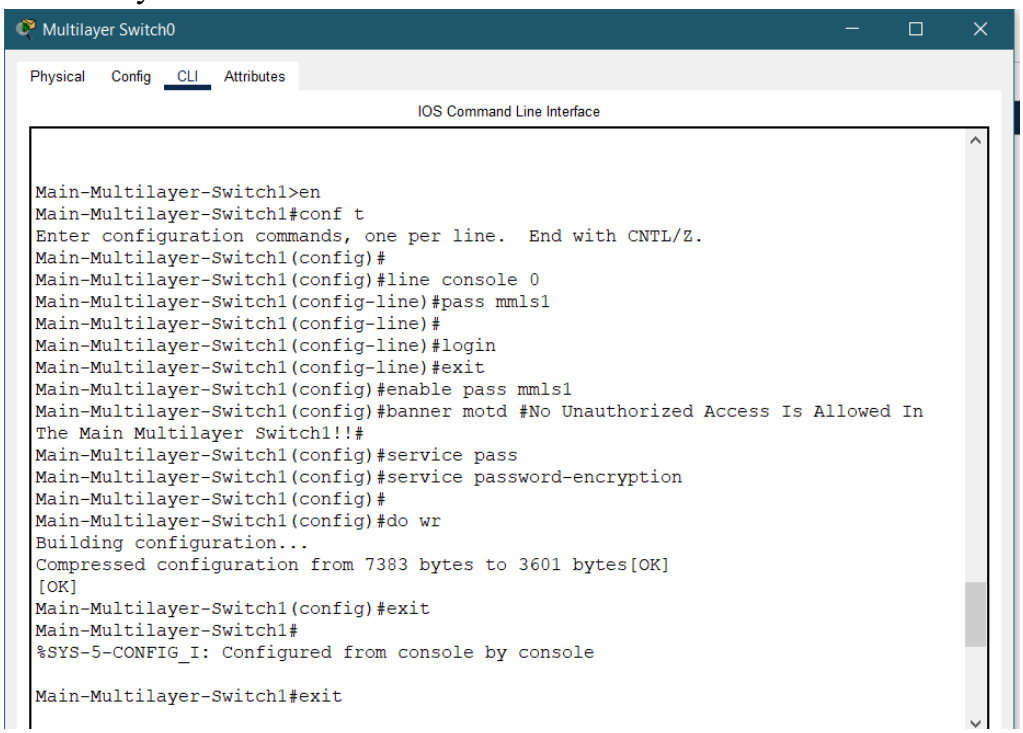
Subnet Name	Subnet Address	First Usable Host	Last Usable Host	Broadcast Address	Subnet Mask
Break Area	192.168.5.0	192.168.5.1	192.168.5.254	192.168.5.255	255.255.255.0/24

10.1 Configuration of hostname, banner message, password, domain lookup, and password encryption on layer2 switches, layer3 switches, and layer3 routers.

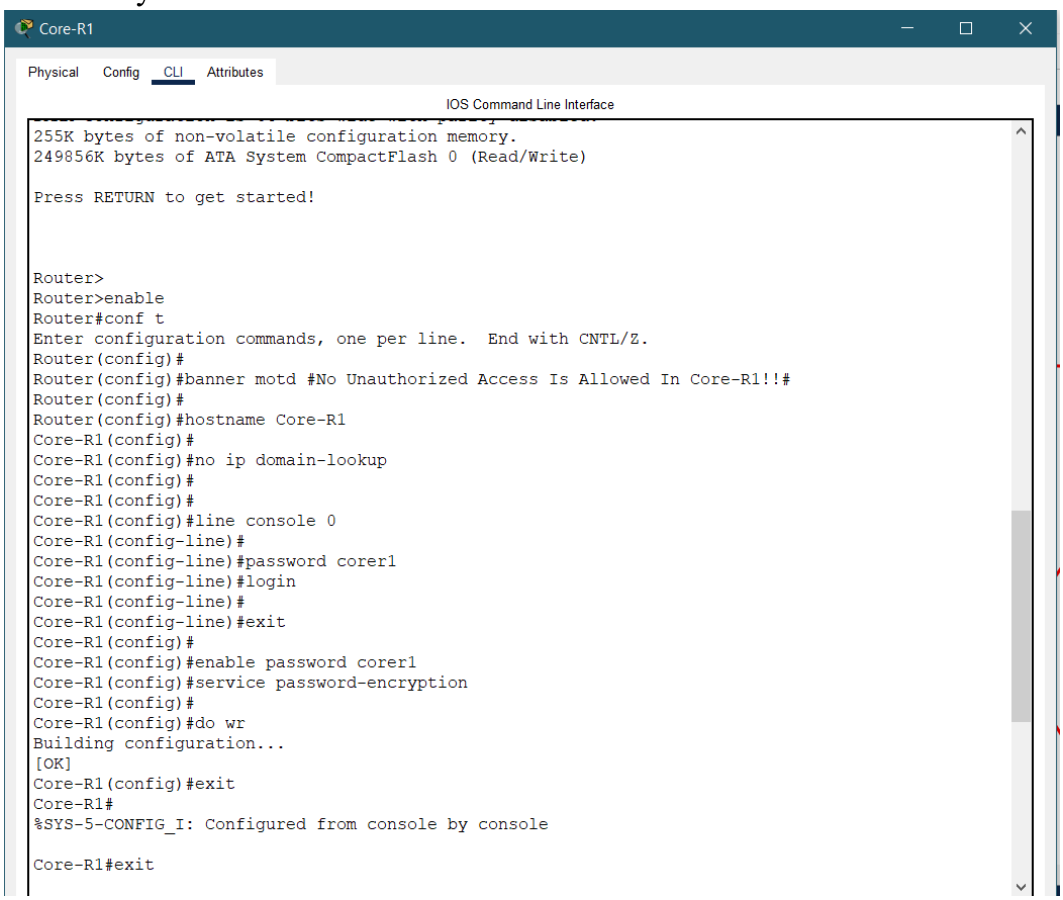
10.1.1 Layer2 Switch



Layer3 switch



10.1.3 Layer3 router



11.1 VLANs

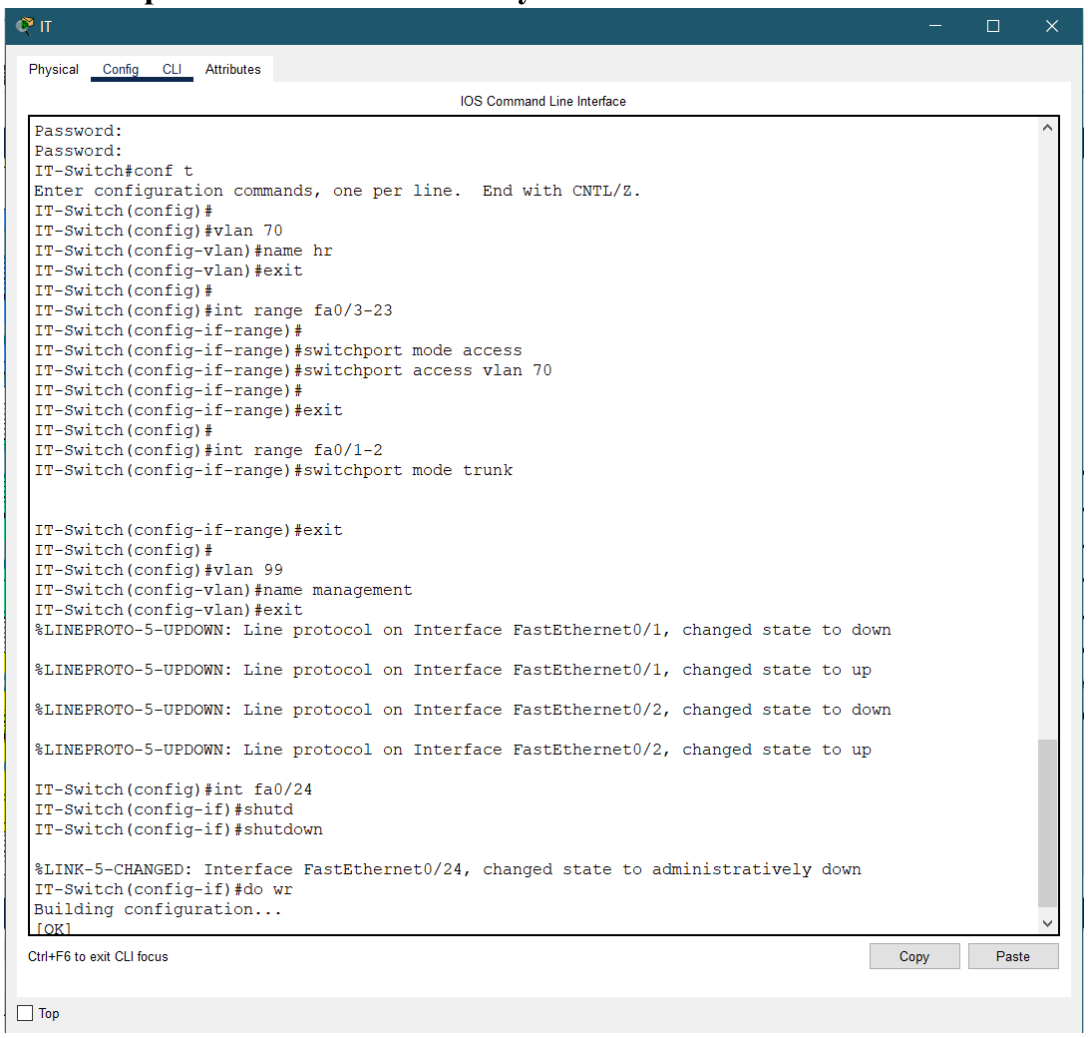
11.1.1 Overview of VLAN

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a network, allowing them to communicate as if they were on the same physical network segment, regardless of their physical location.

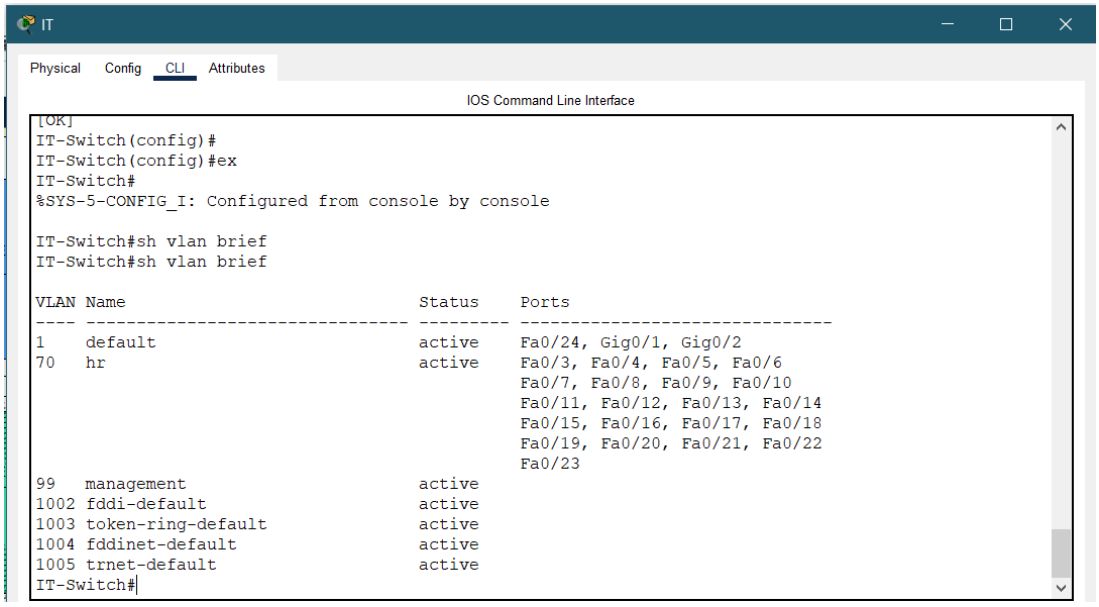
11.1.2 Advantages of VLANs

1. Optimized Resource Utilization
2. Support for Virtualization
3. Simplified Network Management
4. Enhanced Network Security
5. Isolate traffic

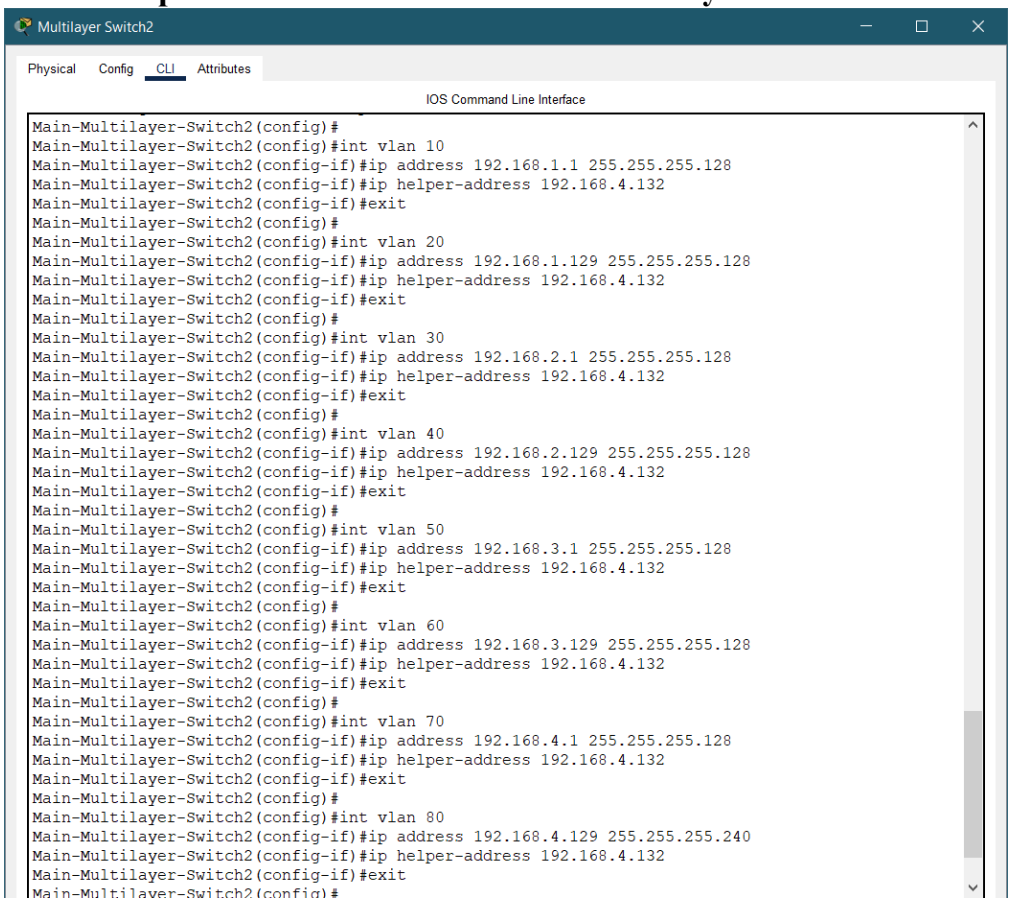
11.1.3 Step#1 VLANs on Access Layer Switches



