Edge Hill University

The Department of Computer Science

CIS2706 Computer Networks

Coursework 1- Portfolio Tasks

2024/2025

Thomas Mason 26040247

Table of Contents

Guidelines:

1. All the explanation should be with proper references in Harvard Style.
2. The figures/tables should be captioned and embedded in the text.
3. The text should be justified and not left aligned and in the same font.
4. The structure of the report should be professional as in the template.

Part I: Portfolio

1. Introduction

- This section should be written after all the activities are complete
- Introduce the contents covered in this module and in the portfolio.
- Reflect on your learning and provide some concluding analysis on the portfolio.
- Do not exceed 1 page.

(Please follow the instructions of each lab to write up the lab reports.)

<u>You are not expected to write the manual again, just answer the questions and present the results with evidence of screenshots and discussion.</u>

This report covers the contents of Lab Reports 1-5, which include packet sniffing using Wireshark, setting up a router with Cisco Packet Tracer, setting up IP address ranges with different subnets using Cisco Packet Tracer, setting up various types of applications using Cisco Packet Tracer and information on network security. In this assignment, the new things I learnt were how to calculate and set different subnets in Report 3, and I also learned in Report 4 how to set up various applications in Cisco packet tracer. Overall, these labs taught me more fundamentals of Cisco Packet Tracer, and I now have a much deeper understanding of the software.

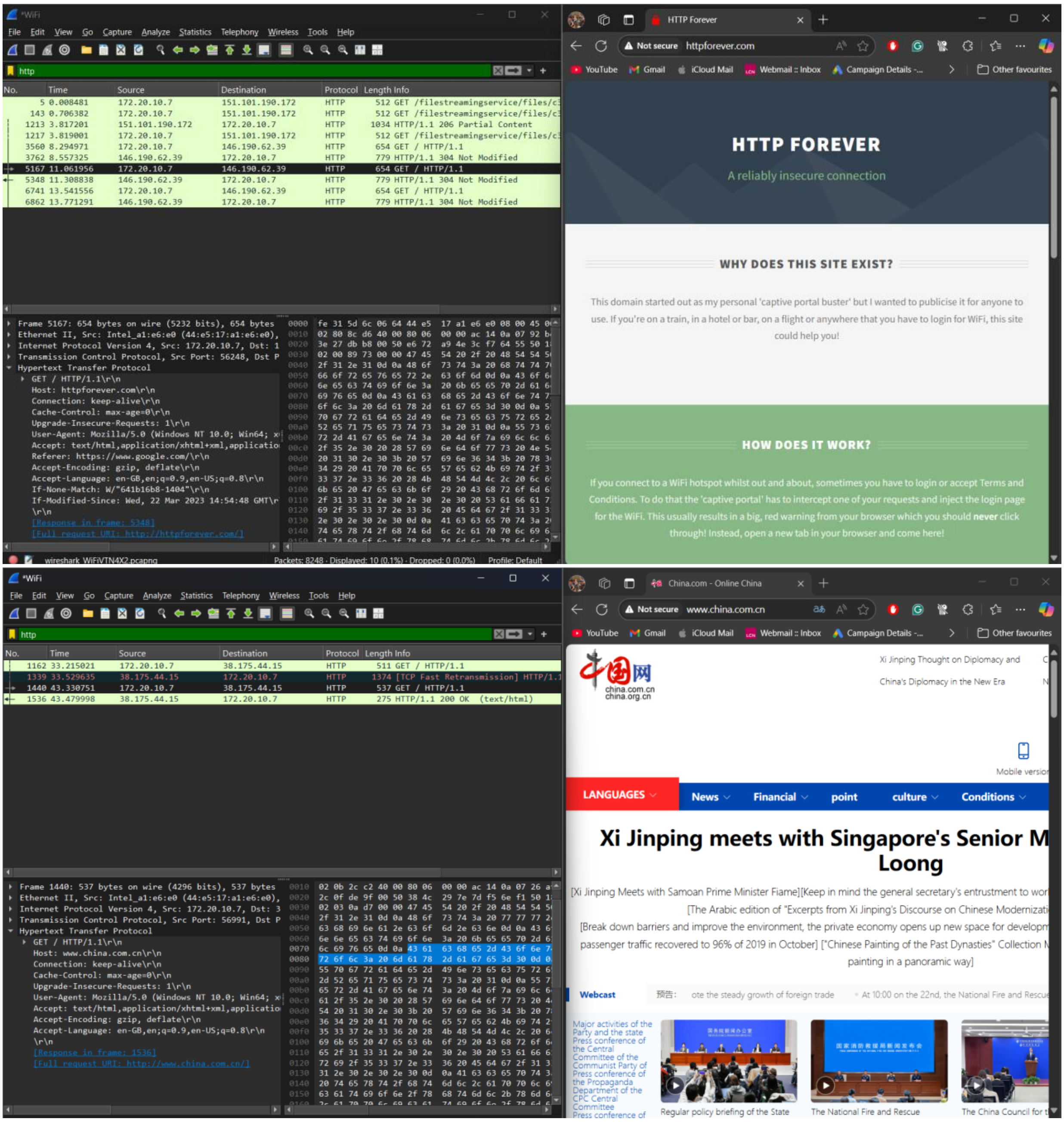
2. Lab Reports 1: Packet Sniffing Using Wireshark

2.1. Introduction

In this lab, I will be using Wireshark to examine network traffic using capture trace, justify three network protocols, and describe the IP header field.

2.2. Answers to Questions

1. Capture trace for two different websites of your choice.



2. List at least 3 different protocols that appear in the protocol column in the unfiltered packet-listing window. (Explain each protocol briefly).

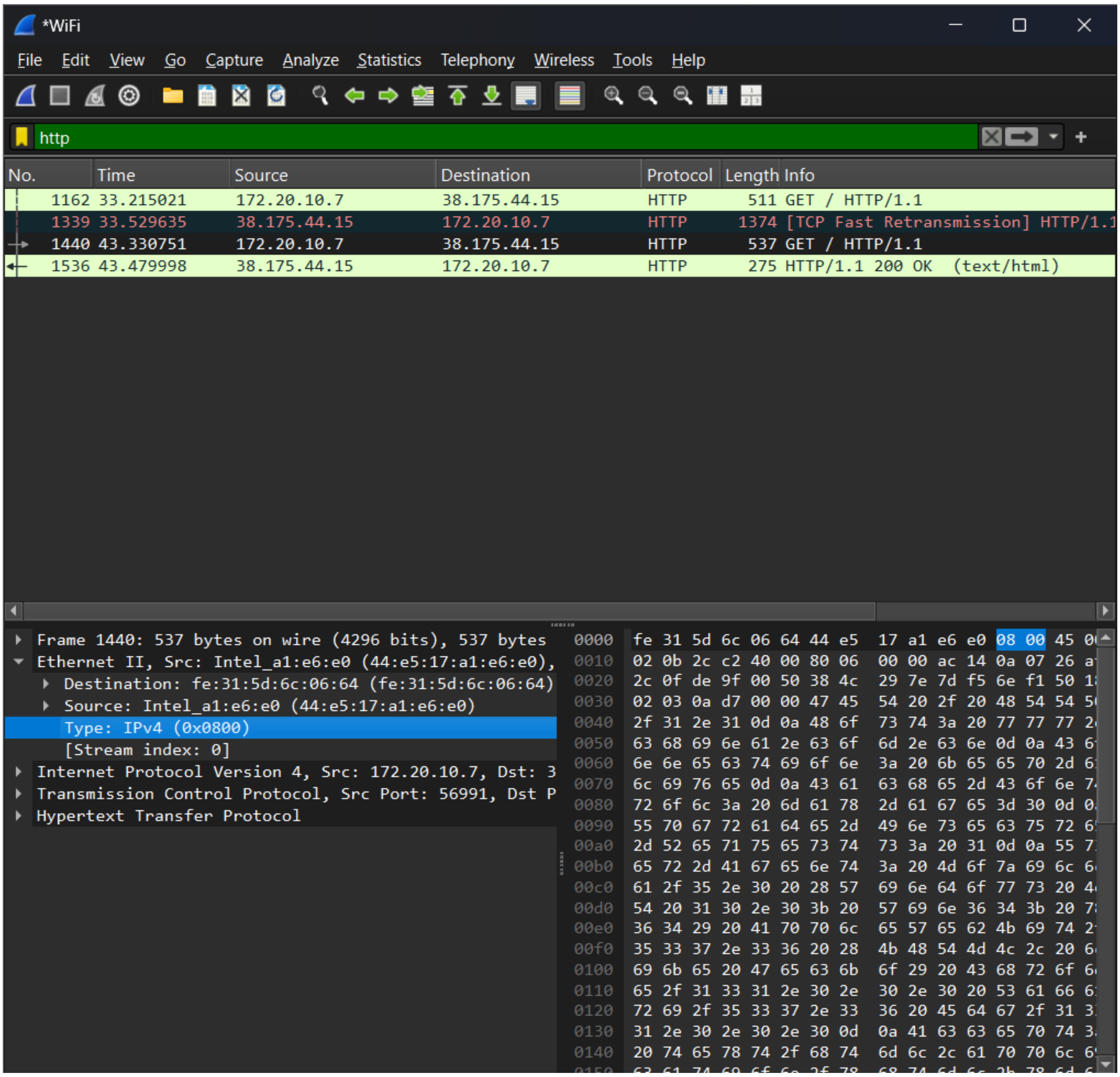
Transport Layer Security: TLS is a cryptographic protocol that was developed initially from SSL. TLS provides end-to-end security for the transfer of data over the Internet. It can be used

for applications such as e-mail, file transfers, video calling, messaging and voice-over-IP, as well as services such as DNS and NTP (Internet Society, 2015).
Transmission control protocol: TCP is a protocol that is used for the transmission of data between devices on a network. It creates and maintains network connections and ensures the data is delivered in sequence, which allows applications to exchange data reliably. (Yasar, 2024).

Hypertext Transfer Protocol: HTTP is a protocol that operates on top of the TCP and IP stack and is used to transfer files over the internet; this could be text images or videos. It is the foundation of the World Wide Web and allows browsers and servers to communicate together. (Chai, 2021).

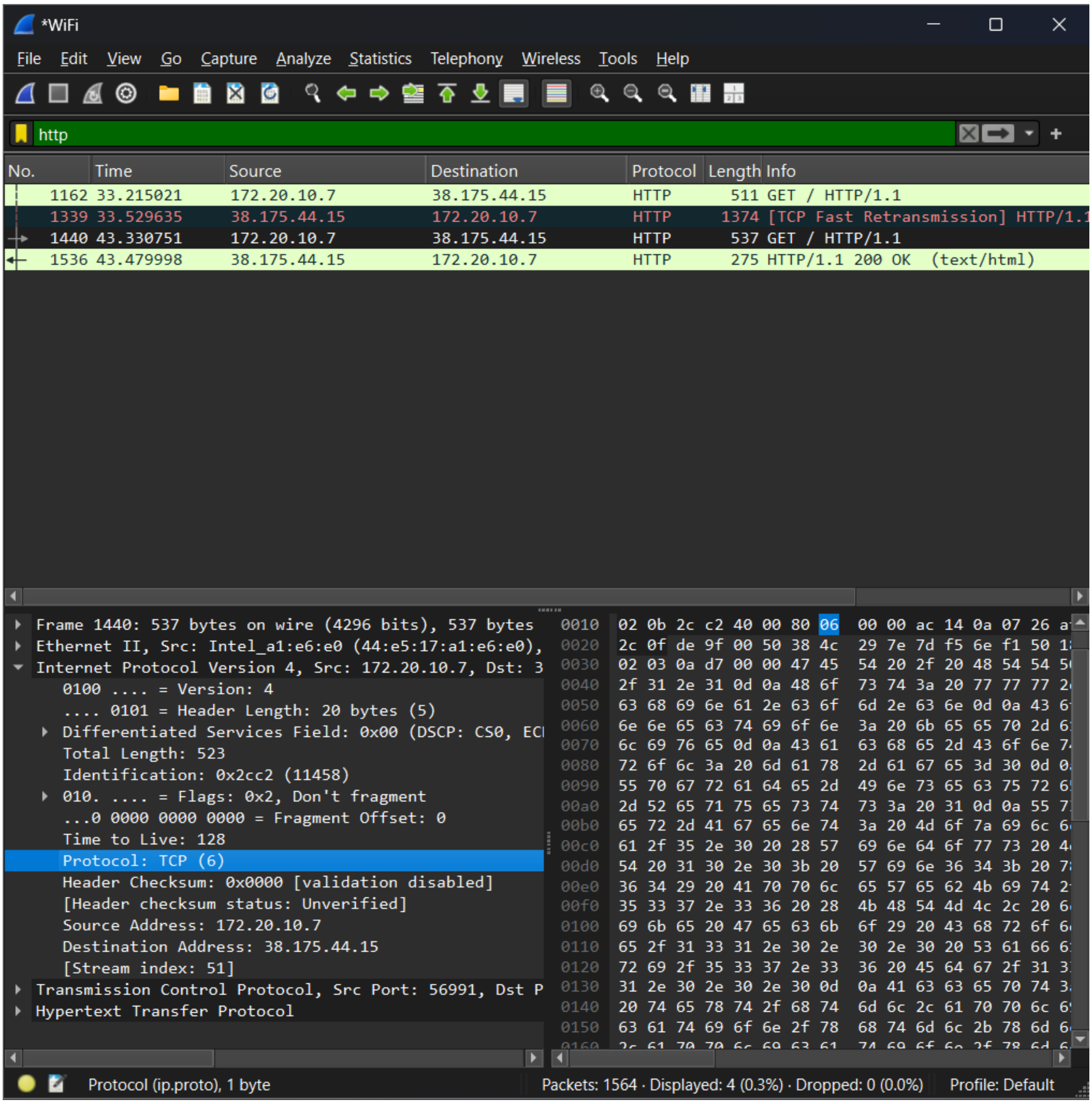
3. Which bytes in the Ethernet header field tell that the next higher layer protocol is IP? What is the hexadecimal value of this field?