Result



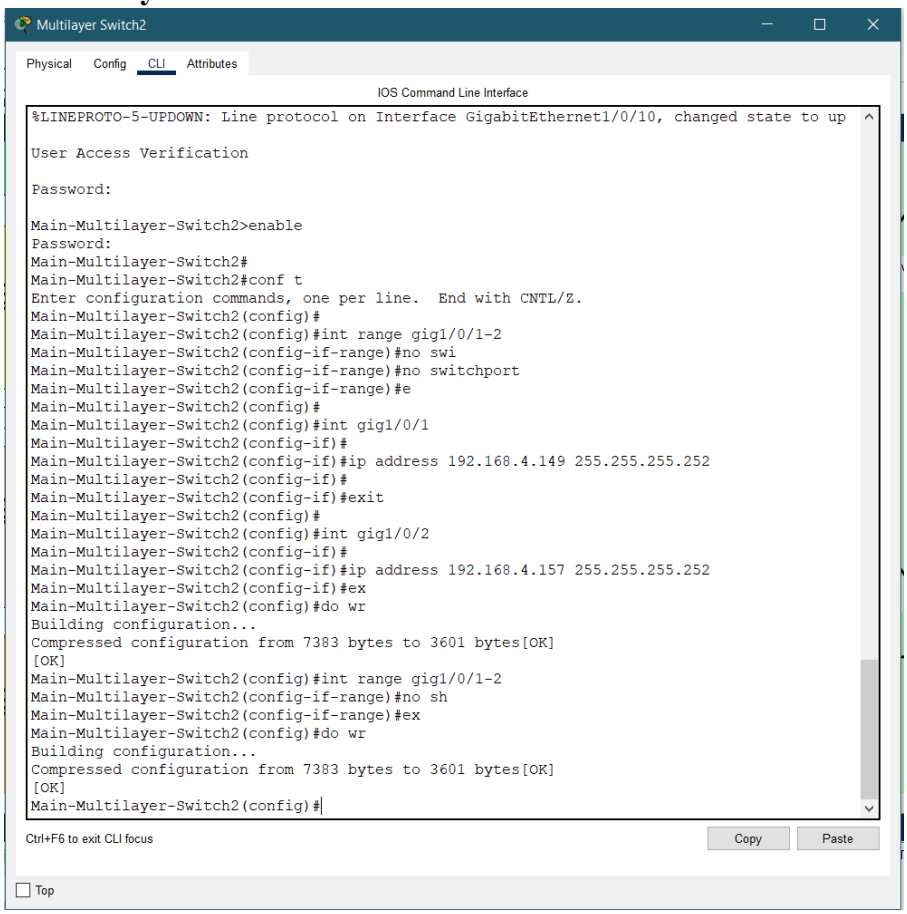
11.1.3 Step#2 VLANs and Inter-VLANS on Layer 3 Switches



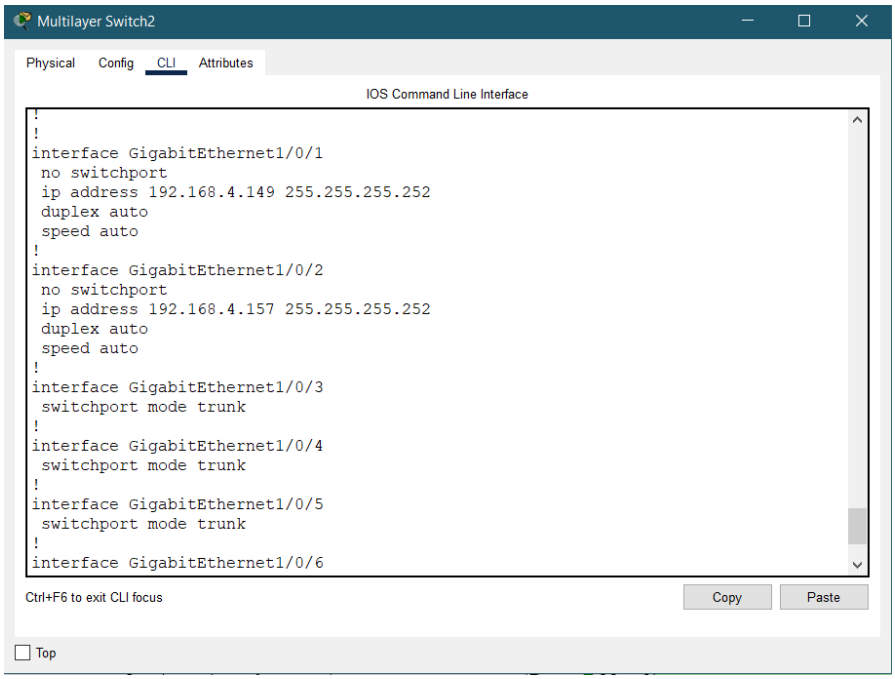
Inter- vlans

12.1 IP Addresses Assignments

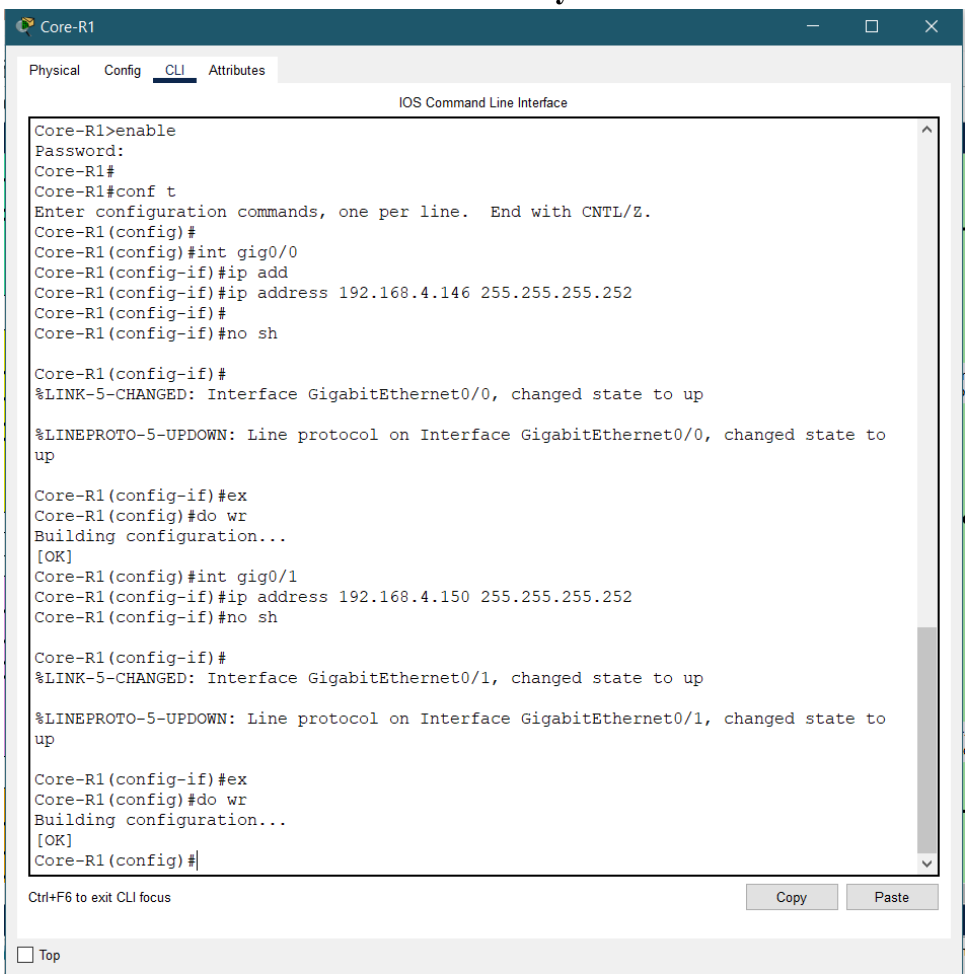
12.1.1 Layer 3 Switch Interfaces to Core routers Interfaces

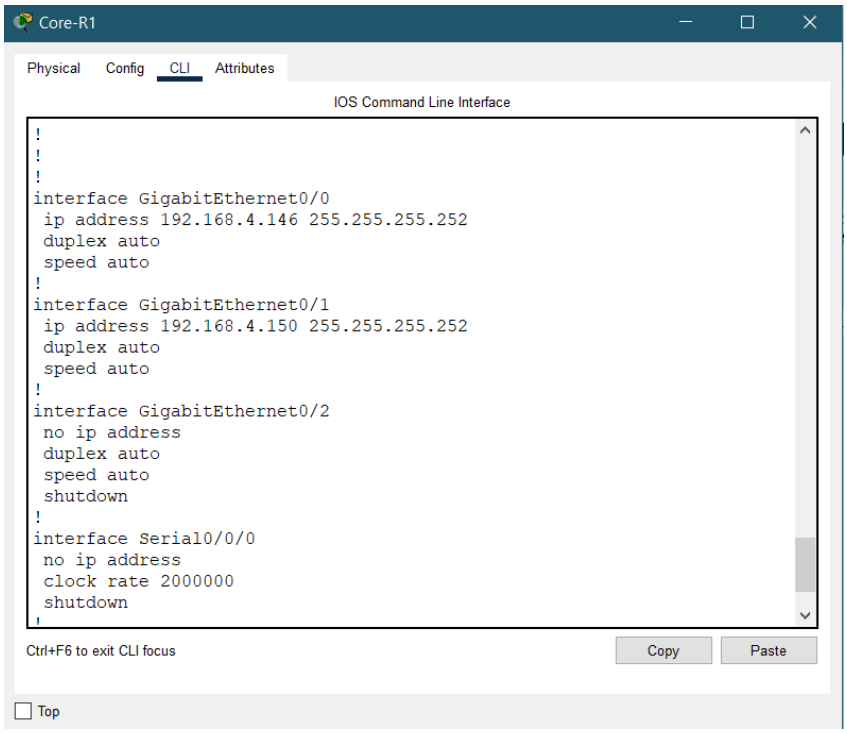


Result

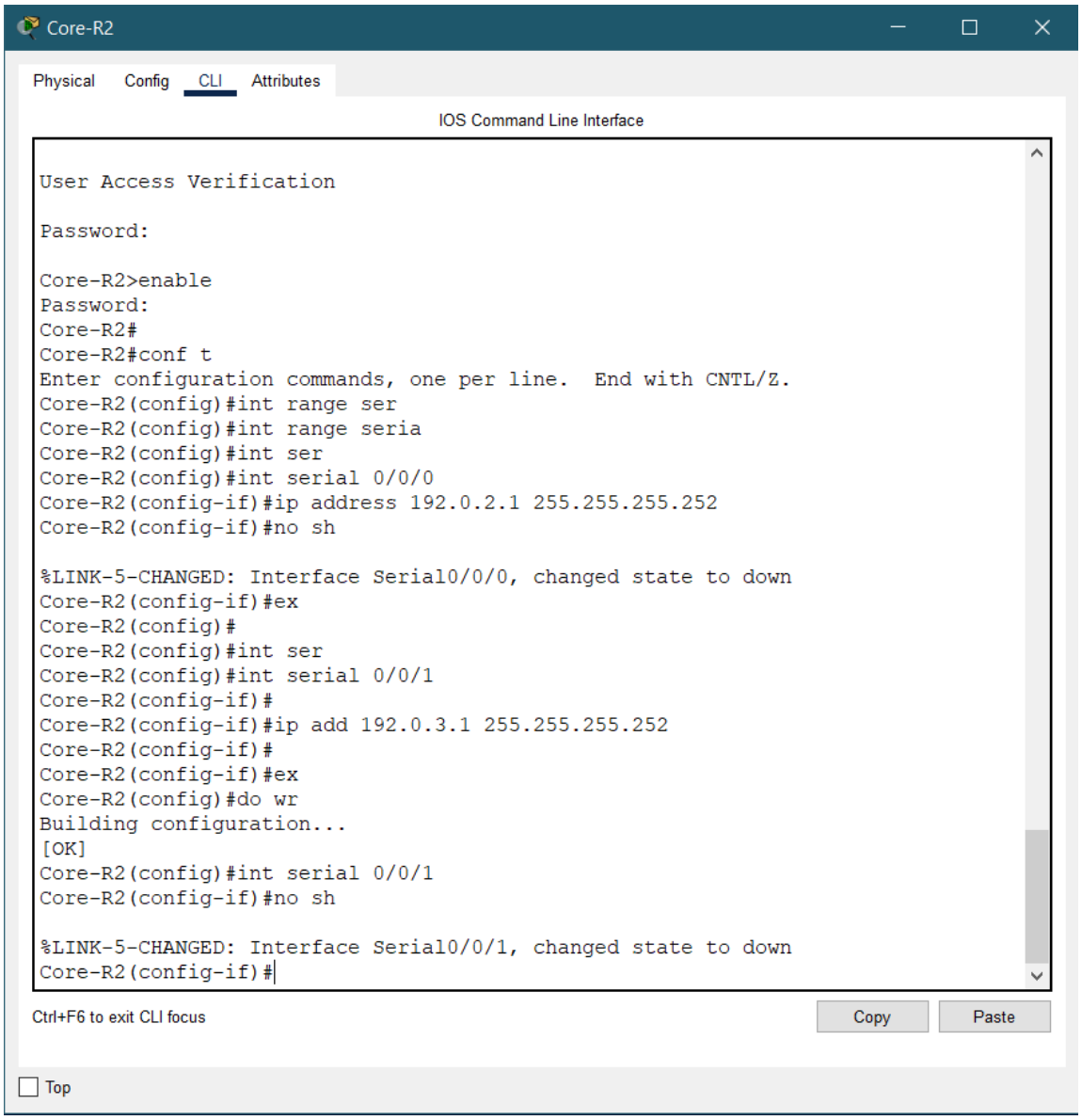


12.1.2 Core Router's Interfaces to Layer 3 Switch Interfaces

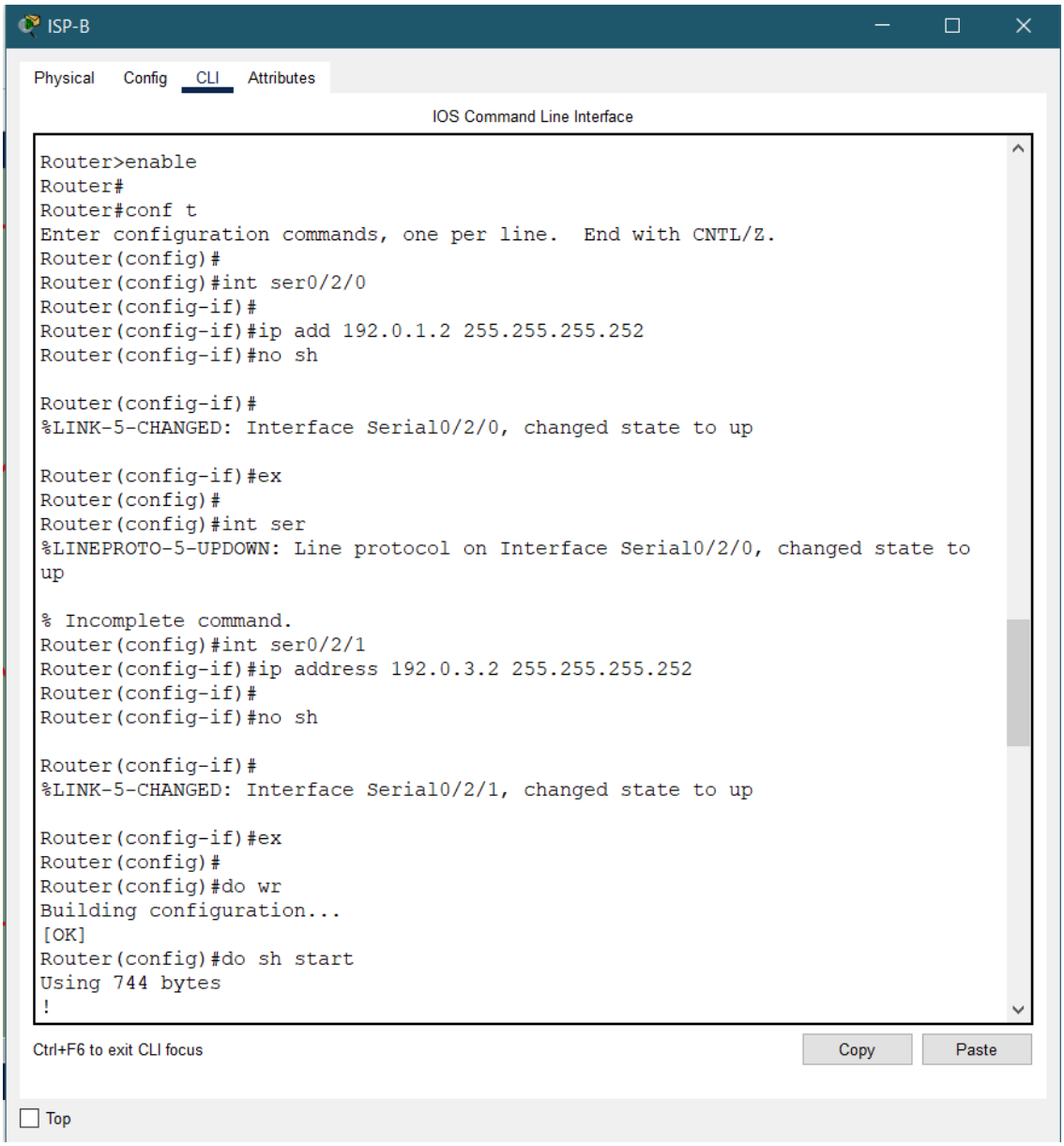




12.1.3 Core Router's Interfaces to ISPs Router's Interfaces



12.1.4 ISPs Router's Interfaces to Core Router's Interfaces



13.1 Secure Shell (SSH) Configuration

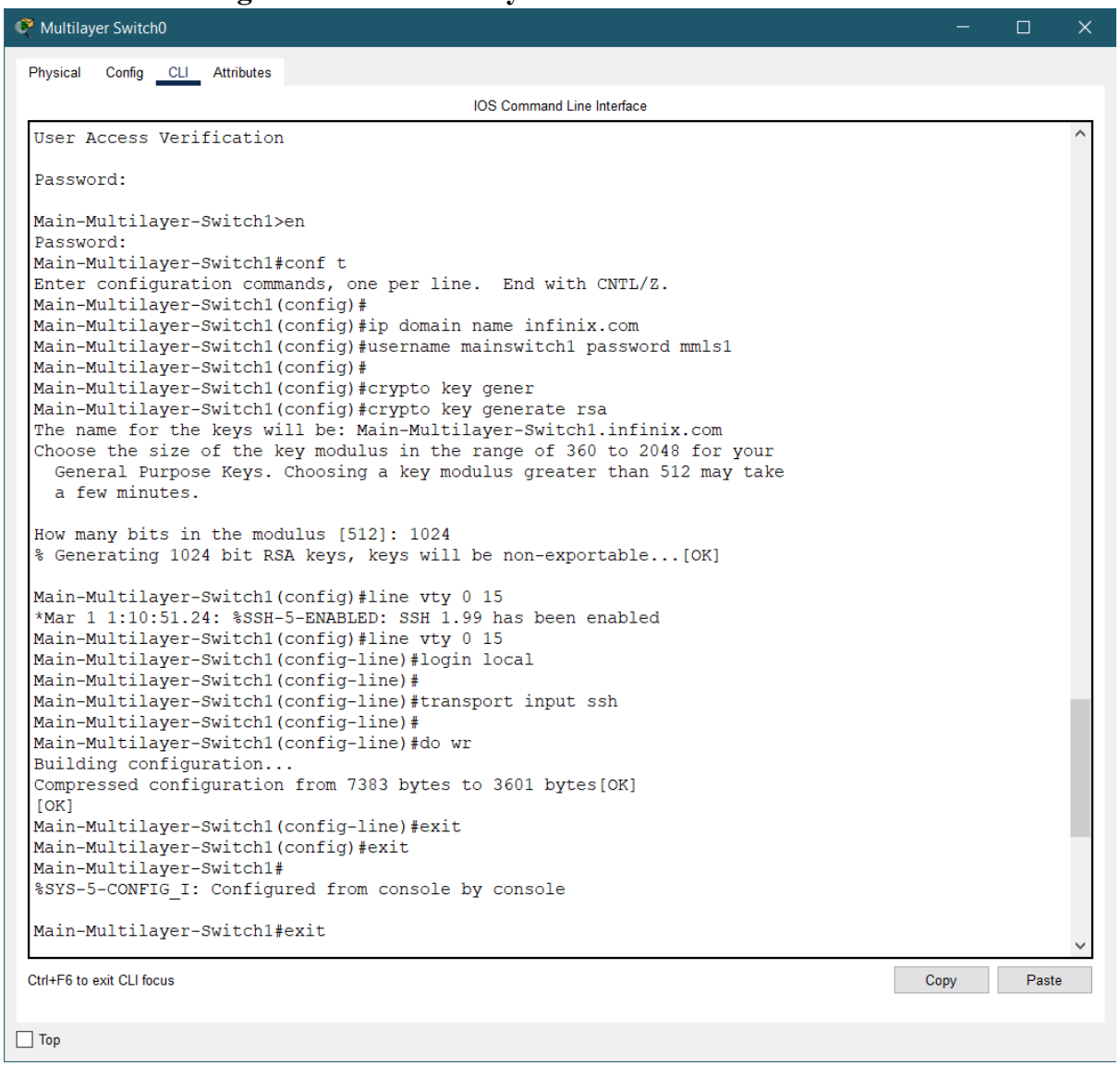
13.1.1 Overview about SSH

SSH (Secure Shell) is a network protocol that enables secure and encrypted remote login and command execution. It replaces insecure protocols like Telnet and rlogin by providing strong encryption, authentication, and data integrity.

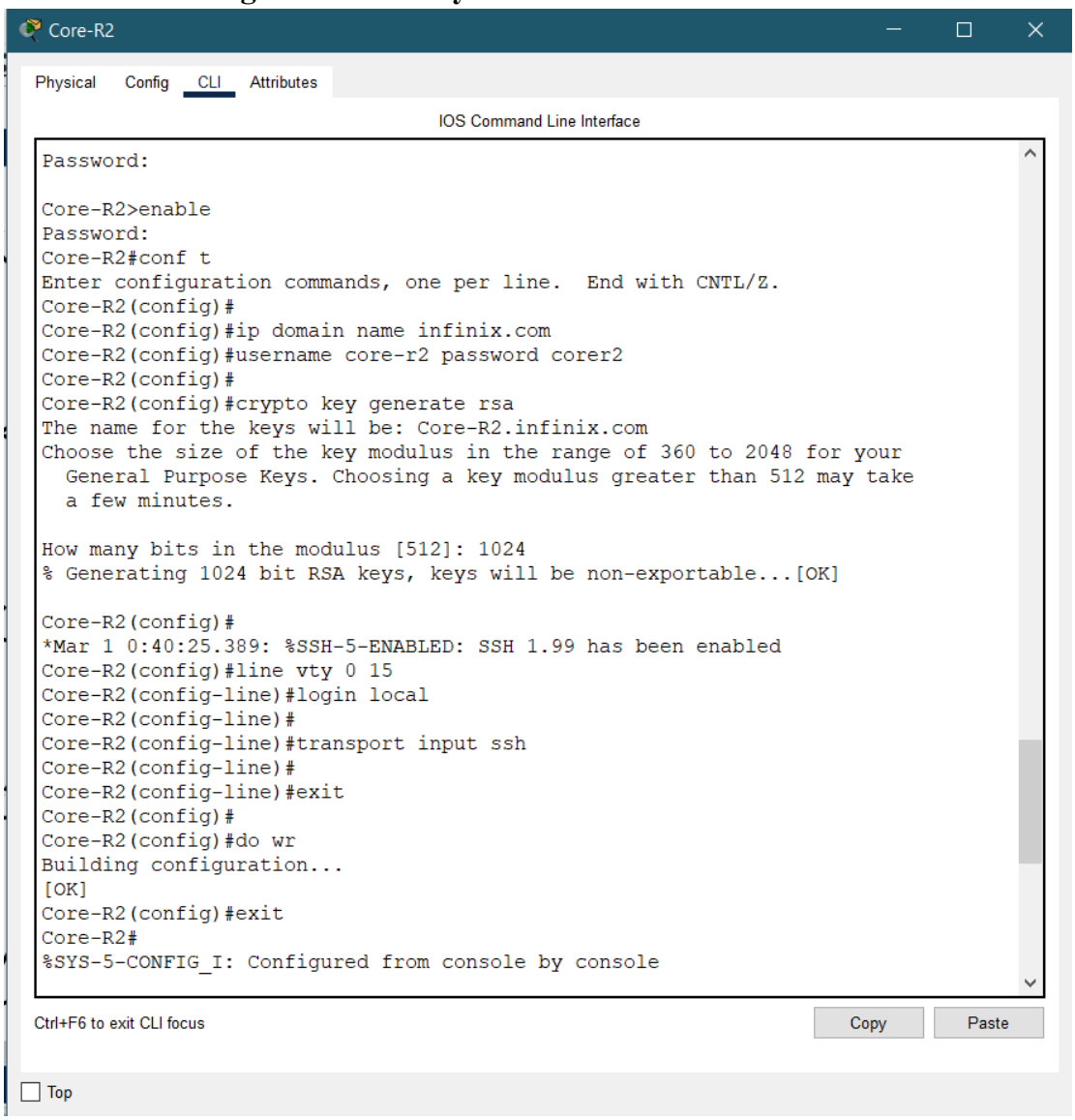
13.1.2 Key points about SSH:

1. Encryption
2. Secure Remote Access
3. Authentication

13.1.3 SSH Configuration on Multilayer Switch



13.1.4 SSH configuration on Layer 3 Routers



Including RSA encryption with login to the local database

14.1 OSPF Configuration

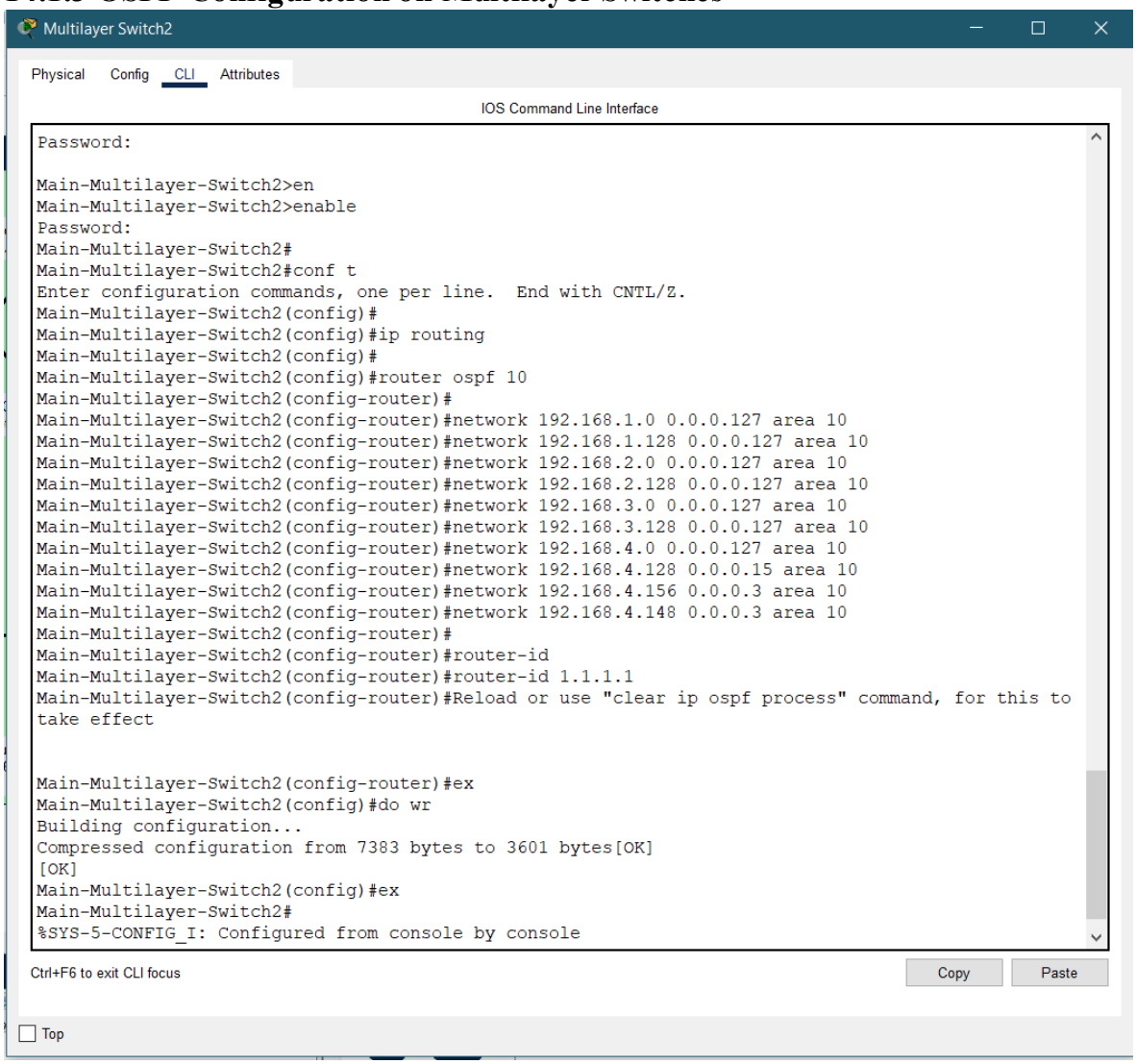
14.1.1 Overview about OSPF

OSPF stands for Open Shortest Path First, and it is a routing protocol used in computer networks to determine the best paths for forwarding network traffic. It is an interior gateway protocol (IGP) commonly used within an autonomous system (AS), such as an enterprise network or an internet service provider's network.

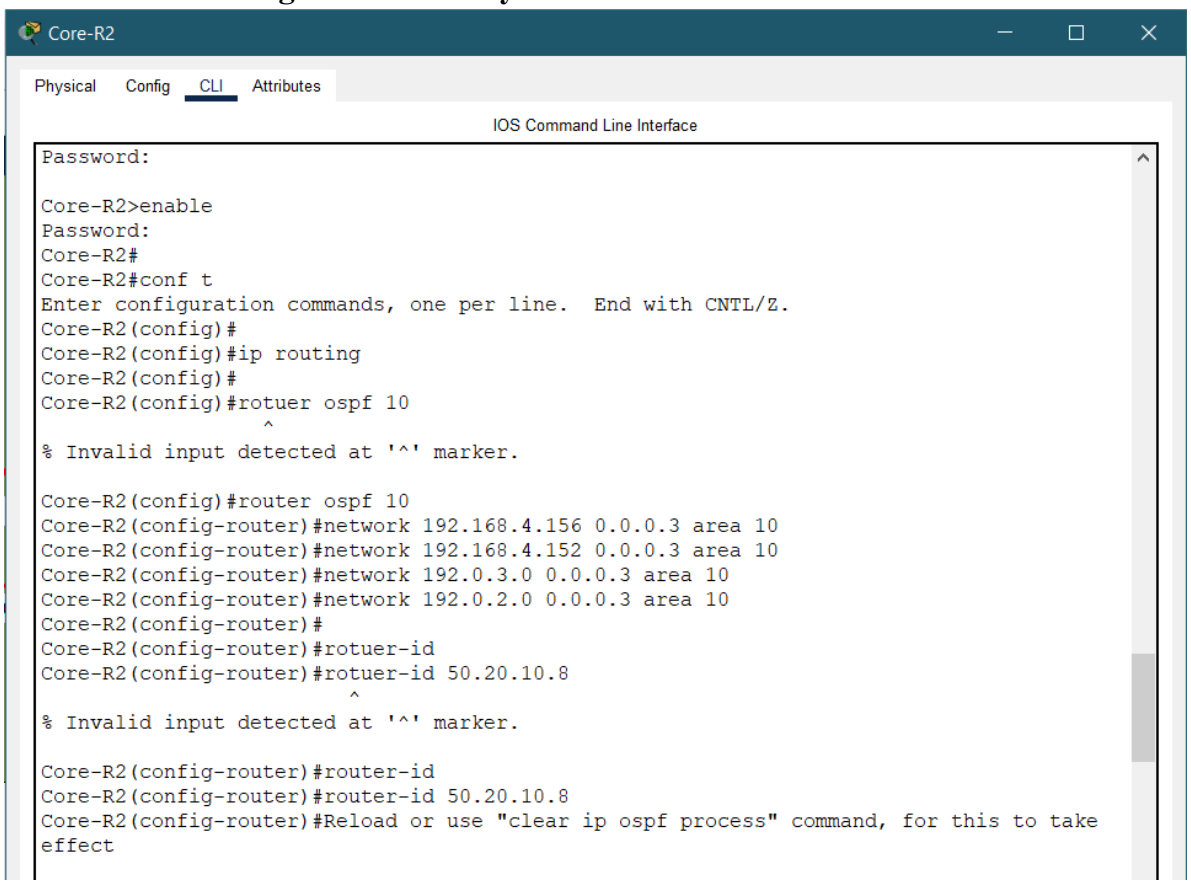
14.1.2 Key points about OSPF:

1. Link-State Protocol
2. Dynamic Routing Updates
3. Shortest Path Calculation
4. Load Balancing

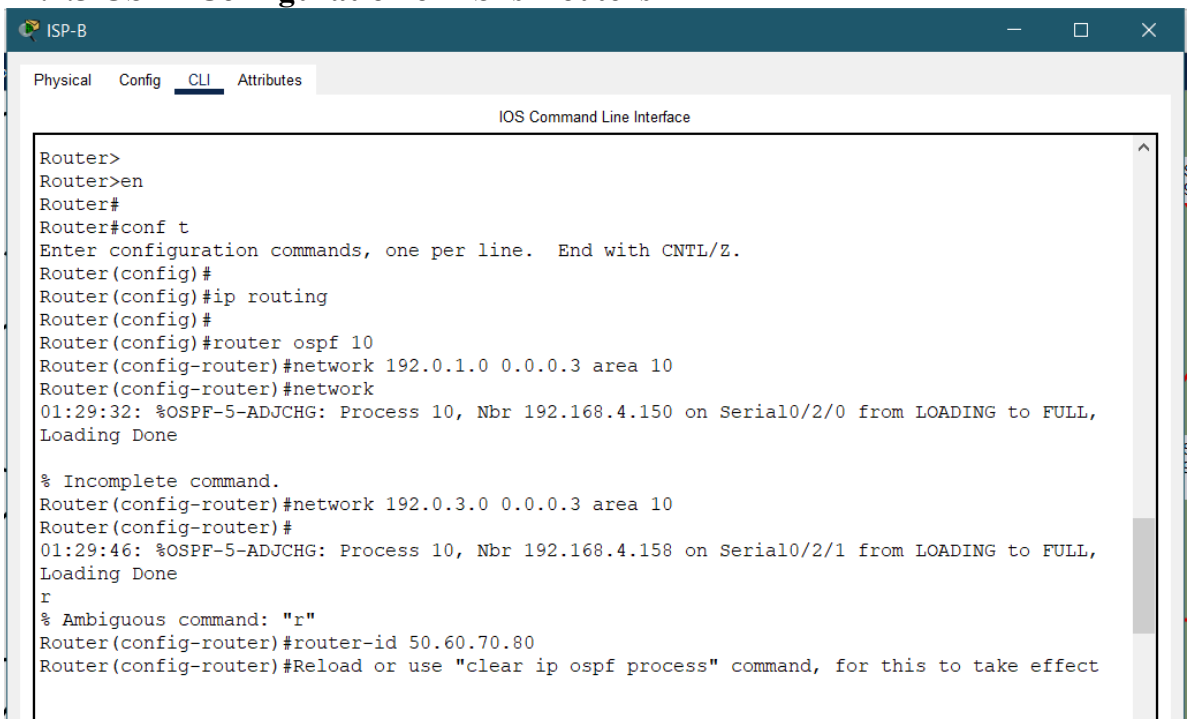
14.1.3 OSPF Configuration on Multilayer Switches



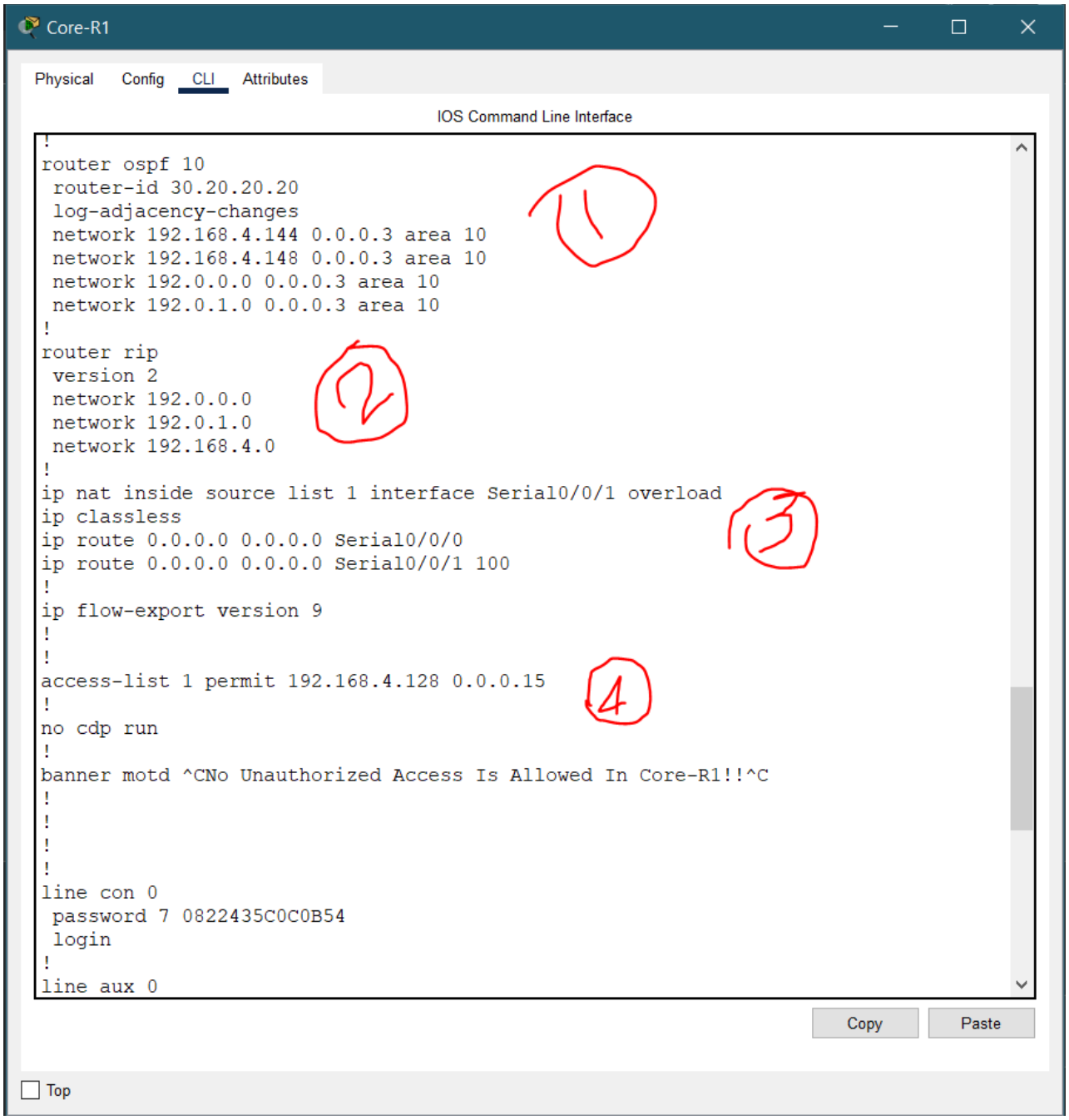
14.1.4 OSPF Configuration on Layer3 Routers