In the ethernet frame, the Ethernet Type field indicates the next higher layer protocol. The hexadecimal value for this field is 0x0800.



4. Which bytes in the IP header field tell that the next higher layer protocol is TCP? What is the hexadecimal value of this field?

   The protocol field is the 9th byte, and in hexadecimal, it represents 0x06, which indicates the following higher-layer protocol field.



Each lab report should start from new page.

3. Lab Reports 2: Routers

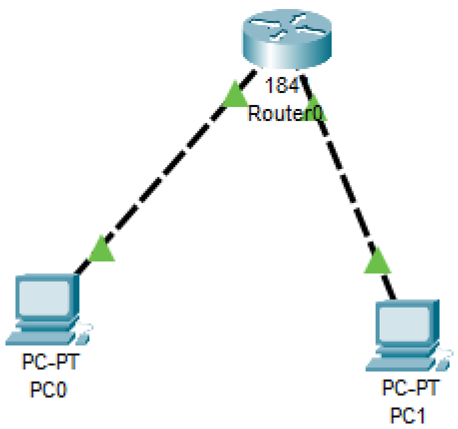
3.1. Introduction

In lab report 2, for part 1, I set up a basic router, connecting it with two PCs, then connecting them with the same default gateway as the router and added a subnet mask and IPv4, then tested them with a ping test, and documenting my steps and setup below. For the second part, using a similar process, I set up two routers and three switches with a PC at both ends and tested the ping between both networks.

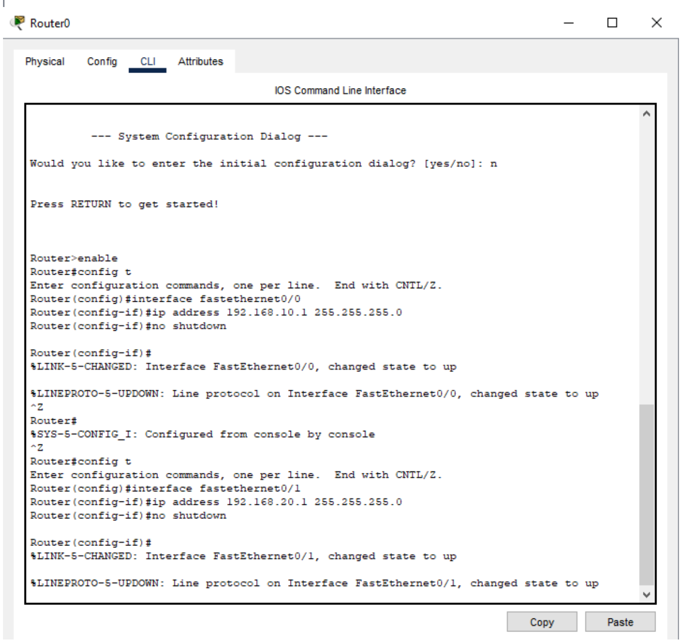
3.2. Answers to Questions

1. Ping: Verify Connectivity

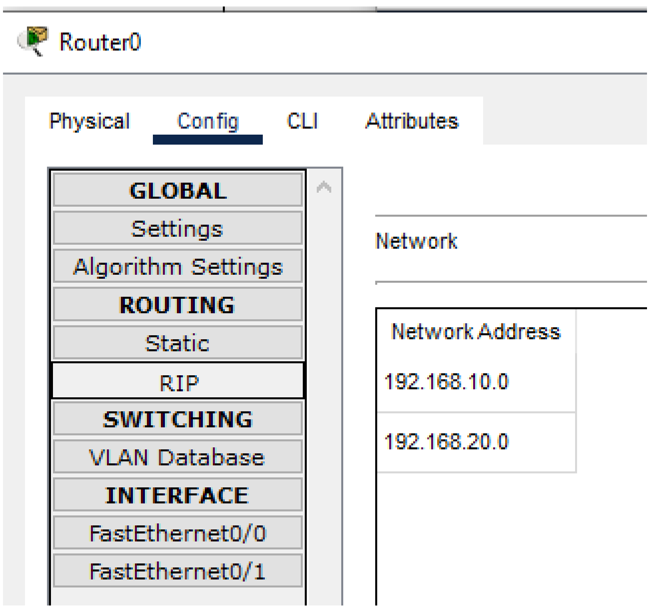
Part 1:

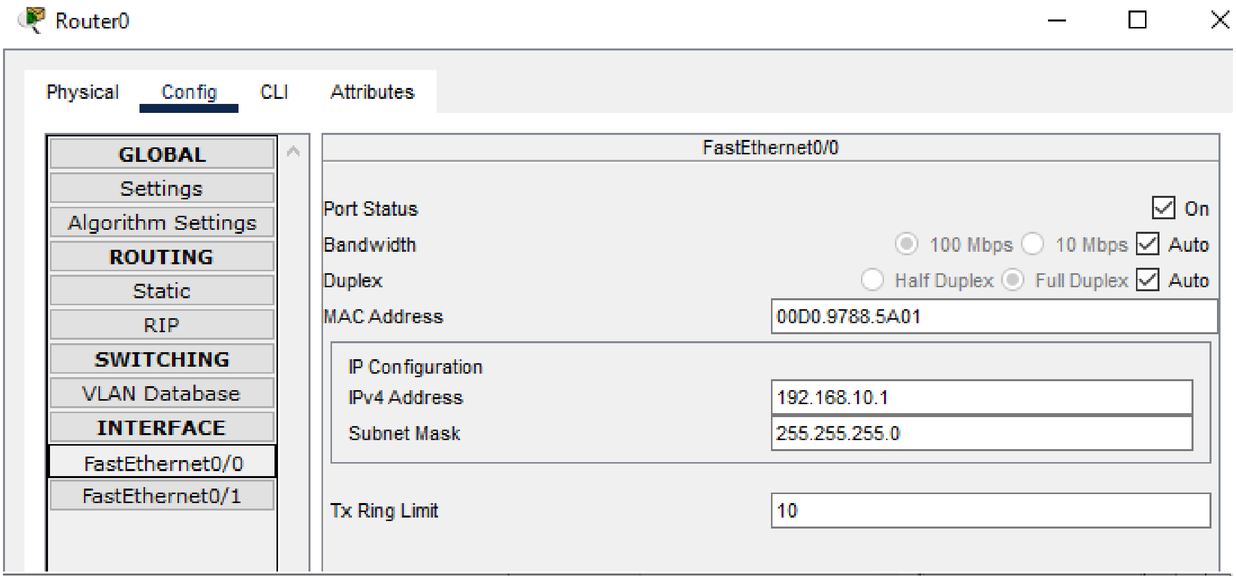


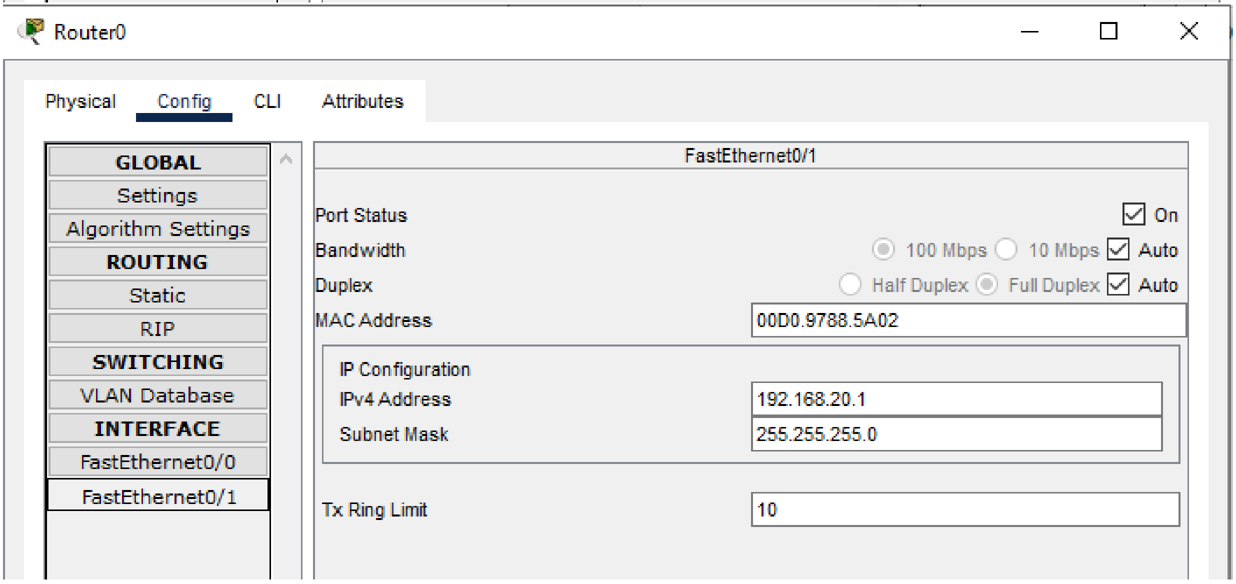
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC0	ICMP		0.000	N	1	(edit)	(delete)