14.1.5 OSPF Configuration on ISPs Routers

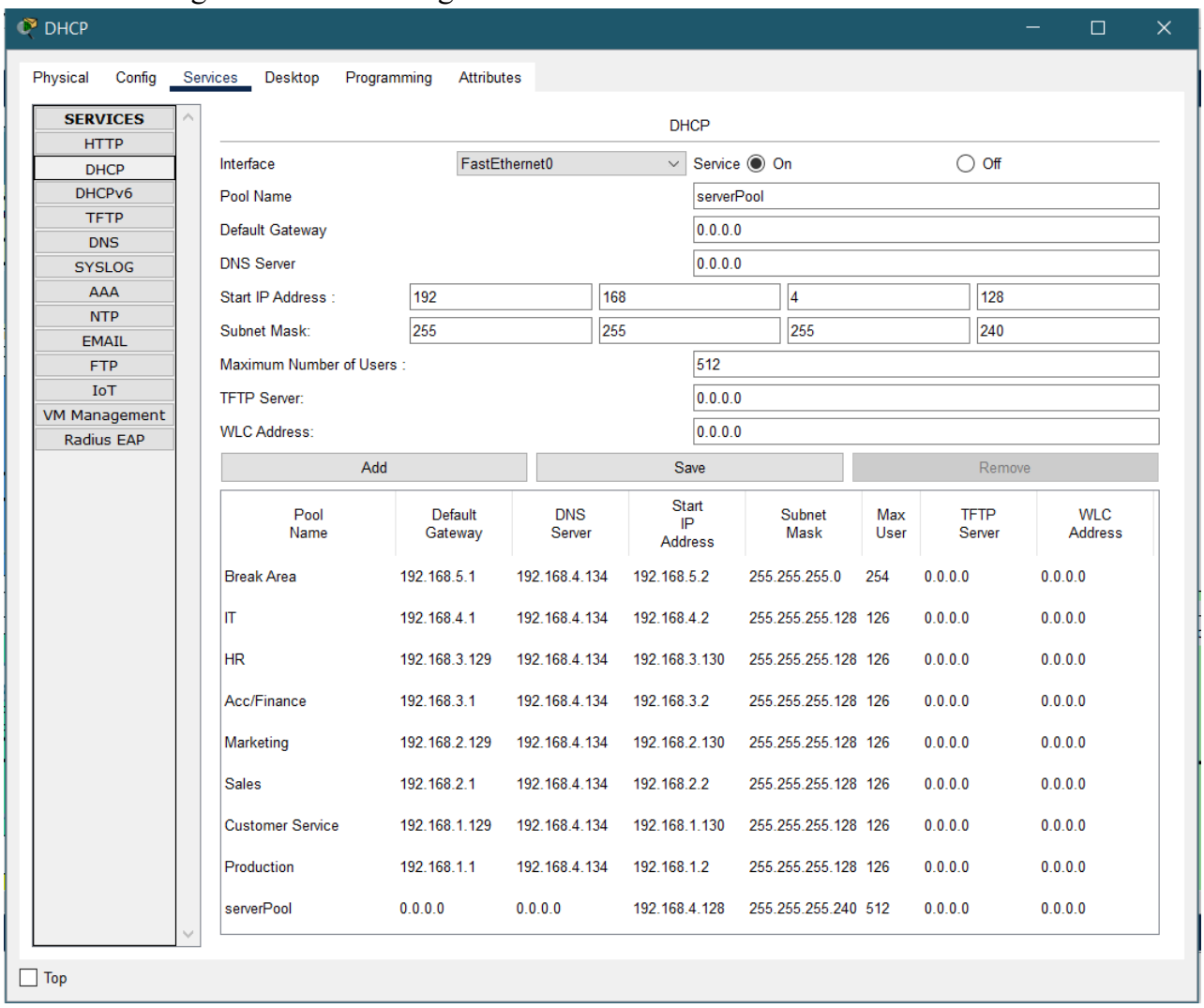


14.1.6 OSPF, NAT Overload, RIP, ACL Show Results



15.1 Servers Infrastructure and configuration

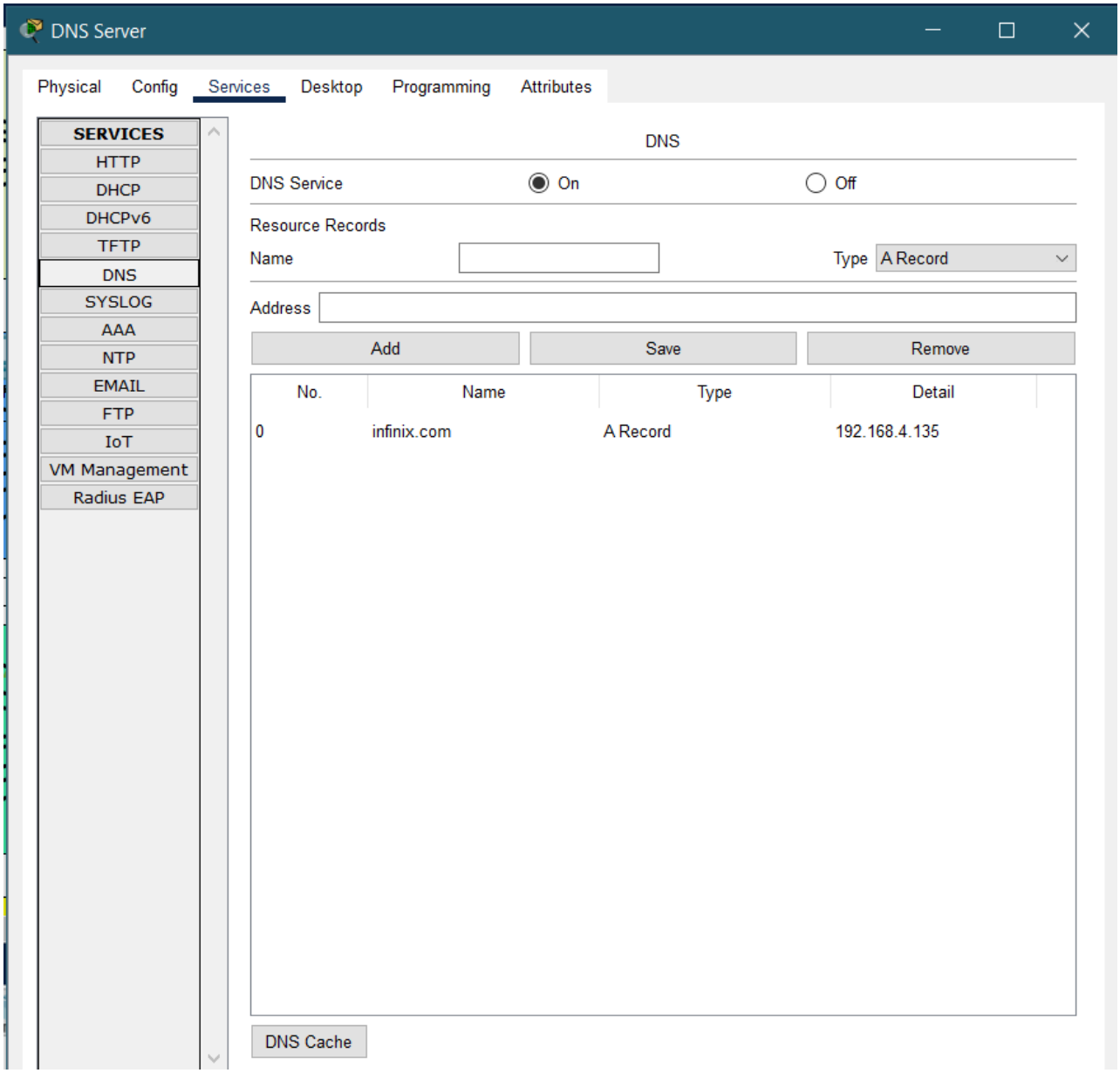
15.1.1 DHCP Server: is a network server that automatically assigns IP addresses and network configuration parameters to devices on a network. It dynamically manages the allocation of IP addresses and other network settings to clients, simplifying the process of network configuration and management.



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Break Area	192.168.5.1	192.168.4.134	192.168.5.2	255.255.255.0	254	0.0.0.0	0.0.0.0
IT	192.168.4.1	192.168.4.134	192.168.4.2	255.255.255.128	126	0.0.0.0	0.0.0.0
HR	192.168.3.129	192.168.4.134	192.168.3.130	255.255.255.128	126	0.0.0.0	0.0.0.0
Acc/Finance	192.168.3.1	192.168.4.134	192.168.3.2	255.255.255.128	126	0.0.0.0	0.0.0.0
Marketing	192.168.2.129	192.168.4.134	192.168.2.130	255.255.255.128	126	0.0.0.0	0.0.0.0
Sales	192.168.2.1	192.168.4.134	192.168.2.2	255.255.255.128	126	0.0.0.0	0.0.0.0
Customer Service	192.168.1.129	192.168.4.134	192.168.1.130	255.255.255.128	126	0.0.0.0	0.0.0.0
Production	192.168.1.1	192.168.4.134	192.168.1.2	255.255.255.128	126	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.4.128	255.255.255.240	512	0.0.0.0	0.0.0.0

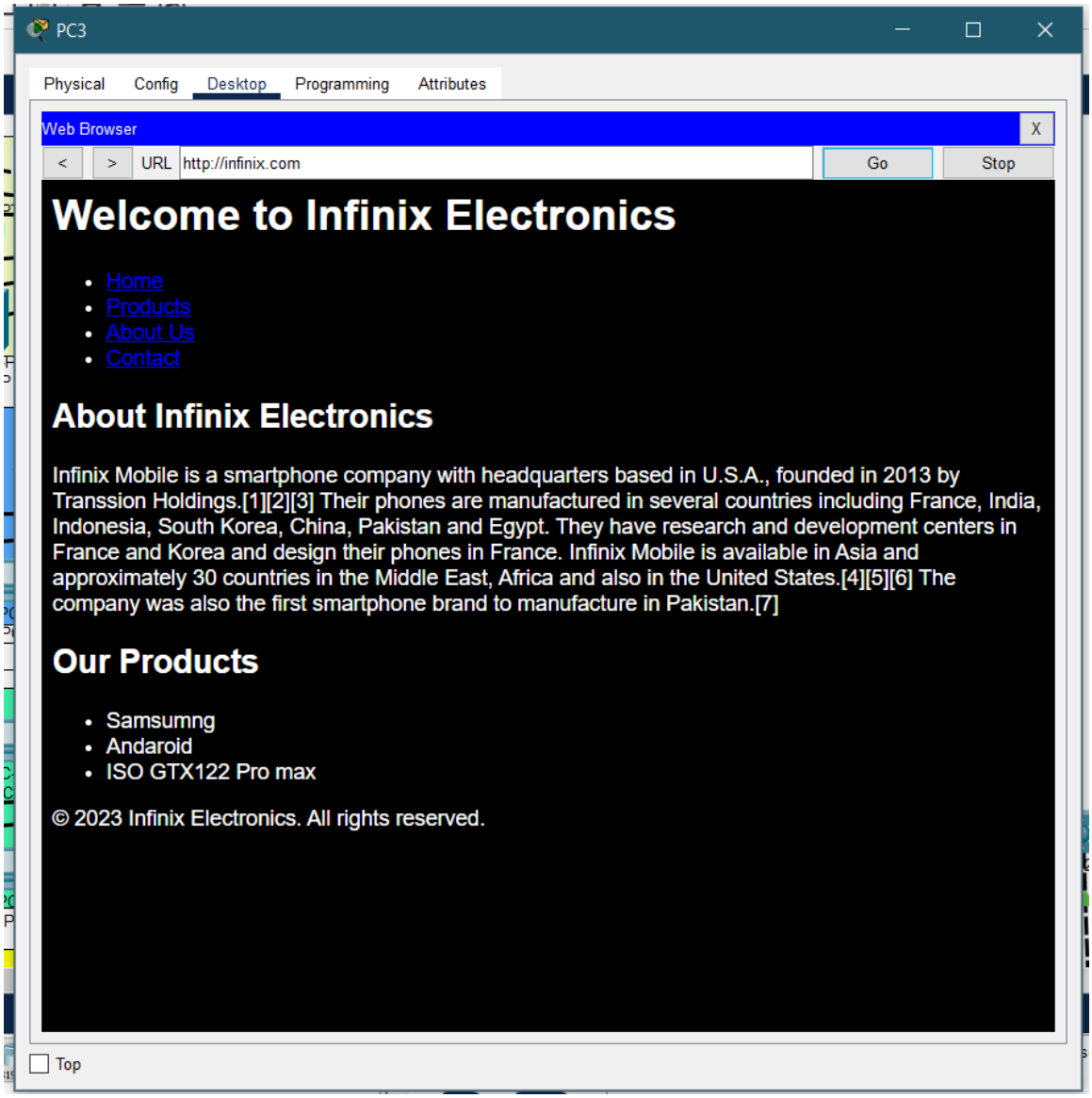
In the DHCP server, we accessed the DHCP server configuration and identified the subnets we wanted to create pools for, ensuring each subnet had a unique network address and subnet mask. We created a DHCP pool for each subnet, specifying the IP address range default gateway, DNS server, and other relevant options. We repeated this process for each subnet. We saved and applied the changes, and then tested the DHCP pools by connecting devices within the subnets to ensure proper IP address assignment. We referred to the documentation or resources specific to our DHCP server software for detailed instructions. For the IP addresses of the DHCP server, we assigned it statically.

15.1.2 DNS Server: is a network server that translates domain names into their corresponding IP addresses. It acts as a directory service that allows users to access websites, send emails, or use other internet services by using easy-to-remember domain names instead of numeric IP addresses.