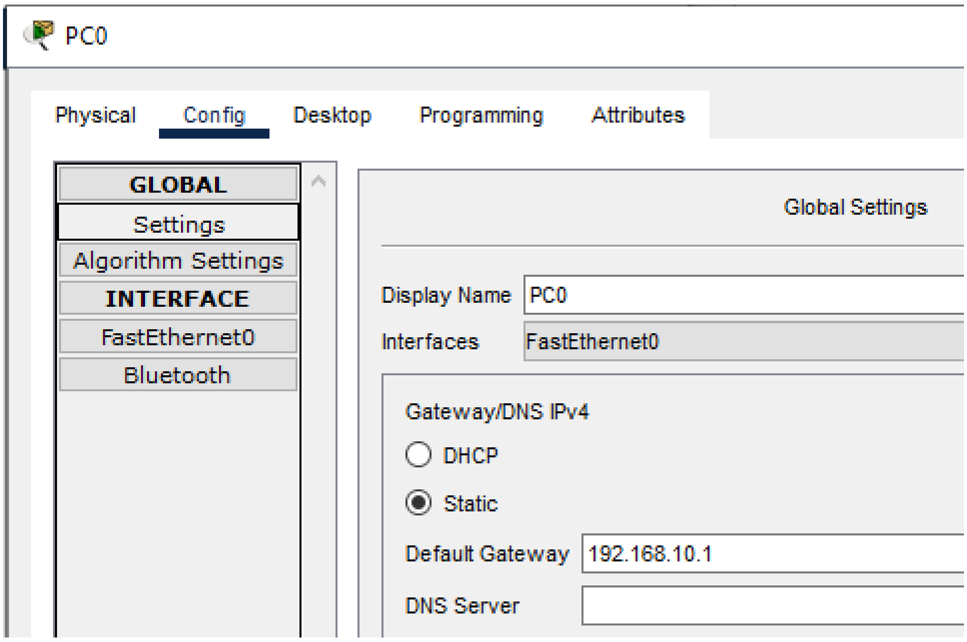


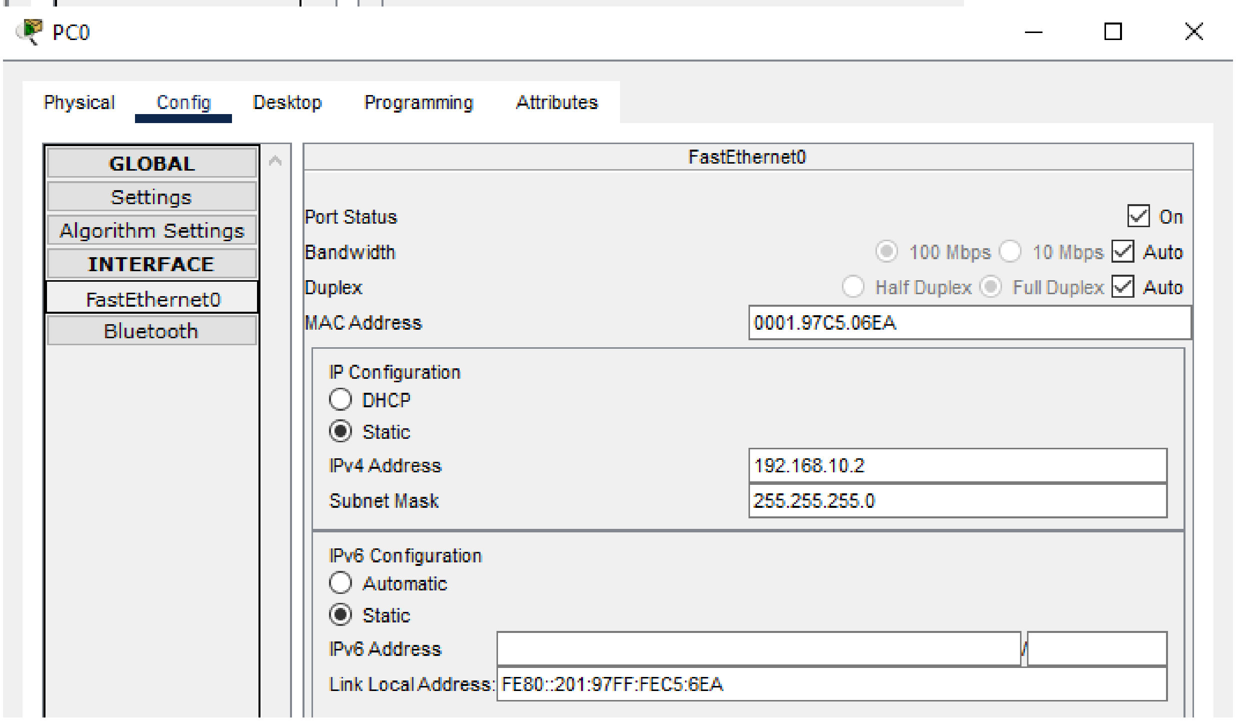
Configuring the Router in the command Line Interface.

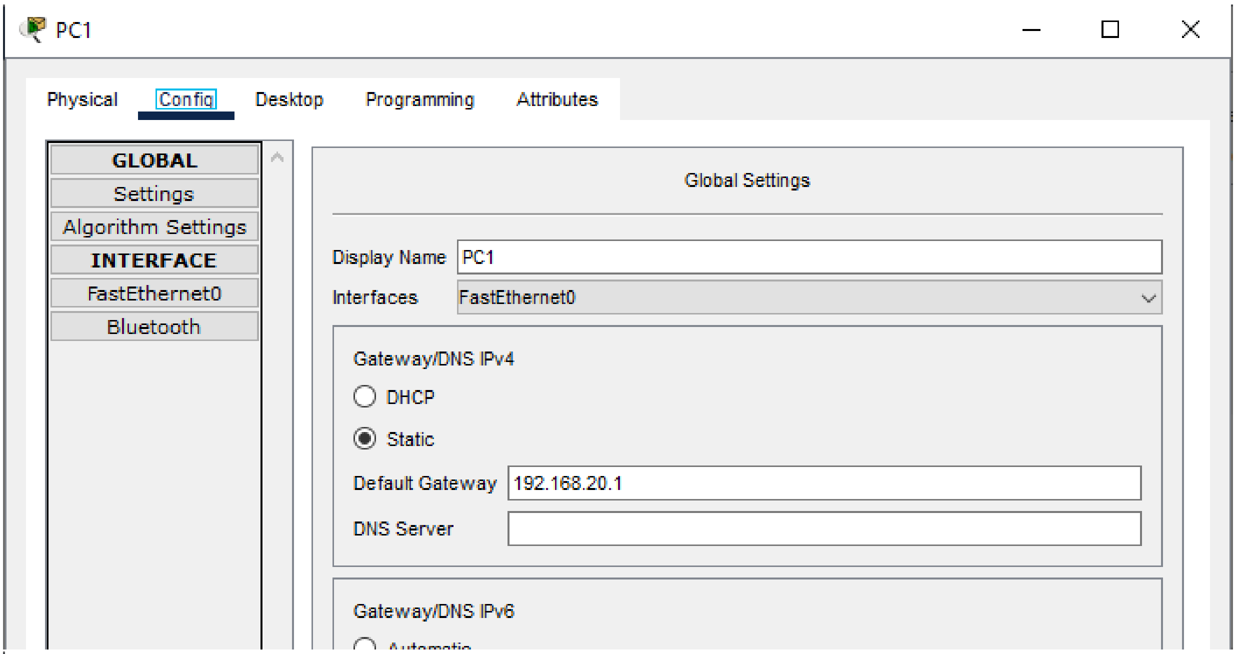

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Network
Network Address
192.168.10.0
192.168.20.0

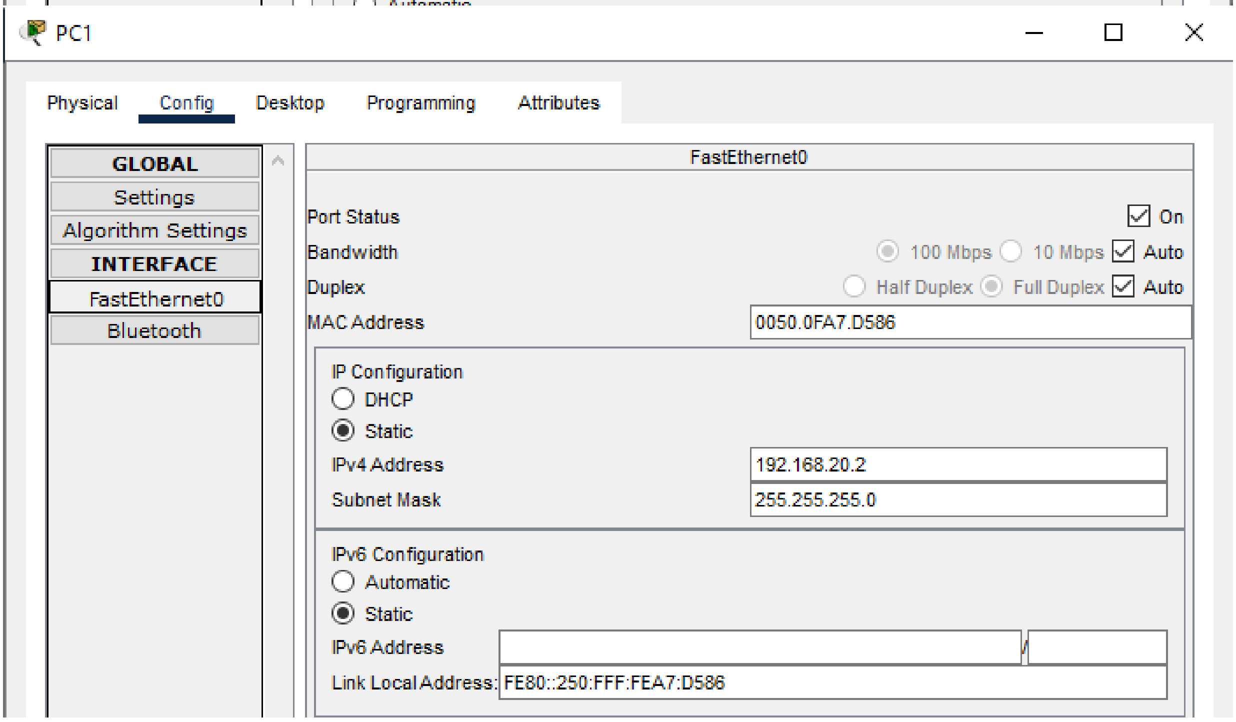

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.9788.5A01
IP Configuration
IPv4 Address
192.168.10.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.9788.5A02
IP Configuration
IPv4 Address
192.168.20.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
PC0
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.10.1
DNS Server


PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.97C5.06EA
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.2
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:97FF:FEC5:6EA


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name PC1
Interfaces FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway 192.168.20.1
DNS Server
Gateway/DNS IPv6


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address 0050.0FA7.D586
IP Configuration
DHCP
Static
IPv4 Address 192.168.20.2
Subnet Mask 255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::250:FFF:FEA7:D586

Part 2:

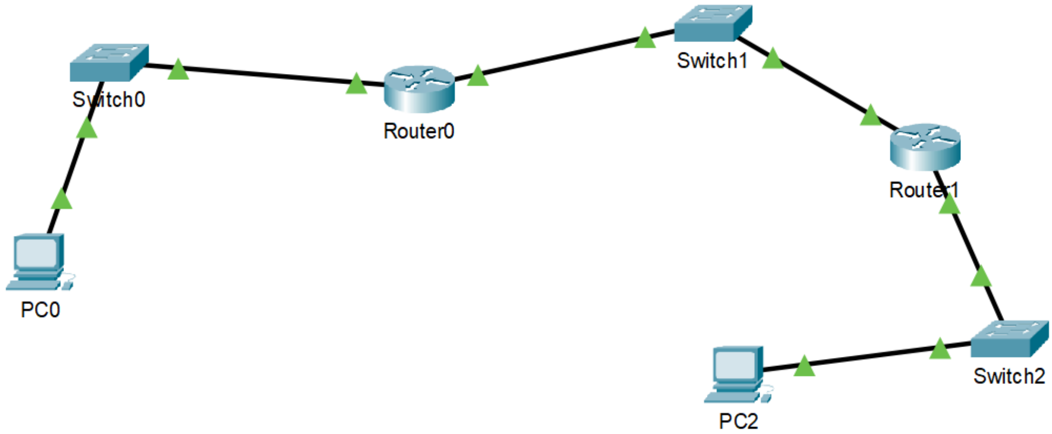
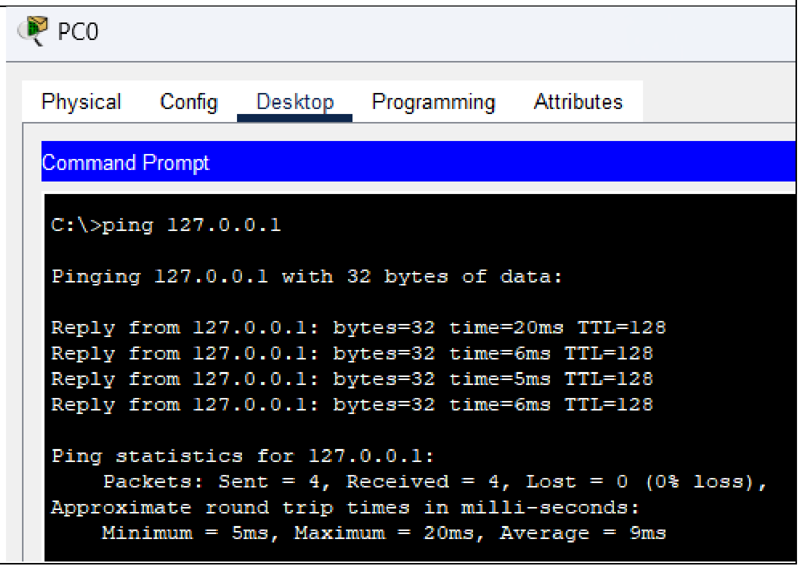
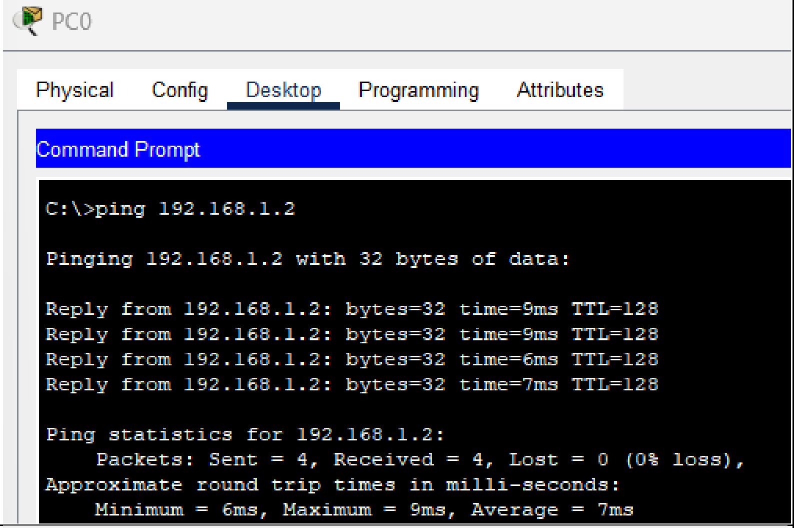
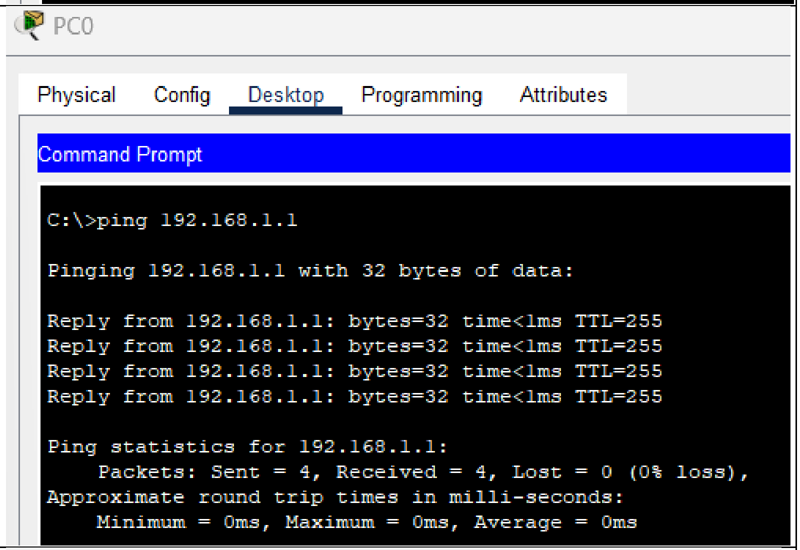
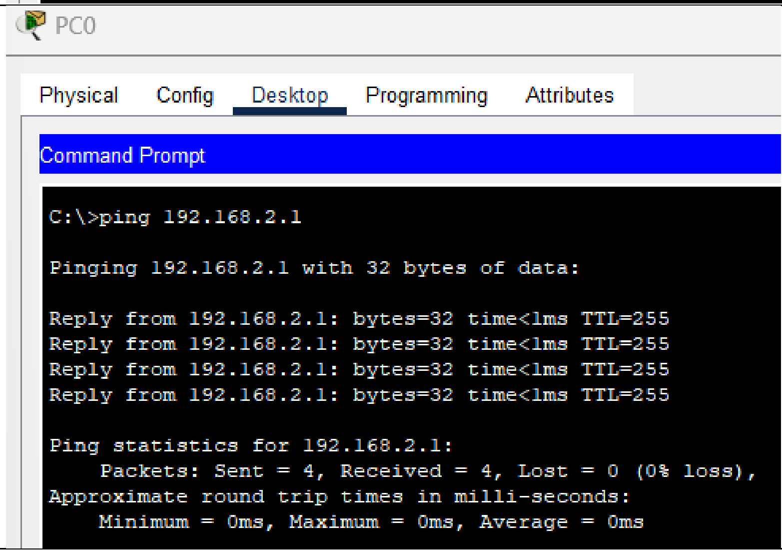
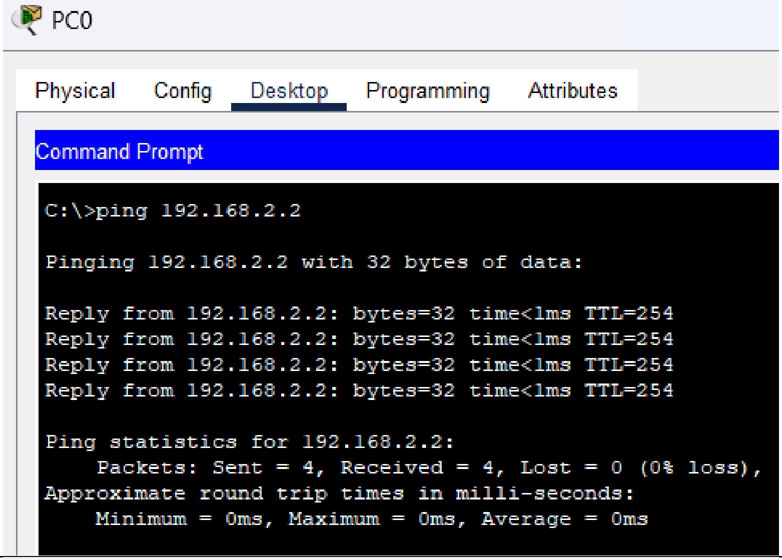
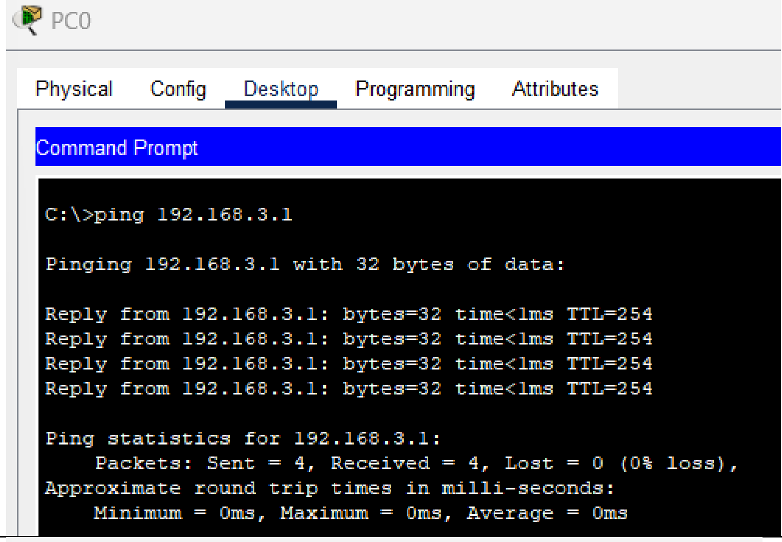
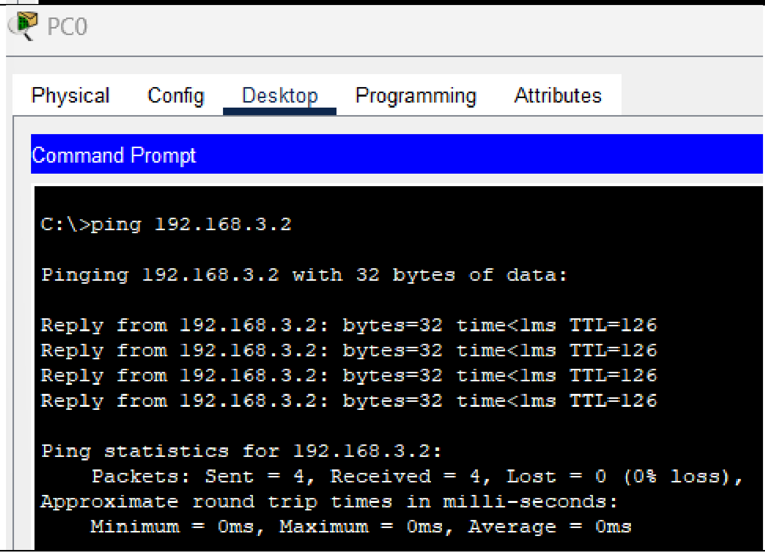
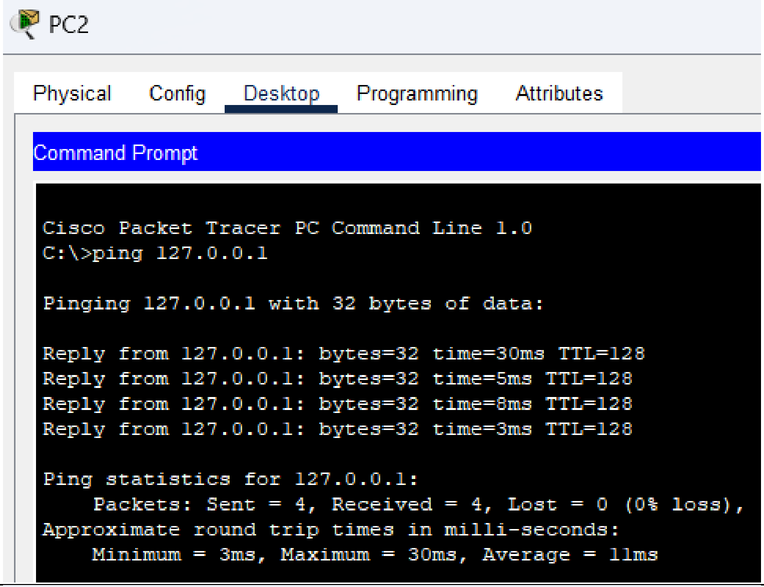
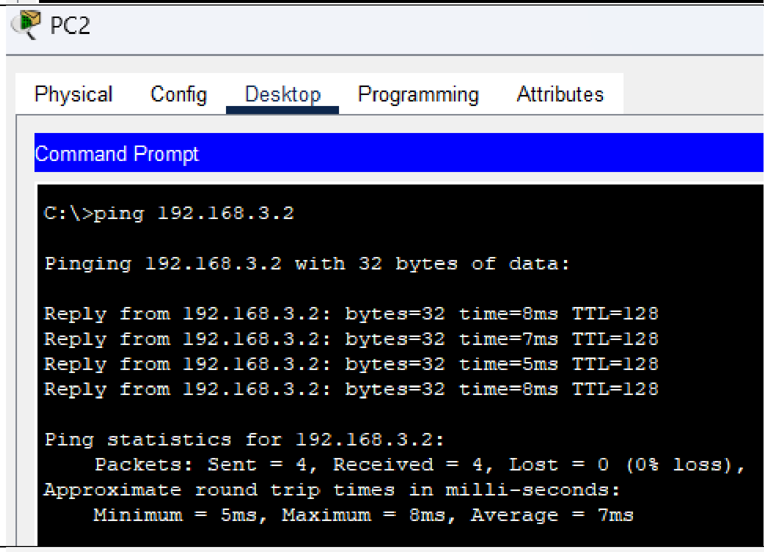
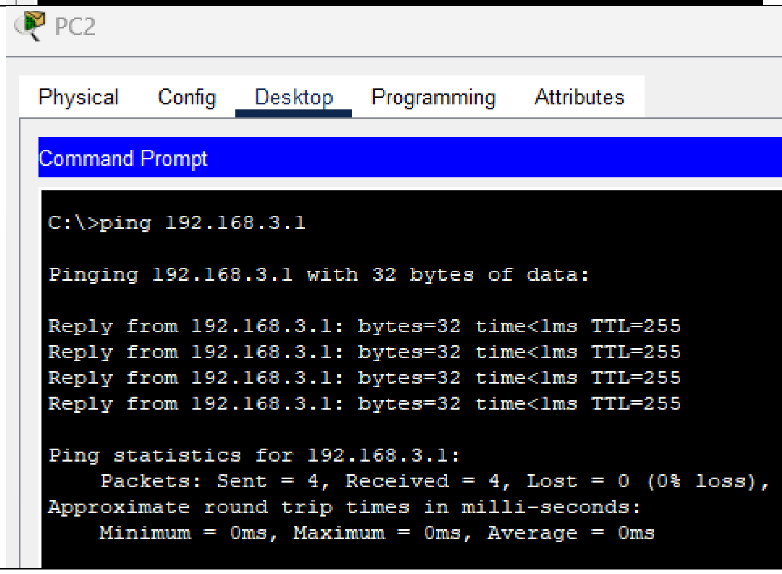