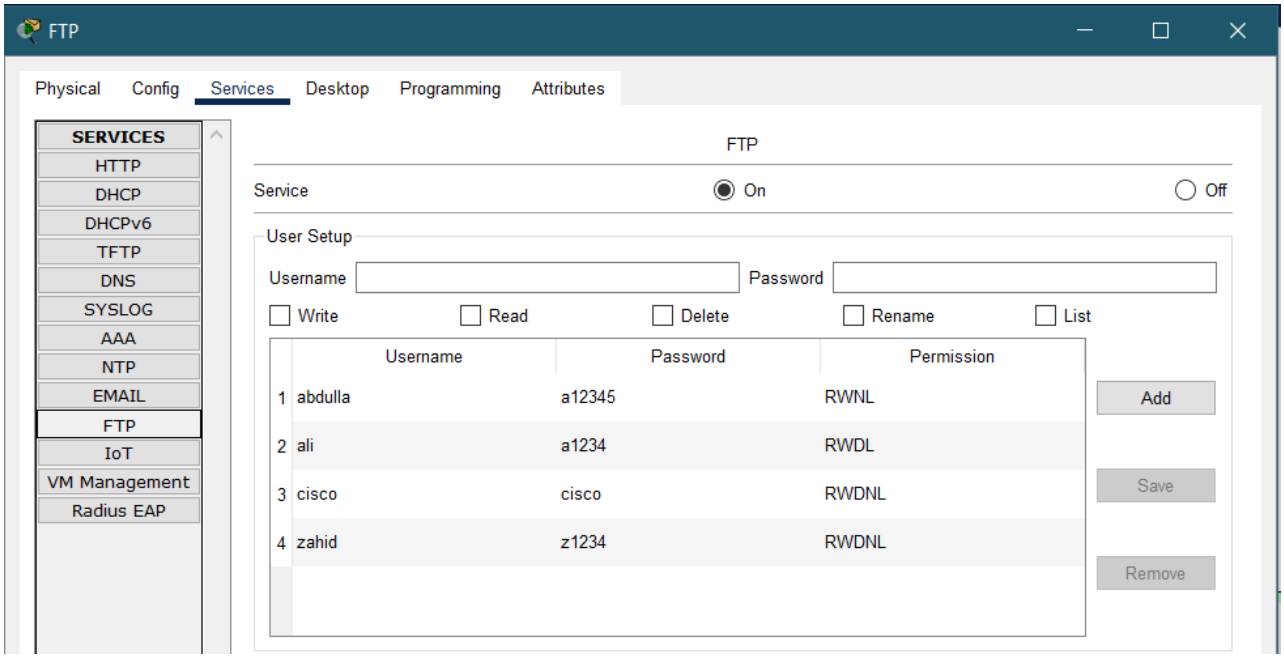
In the DNS server, we added the IP address of the web server of Infinix company. We did this to enable DNS resolution and allow clients to access the website hosted on the Infinix web server using its domain name. By associating the IP address with the domain name in the DNS server, we ensured that when users entered the Infinix website's domain name in their web browsers, the DNS server would provide the corresponding IP address, allowing the browser to establish a connection to the correct web server and retrieve the website's content.

15.1.3 Web Server is a software application that runs on a computer and serves web pages and other web content to clients upon request. It is a fundamental component of the World Wide Web, allowing websites and web applications to be accessible to users over the Internet.

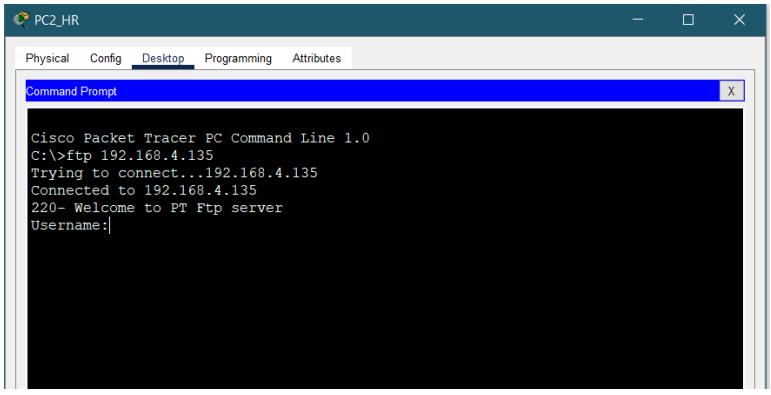


Here is the output of the web server.

15.1.4 FTP Server: is a type of server software that facilitates the transfer of files between computers over a network. It enables users to upload, download, and manage files on a remote server using the FTP protocol.

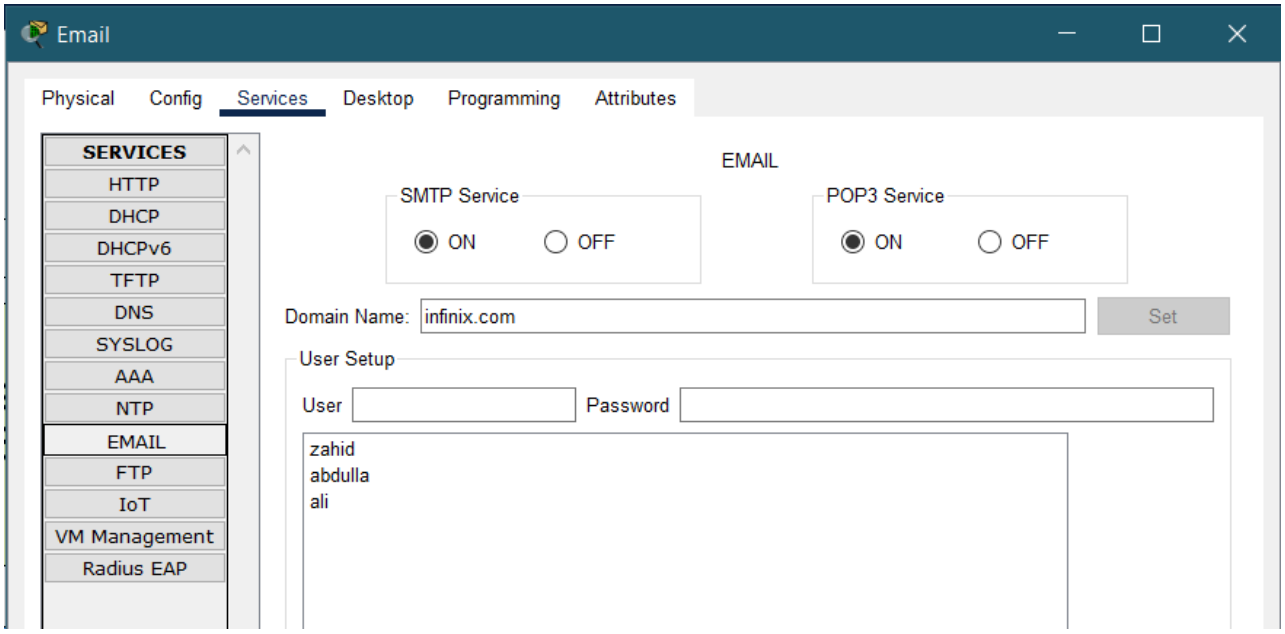


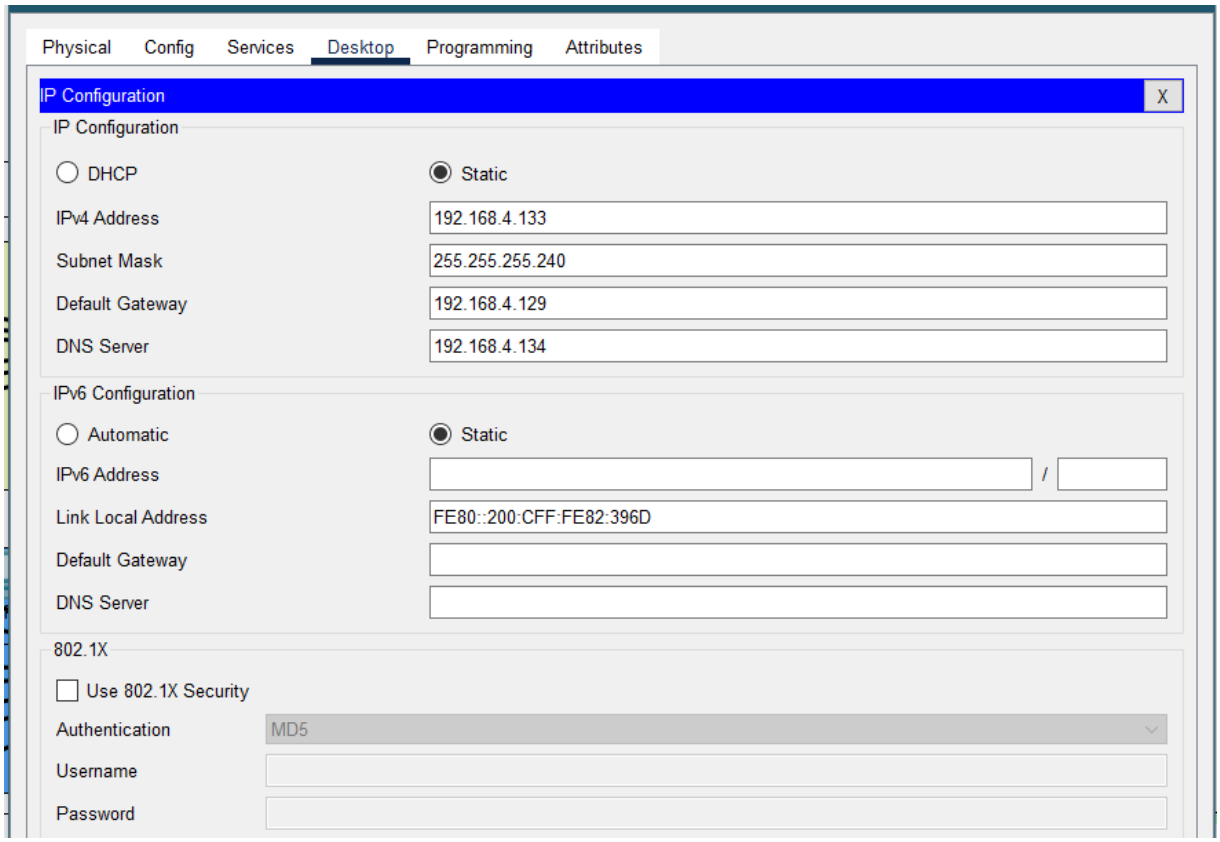
We added users to the FTP server and assigned specific permissions to them for security and access control purposes. By adding users and configuring permissions, we ensured that only authorized individuals or entities could access and interact with the files and directories stored on the FTP server.



This figure shows that the FTP server is accessible

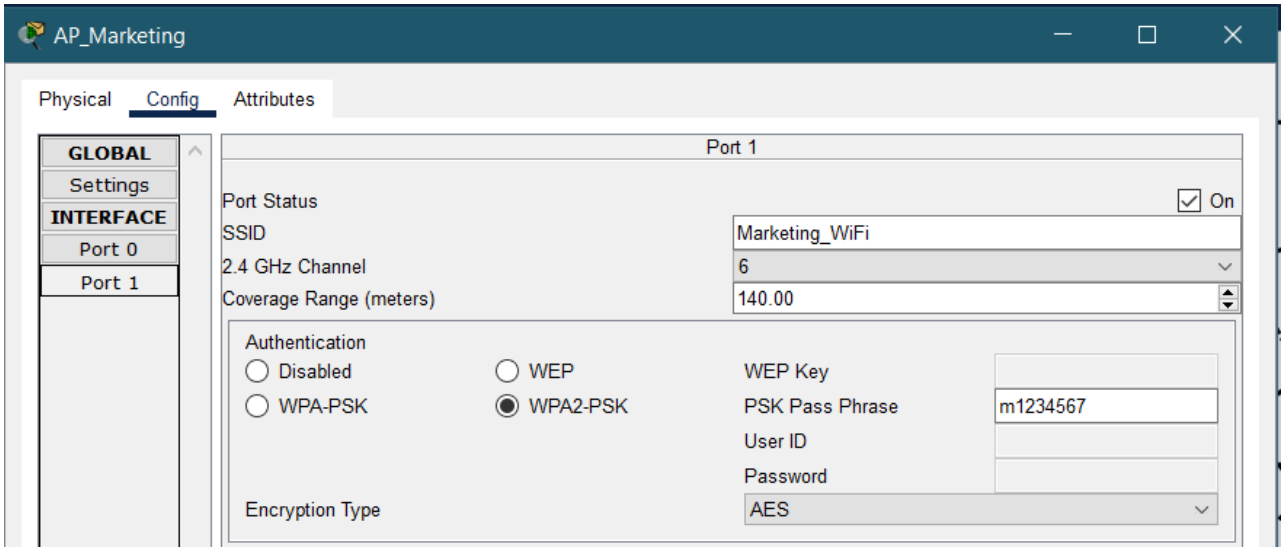
15.1.5 Email Server: is a server computer or software application that handles the sending, receiving, storage, and routing of email messages. It provides the infrastructure and protocols necessary for email communication within a network or across the internet.