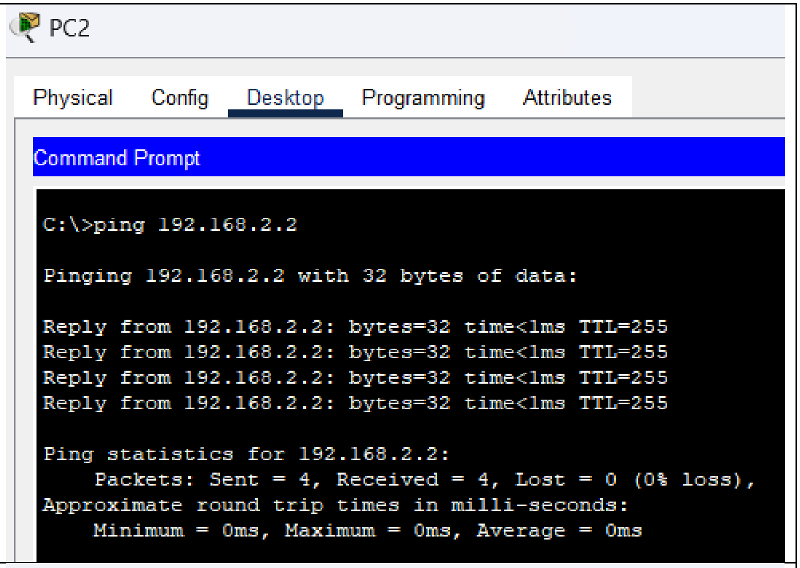
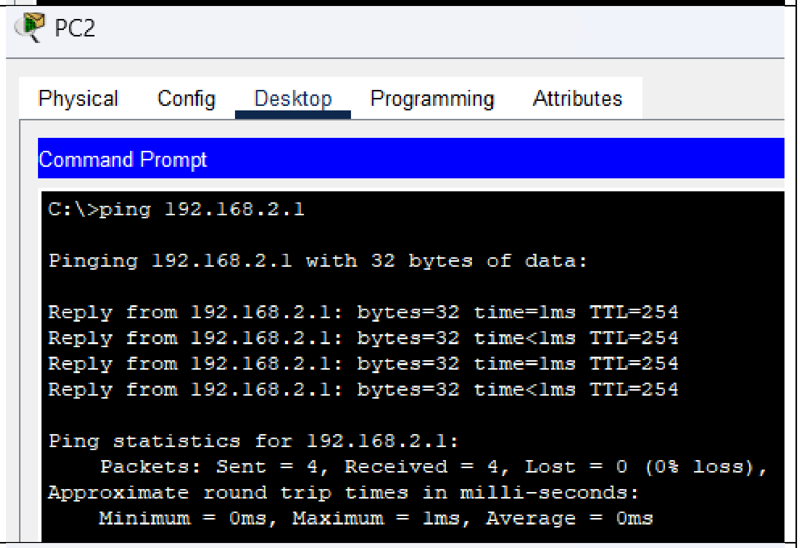
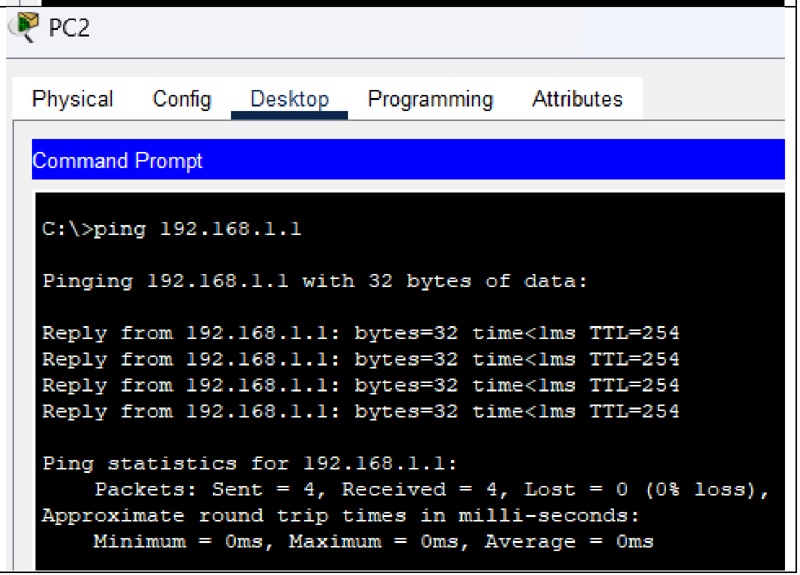
Table: Showing testing with command ping to routers and other PCs on the network.

<table>
<tr><th>Source PC</th><th>Destination Address</th><th>Reachable</th><th>Screenshot</th></tr>
<tr><td>PC0</td><td>127.0.0.1</td><td>Yes</td><td>
</td></tr>
</table>

PC0	192.168.1.2	Yes	
PC0	192.168.1.1	Yes	
PC0	192.168.2.1	Yes	

<table>
<tr><td>PC0</td><td>192.168.2.2</td><td>Yes</td><td>
</td></tr>
<tr><td>PC0</td><td>192.168.3.1</td><td>Yes</td><td>
</td></tr>
<tr><td>PC0</td><td>192.168.3.2</td><td>Yes</td><td>
</td></tr>
</table>

<table>
<tr><td>PC2</td><td>127.0.0.1</td><td>Yes</td><td>
</td></tr>
<tr><td>PC2</td><td>192.168.3.2</td><td>Yes</td><td>
</td></tr>
<tr><td>PC2</td><td>192.168.3.1</td><td>Yes</td><td>
</td></tr>
</table>

<table>
<tr><td>PC2</td><td>192.168.2.2</td><td>Yes</td><td>
</td></tr>
<tr><td>PC2</td><td>192.168.2.1</td><td>Yes</td><td>
</td></tr>
<tr><td>PC2</td><td>192.168.1.1</td><td>Yes</td><td>
</td></tr>
</table>

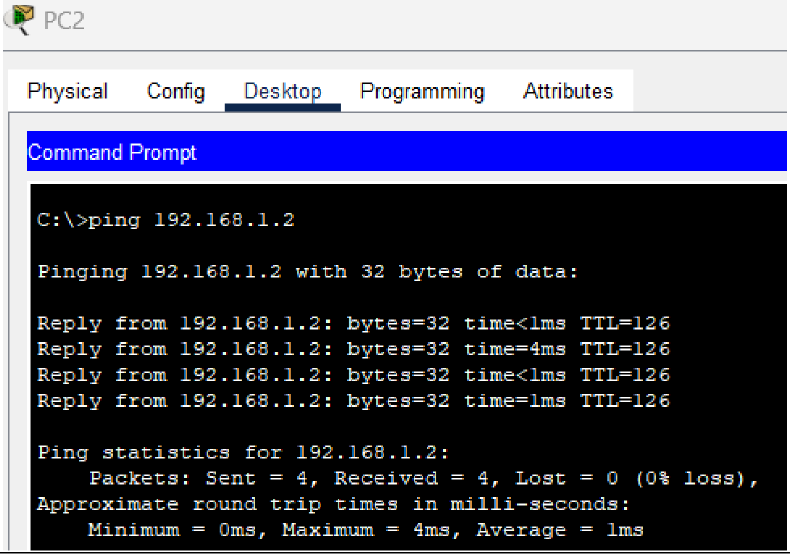
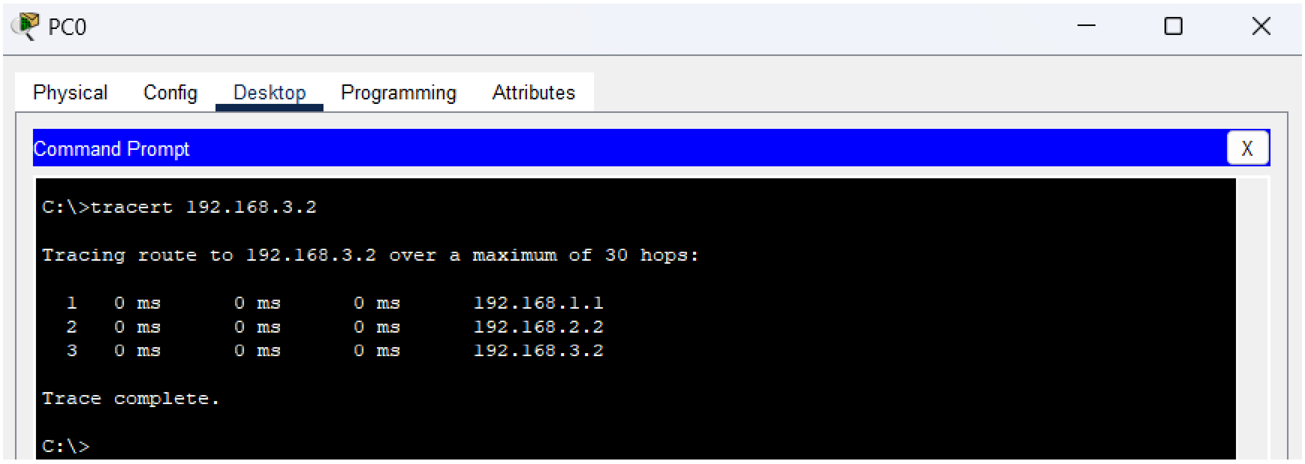
PC2	192.168.1.2	Yes	

Table: Showing the hop route from PC0 to PC2

Hop Number	**IP Address**	**Device Name**
1	N/A	Switch0
2	Input: FastEthernet0/0: 192.168.1.1 Output: FathEthernet0/1: 192.168.2.1	Router0
3	N/A	Switch1
4	Input: FastEthernet0/0: 192.168.2.2 Output: FathEthernet0/1: 192.168.3.1	Router1
5	N/A	Switch2
6	192.168.3.2	PC2

2. Traceroute: Command – Table: Showing the tracing route from PC0 to PC2

Hop Number	**IP Address**	**Device Name**
1	192.168.1.1	Router0
2	192.168.2.2	Router1
3	192.168.3.2	PC2