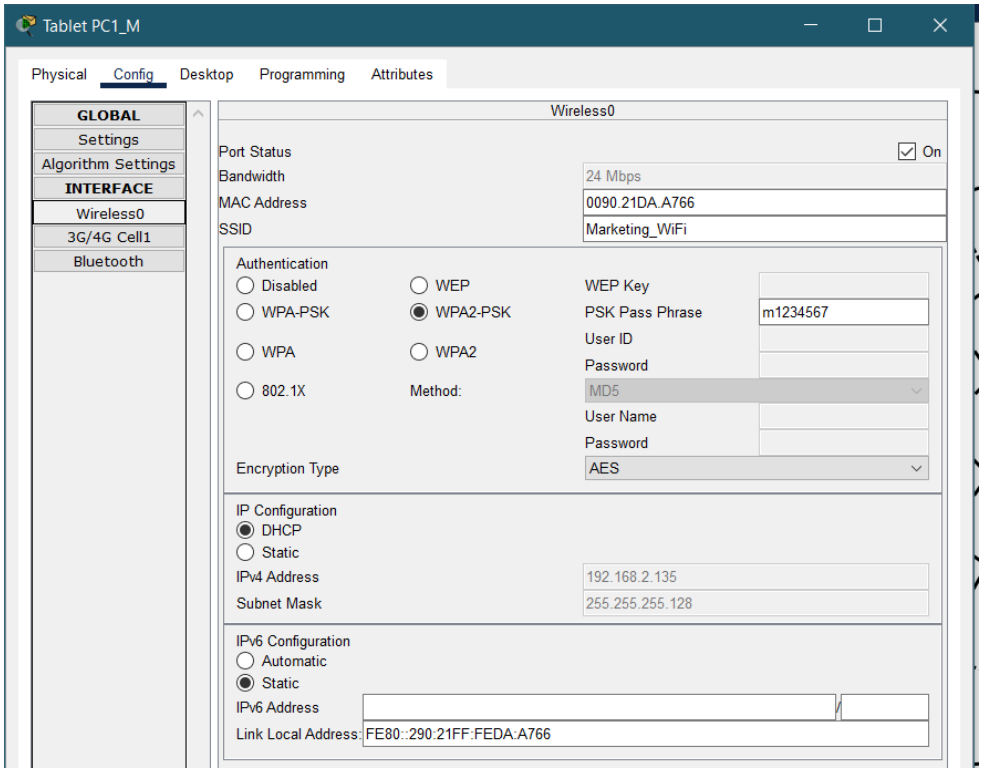


16.1 Wireless Configuration

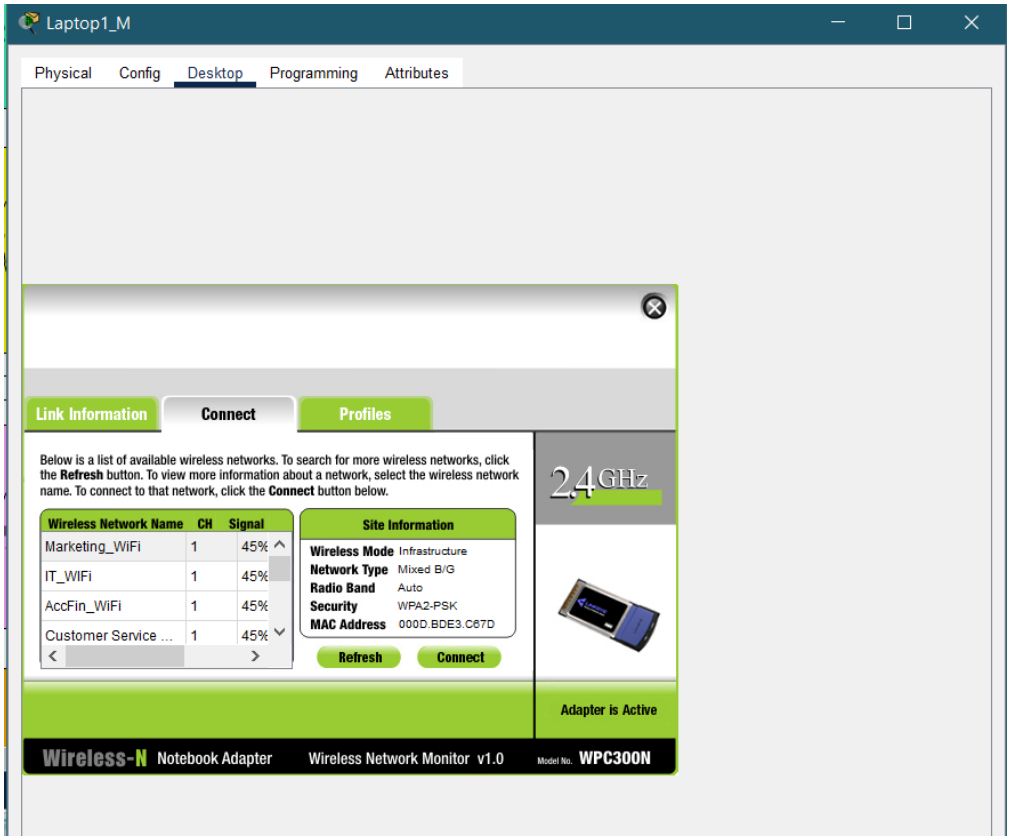
AP is a network device that allows wireless devices, such as laptops, smartphones, and tablets, to connect to a wired network and access network resources and services without requiring a physical connection.



For each AP in every subnet, we added an access point and configure its SSID (name) and setup password for authentication.

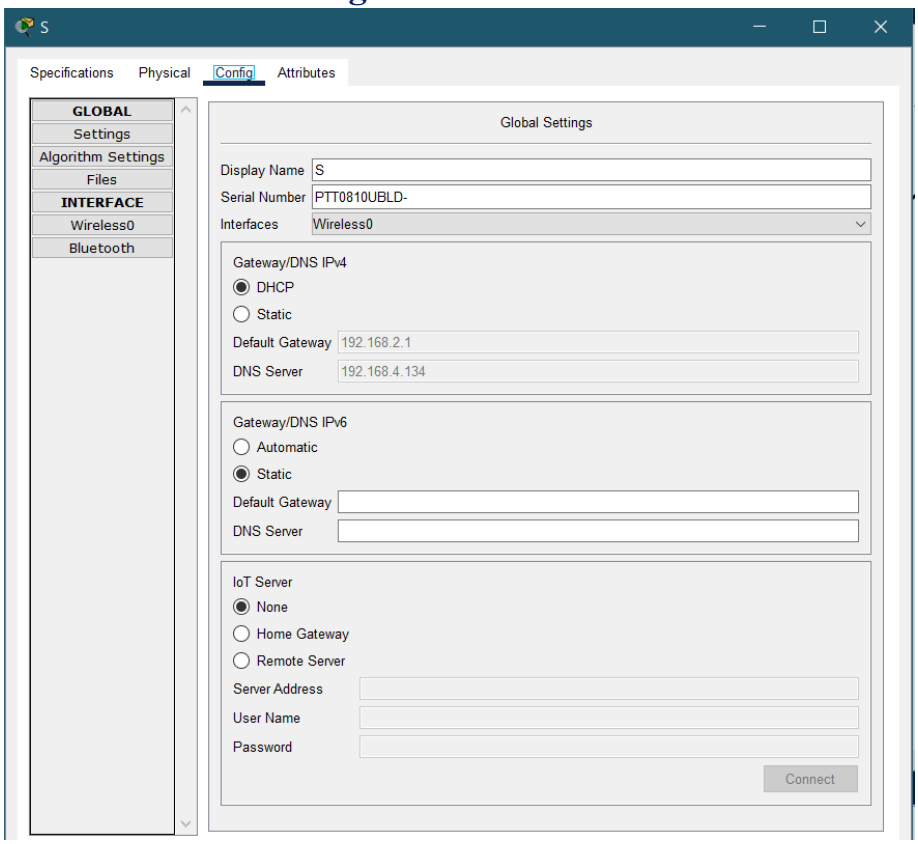


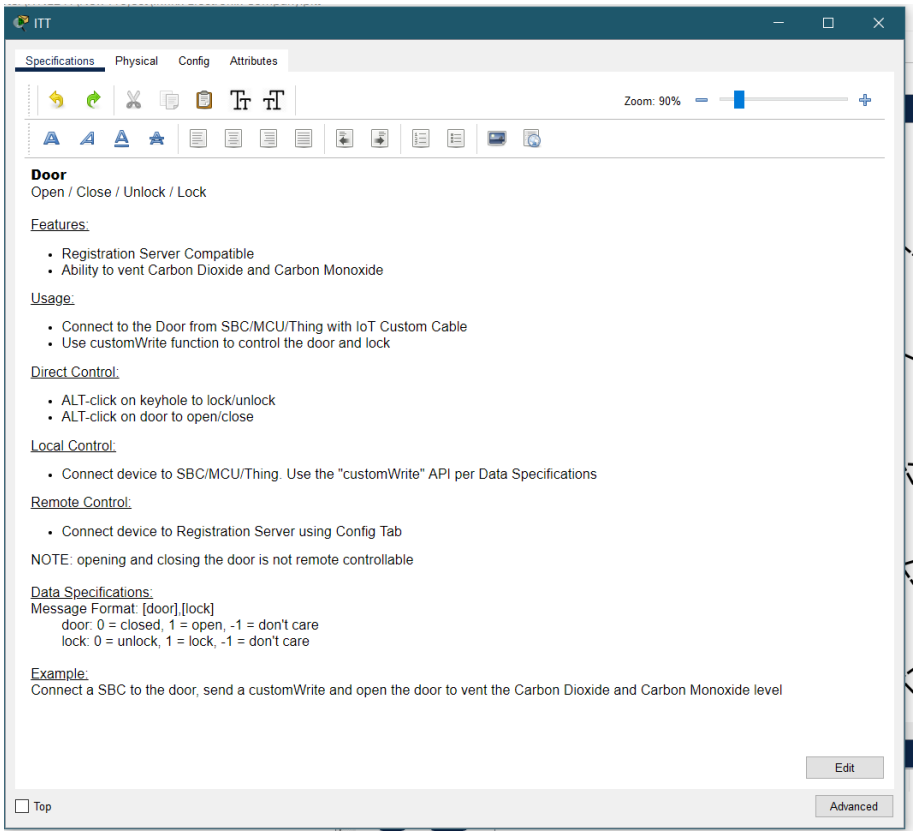
Here is a wireless host that is connected to the access point.



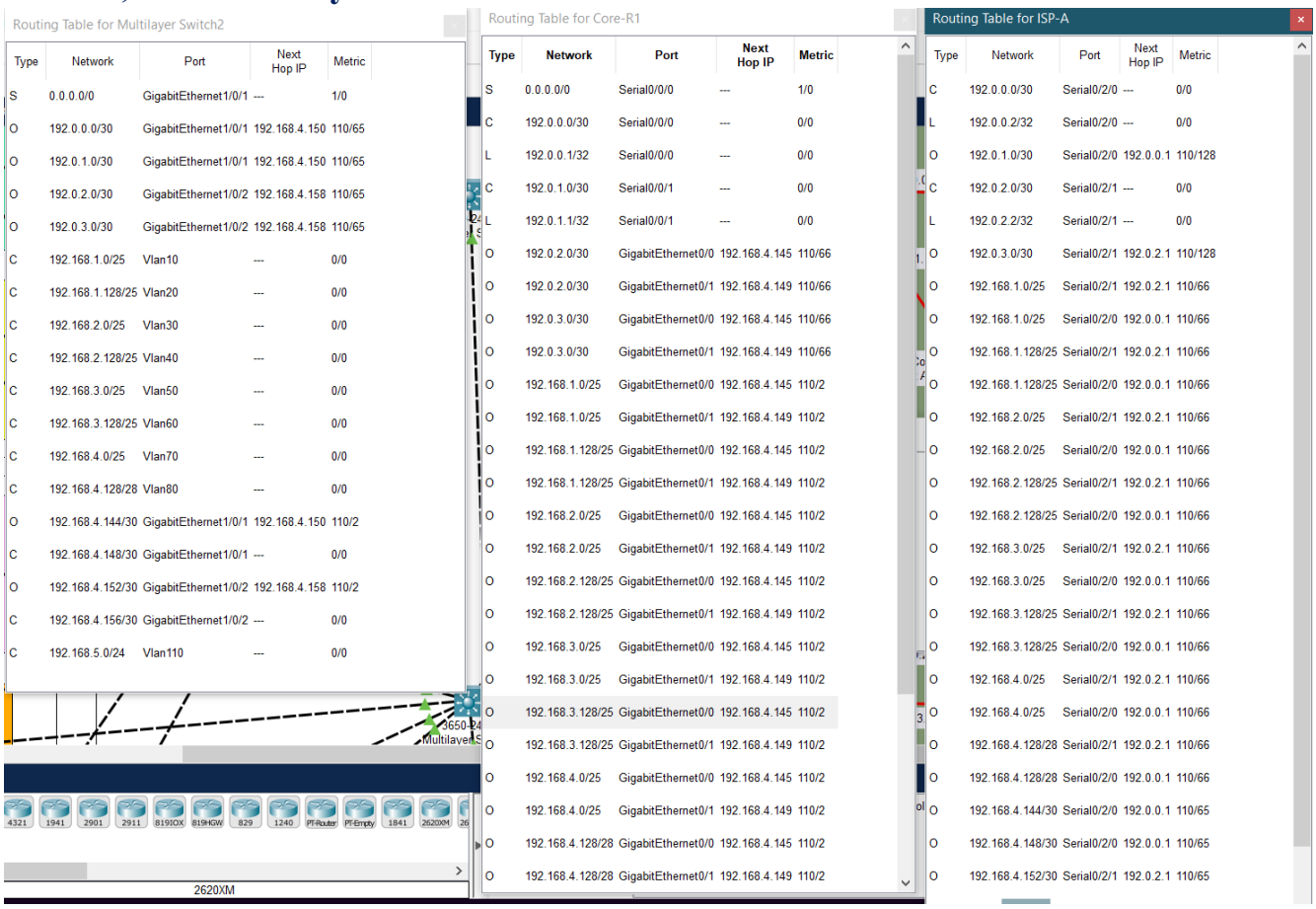
Here is a laptop that shows the wireless networks that are available.

17.1 IOT Door Configuration





18.1 Routing Tables for the core routers, ISP routers, and multilayer switches



Routing Table for Multilayer Switch2

Type	Network	Port	Next Hop IP	Metric
S	0.0.0.0/0	GigabitEthernet1/0/1	---	1/0
O	192.0.0.0/30	GigabitEthernet1/0/1	192.168.4.150	110/65
O	192.0.1.0/30	GigabitEthernet1/0/1	192.168.4.150	110/65
O	192.0.2.0/30	GigabitEthernet1/0/2	192.168.4.158	110/65
O	192.0.3.0/30	GigabitEthernet1/0/2	192.168.4.158	110/65
C	192.168.1.0/25	Vlan10	---	0/0
C	192.168.1.128/25	Vlan20	---	0/0
C	192.168.2.0/25	Vlan30	---	0/0
C	192.168.2.128/25	Vlan40	---	0/0
C	192.168.3.0/25	Vlan50	---	0/0
C	192.168.3.128/25	Vlan60	---	0/0
C	192.168.4.0/25	Vlan70	---	0/0
C	192.168.4.128/28	Vlan80	---	0/0
O	192.168.4.144/30	GigabitEthernet1/0/1	192.168.4.150	110/2
C	192.168.4.148/30	GigabitEthernet1/0/1	---	0/0
O	192.168.4.152/30	GigabitEthernet1/0/2	192.168.4.158	110/2
C	192.168.4.156/30	GigabitEthernet1/0/2	---	0/0
C	192.168.5.0/24	Vlan110	---	0/0

Routing Table for Core-R1

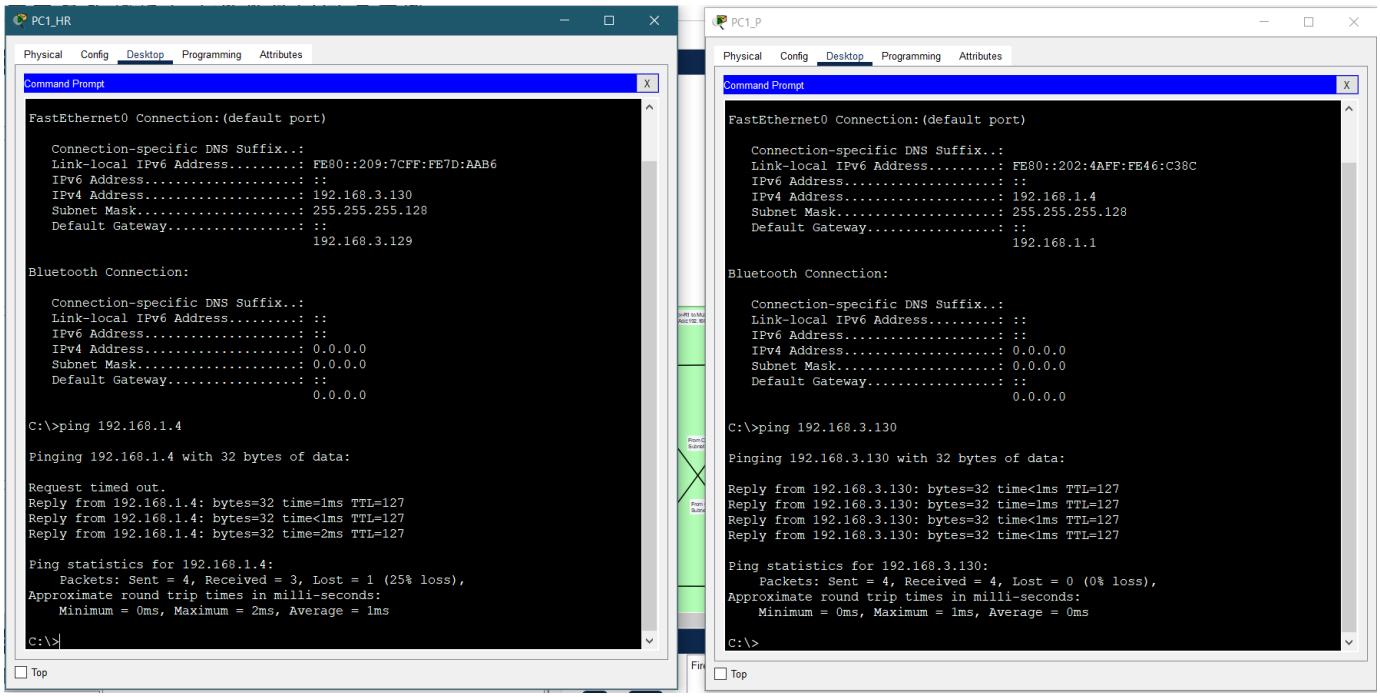
Type	Network	Port	Next Hop IP	Metric
S	0.0.0.0/0	Serial0/0/0	---	1/0
C	192.0.0.0/30	Serial0/0/0	---	0/0
L	192.0.0.1/32	Serial0/0/0	---	0/0
C	192.0.1.0/30	Serial0/0/1	---	0/0
L	192.0.1.1/32	Serial0/0/1	---	0/0
O	192.0.2.0/30	GigabitEthernet0/0	192.168.4.145	110/66
O	192.0.2.0/30	GigabitEthernet0/1	192.168.4.149	110/66
O	192.0.3.0/30	GigabitEthernet0/0	192.168.4.145	110/66
O	192.0.3.0/30	GigabitEthernet0/1	192.168.4.149	110/66
O	192.168.1.0/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.1.0/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.1.128/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.1.128/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.2.0/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.2.0/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.2.128/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.2.128/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.3.0/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.3.0/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.3.128/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.3.128/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.4.0/25	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.4.0/25	GigabitEthernet0/1	192.168.4.149	110/2
O	192.168.4.128/28	GigabitEthernet0/0	192.168.4.145	110/2
O	192.168.4.128/28	GigabitEthernet0/1	192.168.4.149	110/2

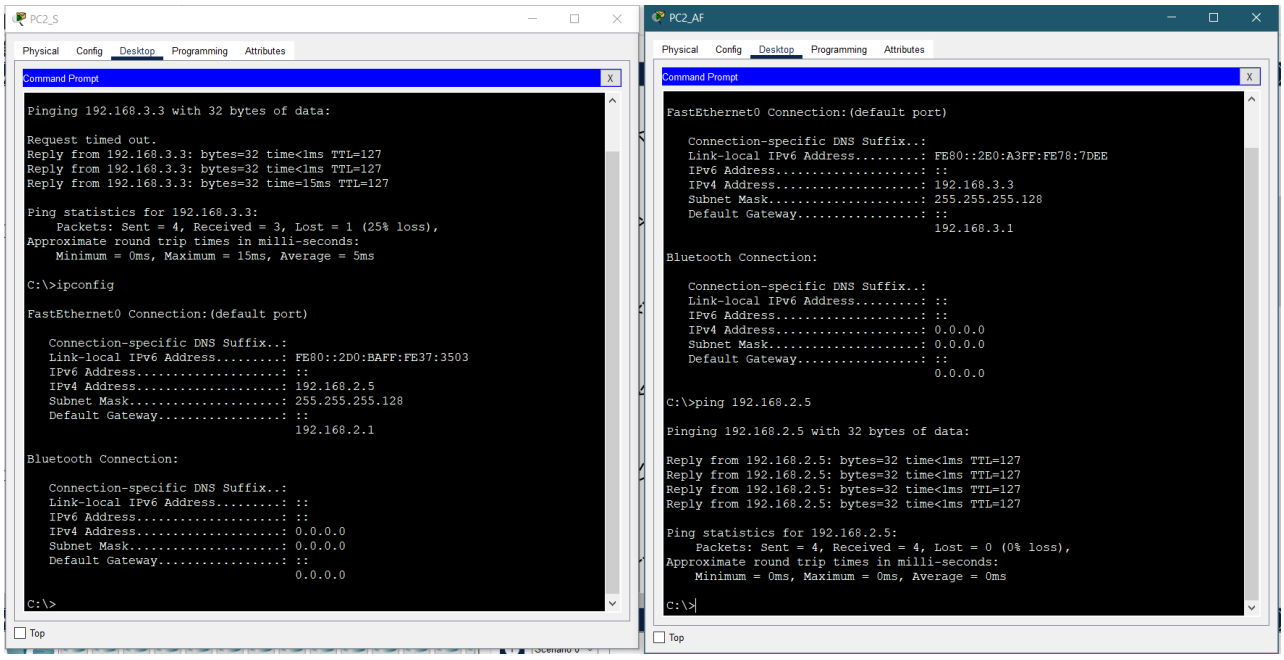
Routing Table for ISP-A

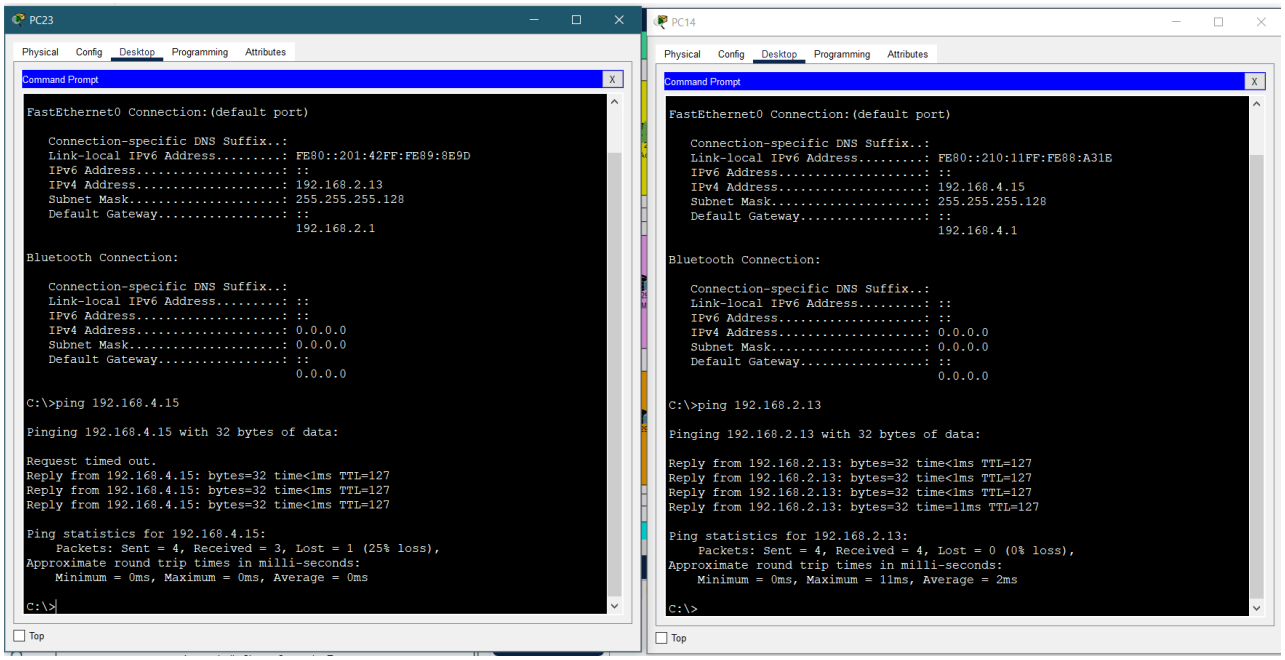
Type	Network	Port	Next Hop IP	Metric
C	192.0.0.0/30	Serial0/2/0	---	0/0
L	192.0.0.2/32	Serial0/2/0	---	0/0
O	192.0.1.0/30	Serial0/2/0	192.0.0.1	110/128
C	192.0.2.0/30	Serial0/2/1	---	0/0
L	192.0.2.2/32	Serial0/2/1	---	0/0
O	192.0.3.0/30	Serial0/2/1	192.0.2.1	110/128
O	192.168.1.0/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.1.0/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.1.128/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.1.128/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.2.0/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.2.0/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.2.128/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.2.128/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.3.0/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.3.0/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.3.128/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.3.128/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.4.0/25	Serial0/2/1	192.0.2.1	110/66
O	192.168.4.0/25	Serial0/2/0	192.0.0.1	110/66
O	192.168.4.128/28	Serial0/2/1	192.0.2.1	110/66
O	192.168.4.128/28	Serial0/2/0	192.0.0.1	110/66
O	192.168.4.144/30	Serial0/2/0	192.0.0.1	110/65
O	192.168.4.148/30	Serial0/2/0	192.0.0.1	110/65
O	192.168.4.152/30	Serial0/2/1	192.0.2.1	110/65

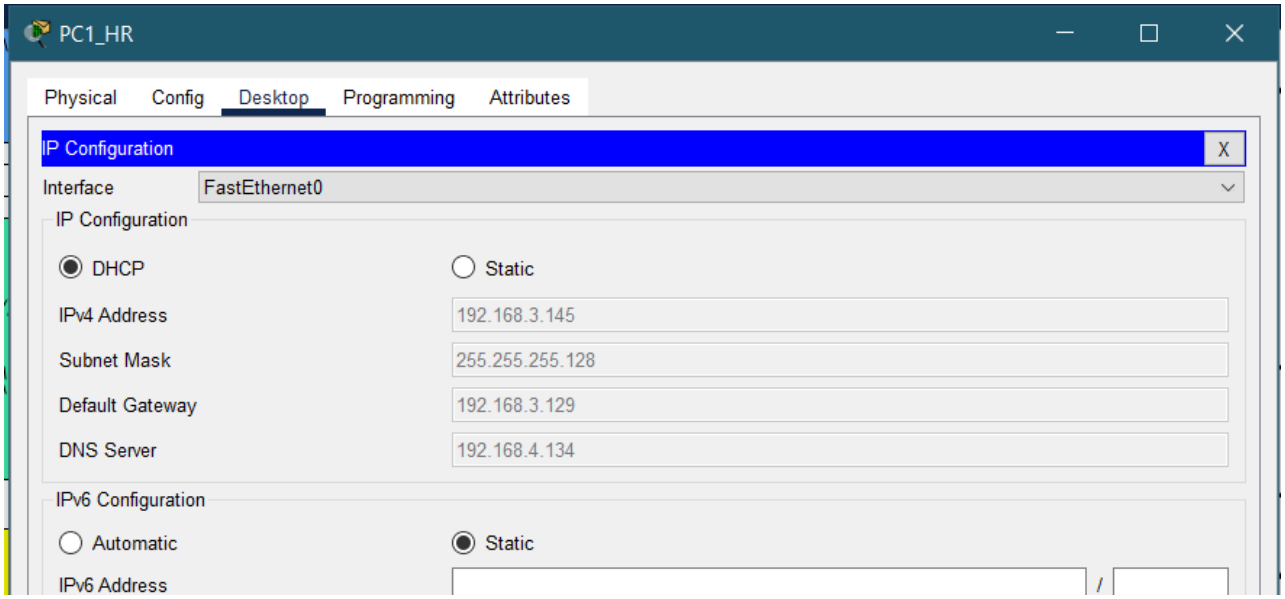
Letter "o" specify the OSPF routing.

19.1 Testing and verifying the connectivity









As shown in this figure, the DHCP server is **enabled.**

20.1 Conclusion

In conclusion, we have designed a comprehensive network for Infinix Electronics, a global mobile electronics company, using Cisco Packet Tracer simulation software. The network encompasses four floors and incorporates various components such as routers, switches, servers, and wireless access points. Our goal was to create an efficient and secure network that meets the company's requirements for high performance, reliability, scalability, and simplified troubleshooting.

Throughout the project, we implemented VLANs, IP routing, DHCP, inter-VLAN configuration, and NAT overload for efficient address utilization. We also configured OSPF as the routing protocol for route advertisement and SSH for secure remote login. By assigning dedicated DHCP servers and implementing proper subnetting and IP addressing, we ensured effective address allocation and management.

To enhance security, we assigned password authentication for each wireless access point, enabling better control and management of the organization's wireless network. Additionally, we implemented ACLs (Access Control Lists) to control network traffic and protect against unauthorized access.

We paid particular attention to fault tolerance by incorporating redundant connections at every layer, ensuring network stability and continuity. Proper cabling and device settings were implemented for optimal performance and connectivity.

Overall, our network design and configuration in Cisco Packet Tracer met the project objectives, providing Infinix Electronics with a robust and secure network infrastructure that supports seamless communication and data transfer between departments.