4. Lab Reports 3: IP Address

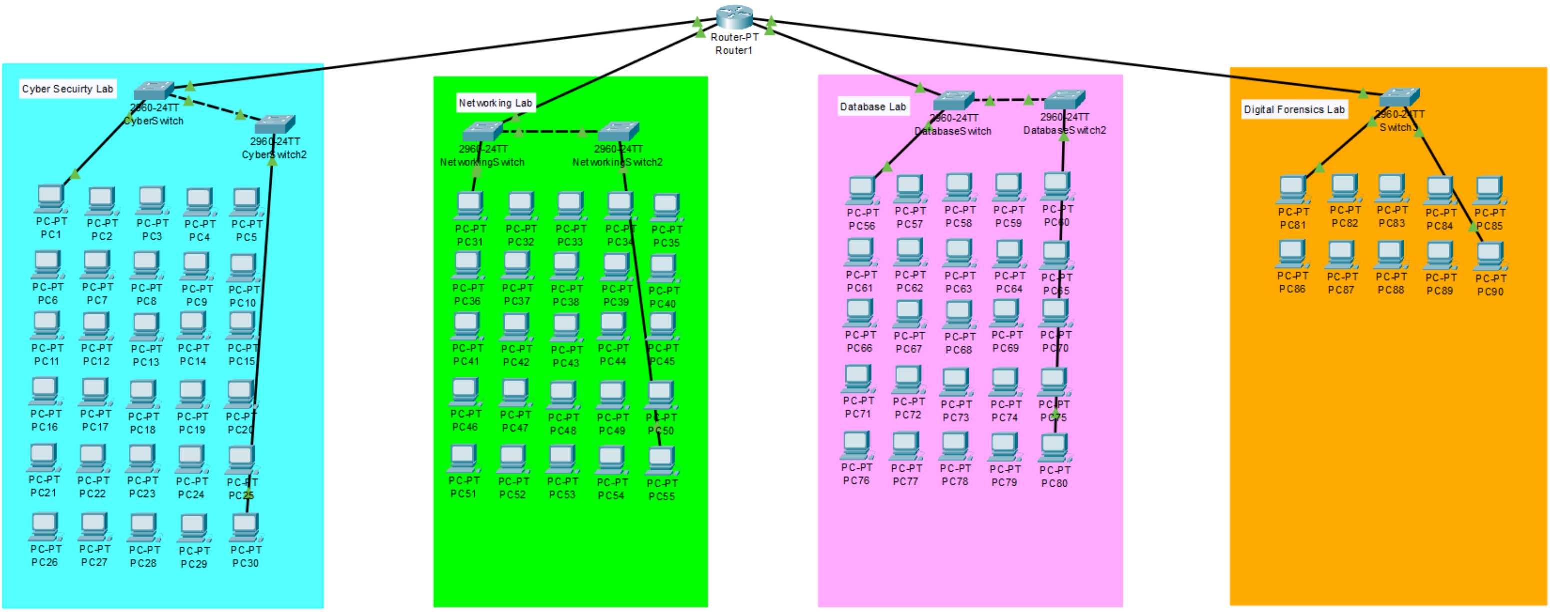
4.1. Introduction

For Lab Report 3, I had to create four subnet networks within a single network. To do this, the subnet was calculated to find which of Edgehill's labs would fit within the smallest subnet masks. Once this was found, I was able to calculate the IP address ranges for each lab and dedicate an IP address to each lab's first PC and last. After this, I set all the devices with the calculated IP addresses and used the same default gateway for all, as they were on the same network. Finally, I successfully tested the network pinging each device from PC1 up to PC90.

4.2. Answers to Questions

1. **What is your network design?**

   My network design is based upon an example of Edgehill's Lab using four subnets. For this task, I have configured 2 PCs for each subnet within the usable IP addresses; this is to simulate the network setup with all devices being configured.



2. **Network Build and IP Address configurations of the network?**

   Firstly, to work out the minimal number of subnets that can be borrowed without going under, use the formula 2^n, where n equals the number of bits borrowed from the host. Next, to calculate the number of usable IP addresses per subnet, we use the formula $2^h - 2$, where h equals the number of host bits borrowed from the original number of host bits. Finally, this will calculate the subnet mask to use based on the number of bits borrowed (Thomas, 2014).

I. Number of Hosts per Subnet

Each subnet needs to support Host Required + 2 for the network address and broadcast address (Thomas, 2014).

Cyber Subnet:
Host Required = 30
Total IPs needed = 30 + 2 = 32

Networking Subnet:
Host Required = 25
Total IPs needed = 25 + 2 = 27

Database Subnet:
Host Required = 25
Total IPs needed = 25 + 2 = 27

Digital Forensics Subnet:
Host Required = 10
Total IPs needed = 10 + 2 = 12

II. Subnet Mask Prefix

The formula for the required number of addresses with each subnet is 2^n, where n equals the number of bits borrowed from the host (GeeksforGeeks, 2024).

- n = The smallest power of 2 that the total amount of IPs can fit within.

For Each subnet:

- Subnet 1: $2^n = 64$, so n = 6 therefore 32 – 6 = prefix of /26.
- Subnet 2: $2^n = 32$, so n = 5 therefore 32 – 5 = prefix of /27.
- Subnet 3: $2^n = 32$, so n = 5 therefore 32 – 5 = prefix of /27.
- Subnet 4: $2^n = 16$, so n = 4 therefore 32 – 4 = prefix of /28.

Converting Prefix to Subnet Mask:

To convert the prefix to a subnet mask, convert the prefix number to ones, then convert the binary into decimal (GeeksforGeeks, 2024).

Cyber Subnet with a prefix of 26:
11111111.11111111.11111111.11000000 = 255.255.255.192

Networking Subnet with a prefix of 27:
11111111.11111111.11111111.11100000 = 255.255.255.224

Database Subnet with a prefix of 27:
11111111.11111111.11111111.11100000 = 255.255.255.224

Digital Forensics Subnet with a prefix of 28:
11111111.11111111.11111111.11110000 = 255.255.255.240

III. Address Ranges

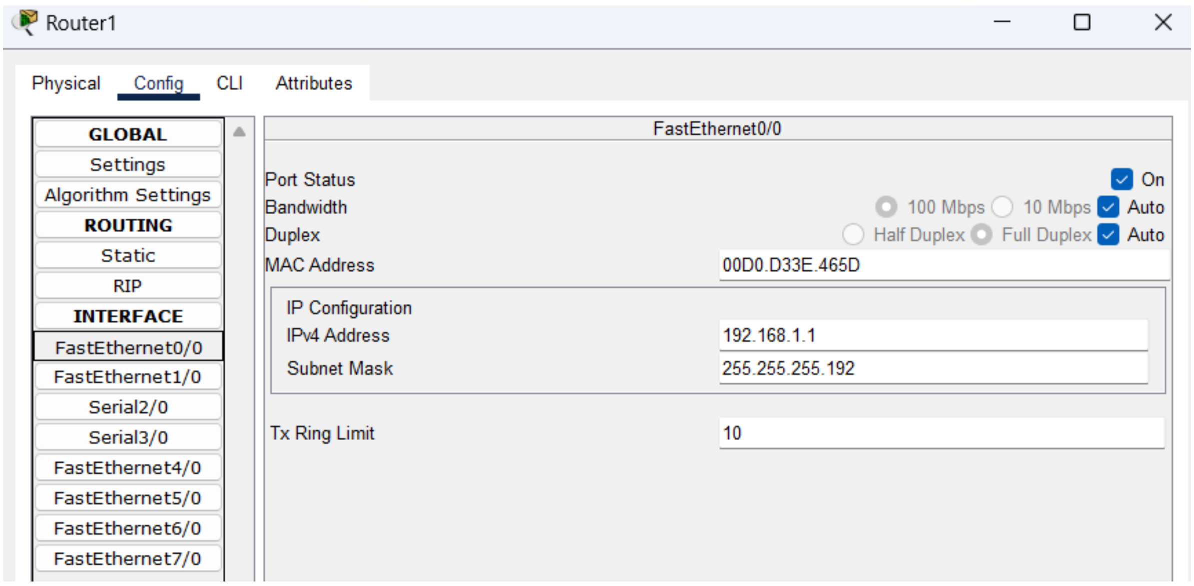
- **Cyber Subnet 1:**
    - Usable Range of Host IP Addresses: 192.168.1.1 to 192.168.1.62
      Broadcast Address: 192.168.1.63
- **Networking Subnet 2:**
    - Usable Range of Host IP Addresses: 192.168.1.65 to 192.168.1.94
      Broadcast Address: 192.168.1.95
- **Database Subnet 3:**
    - Usable Range of Host IP Addresses: 192.168.1.97 to 192.168.1.126
      Broadcast Address: 192.168.1.127
- **Digital Forensics Subnet 4:**
    - Usable Range of Host IP Addresses: 192.168.1.129 to 192.168.1.142
    - Broadcast Address: 192.168.1.143

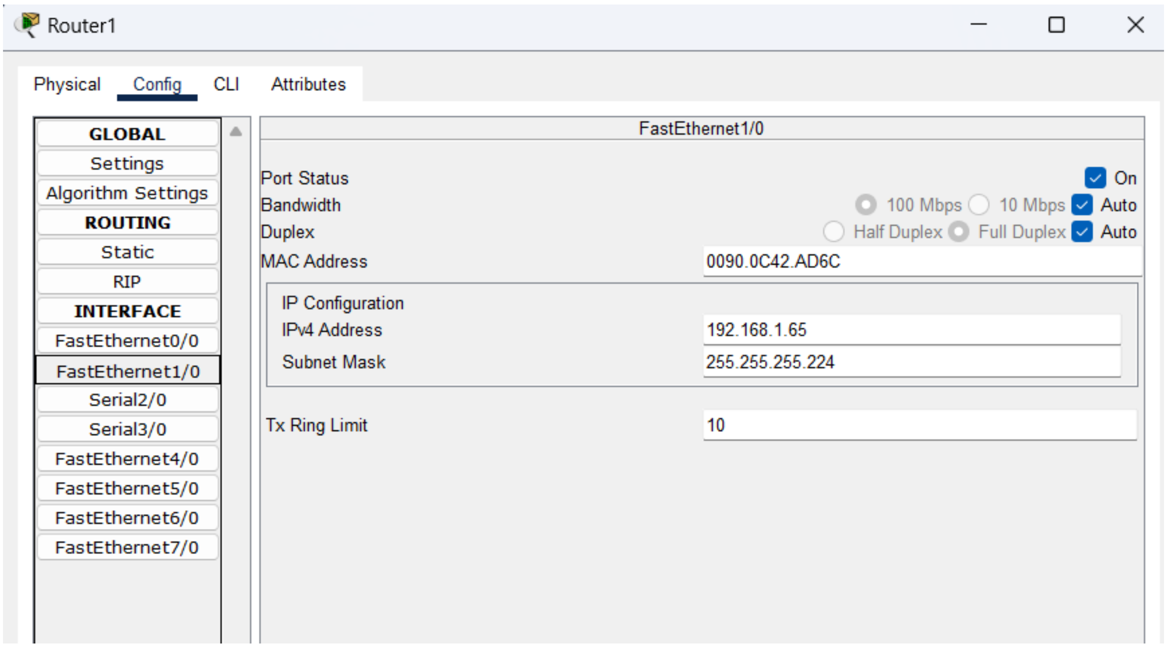
IV. Breakdown:

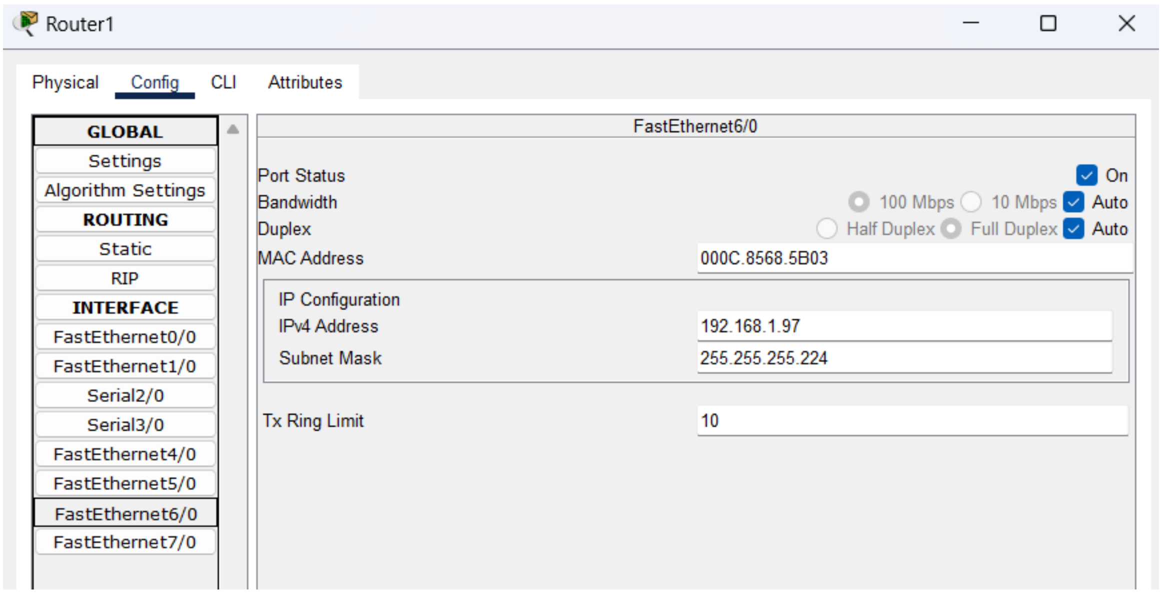
Subnet	Hosts	Subnet Mask	Usable Address Range	Broadcast Address	Network Address
Cyber	30	255.255.255.192	192.168.1.1 to 192.168.1.62	192.168.1.63	192.168.1.0
Networking	25	255.255.255.224	192.168.1.65 to 192.168.1.94	192.168.1.95	192.168.1.64
Database	25	255.255.255.224	192.168.1.97 to 192.168.1.126	192.168.1.127	192.168.96
Digital Forensics	10	255.255.255.240	192.168.1.129 to 192.168.1.142	192.168.1.143	192.168.1.128

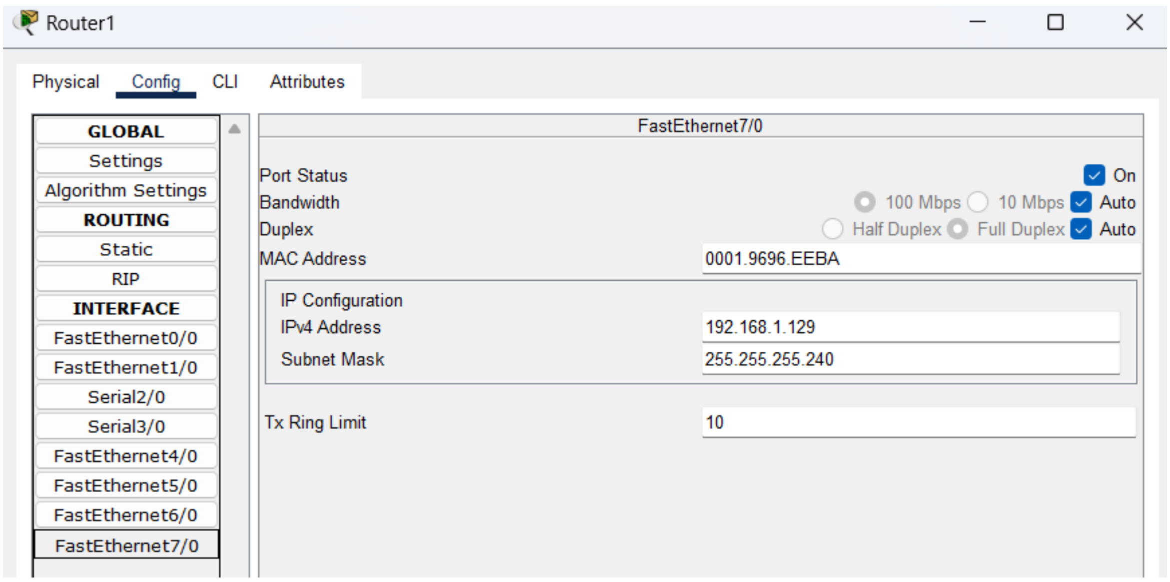
Configuration & Testing Screenshots:

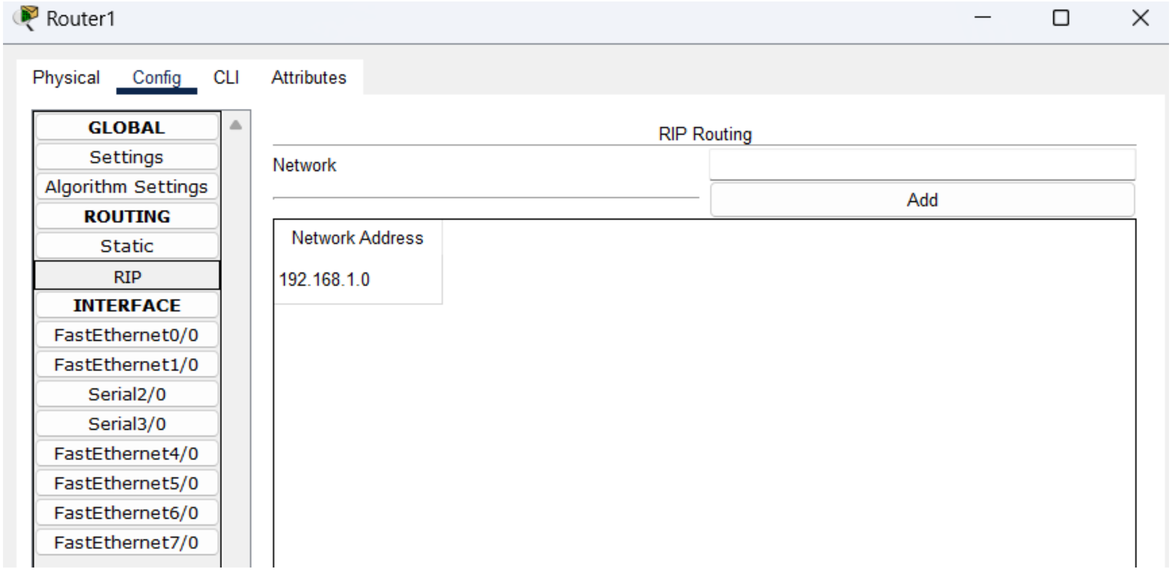
Configurations for the Router:



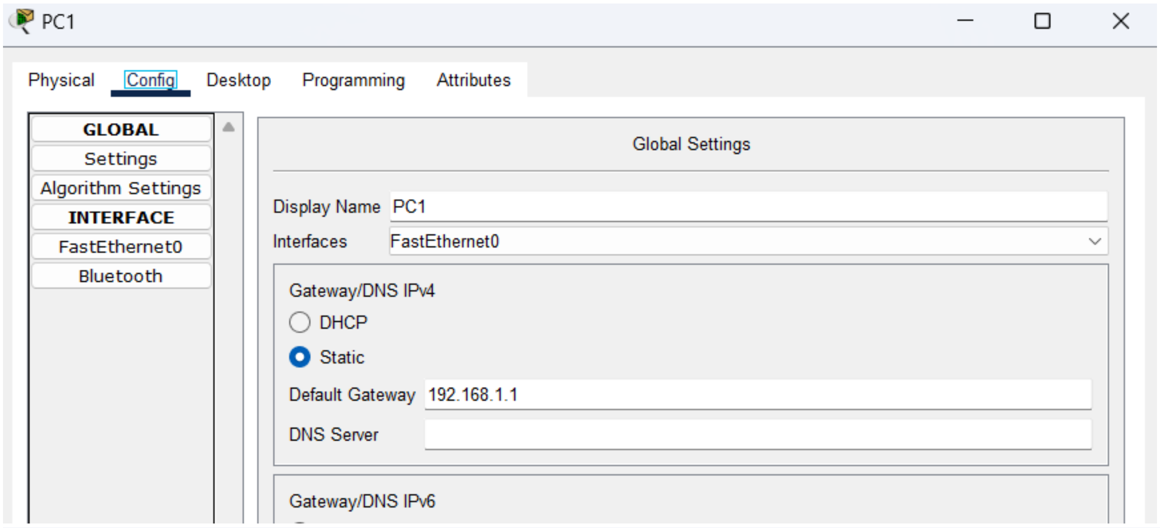

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet6/0
FastEthernet7/0
FastEthernet1/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.0C42.AD6C
IP Configuration
IPv4 Address
192.168.1.65
Subnet Mask
255.255.255.224
Tx Ring Limit
10

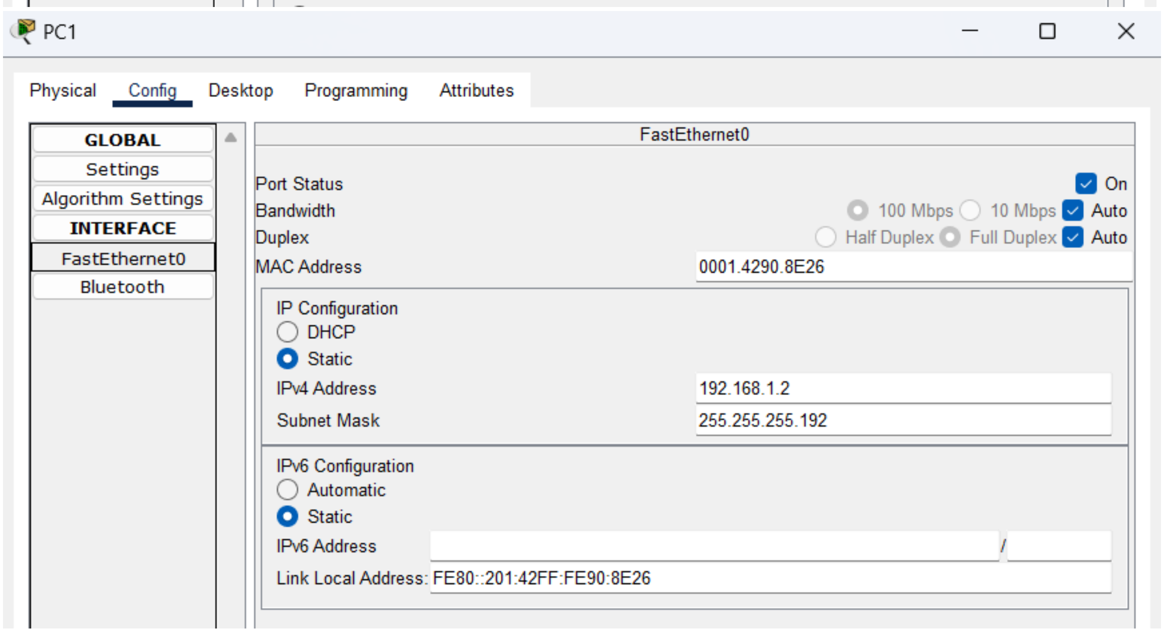

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet6/0
FastEthernet7/0
FastEthernet6/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8568.5B03
IP Configuration
IPv4 Address
192.168.1.97
Subnet Mask
255.255.255.224
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet6/0
FastEthernet7/0
FastEthernet7/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.9696.EEBA
IP Configuration
IPv4 Address
192.168.1.129
Subnet Mask
255.255.255.240
Tx Ring Limit
10

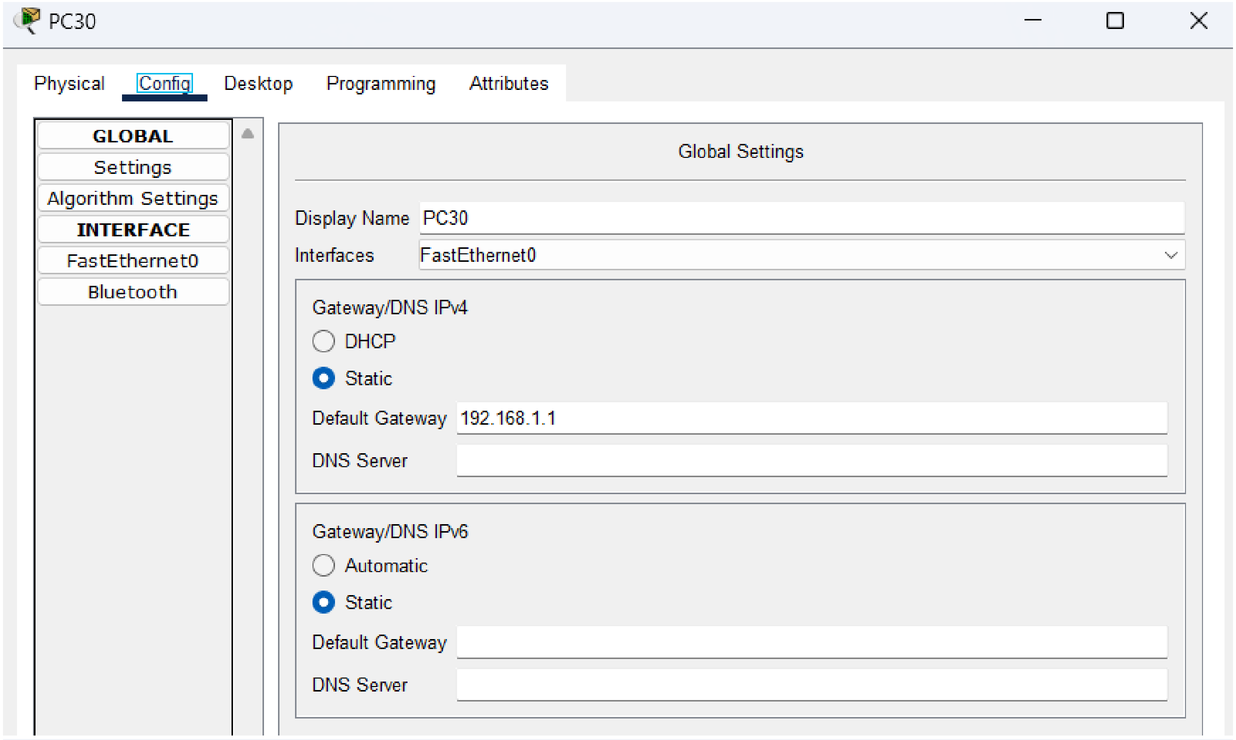


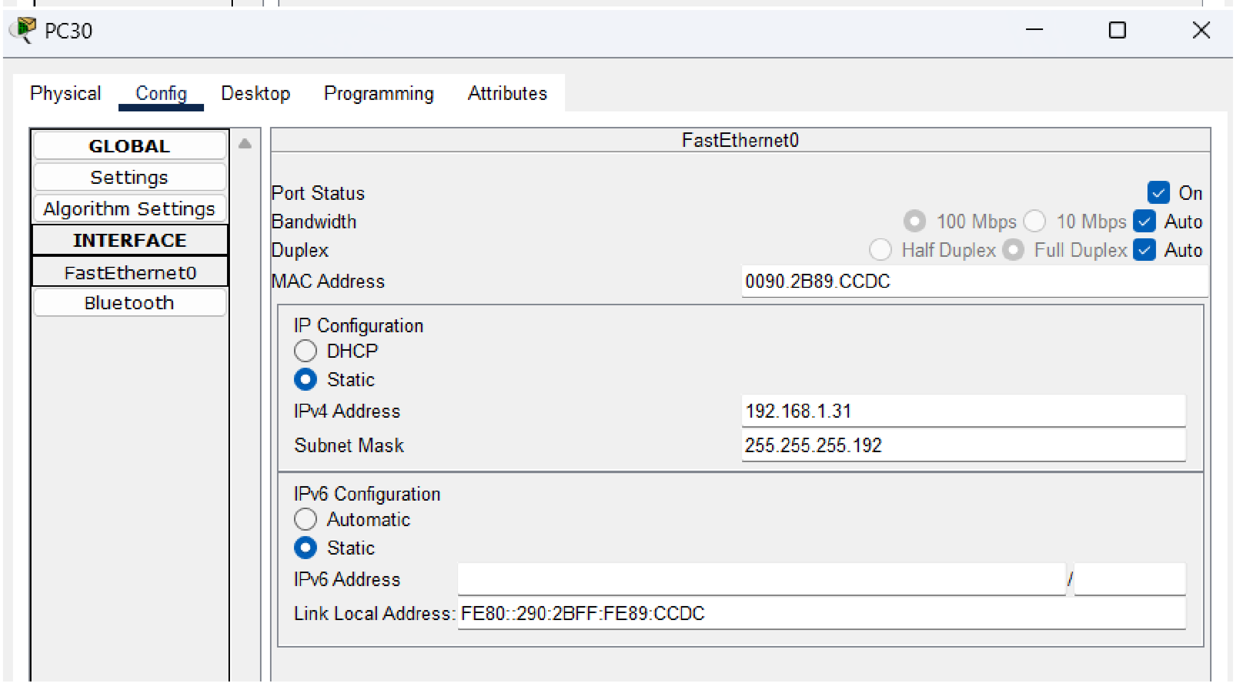
Configurations for PC 1 within Cyber Security Lab:



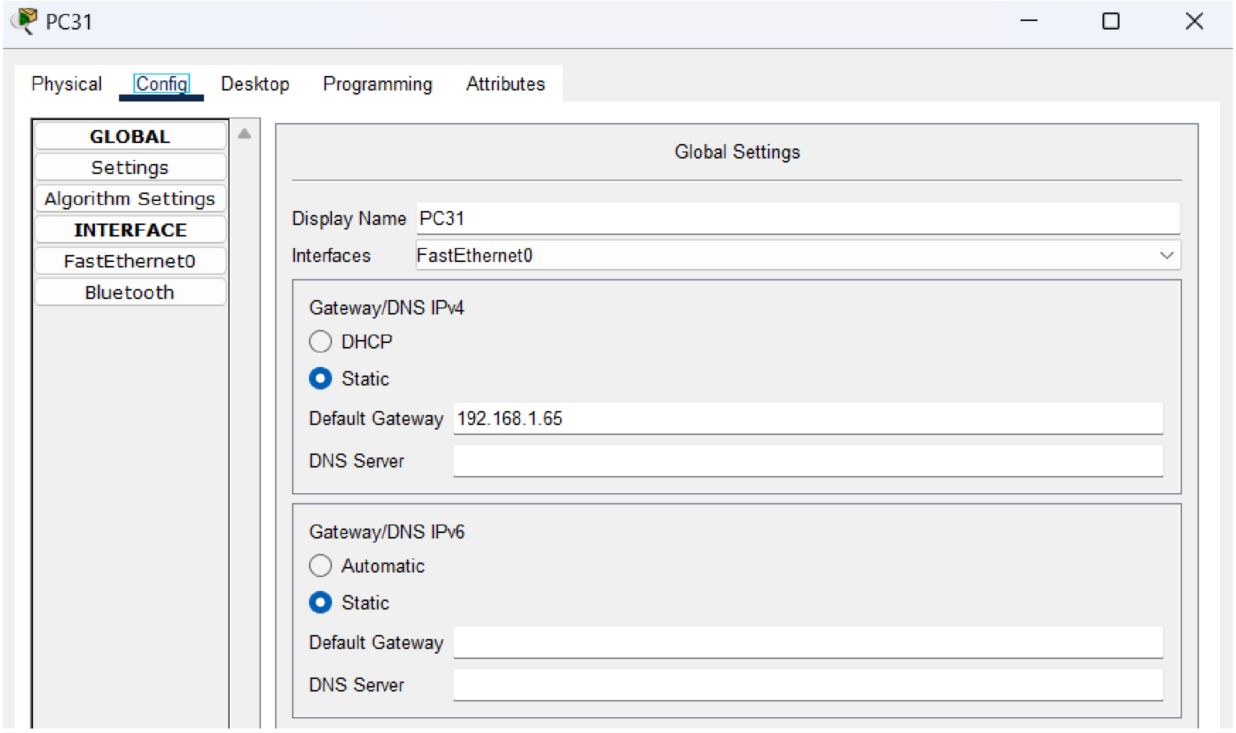


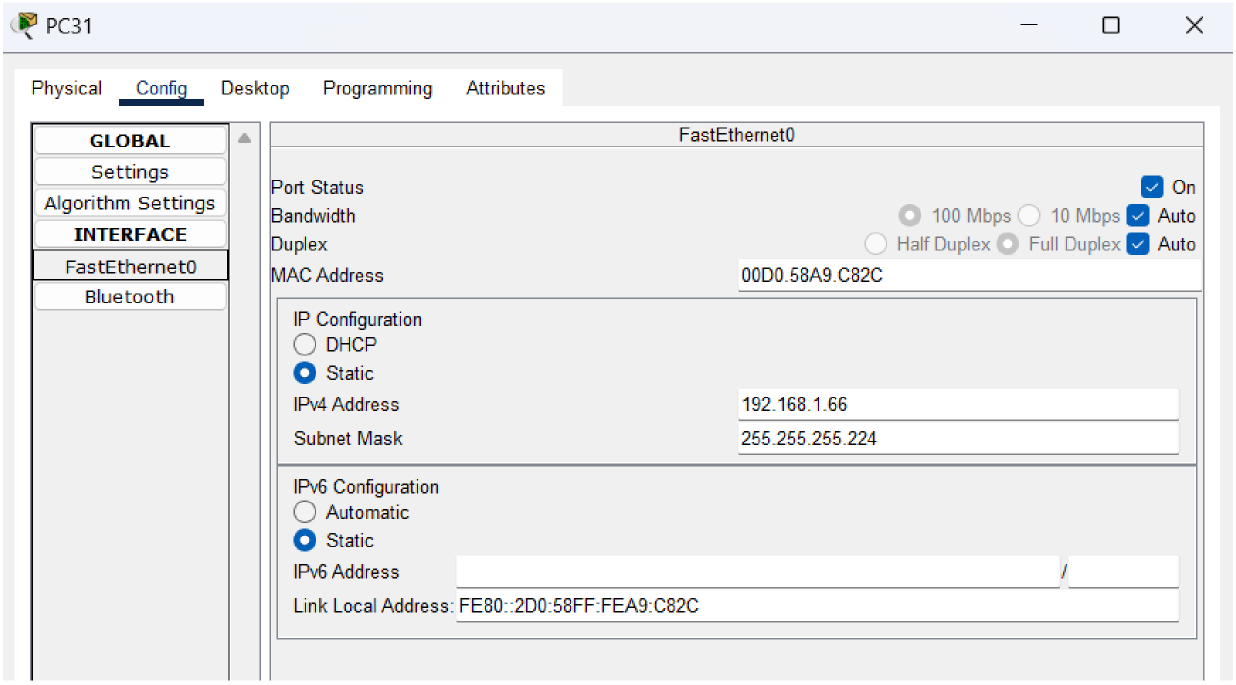
Configurations for PC 30 within Cyber Security Lab:



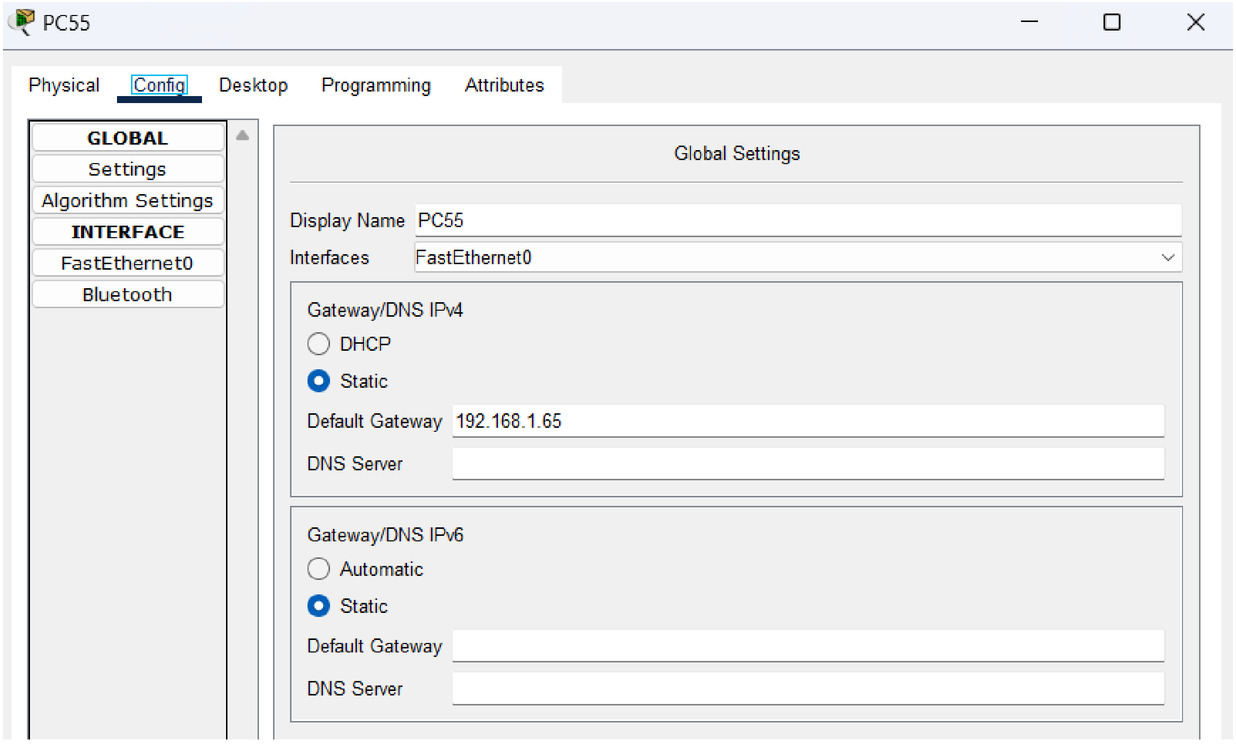


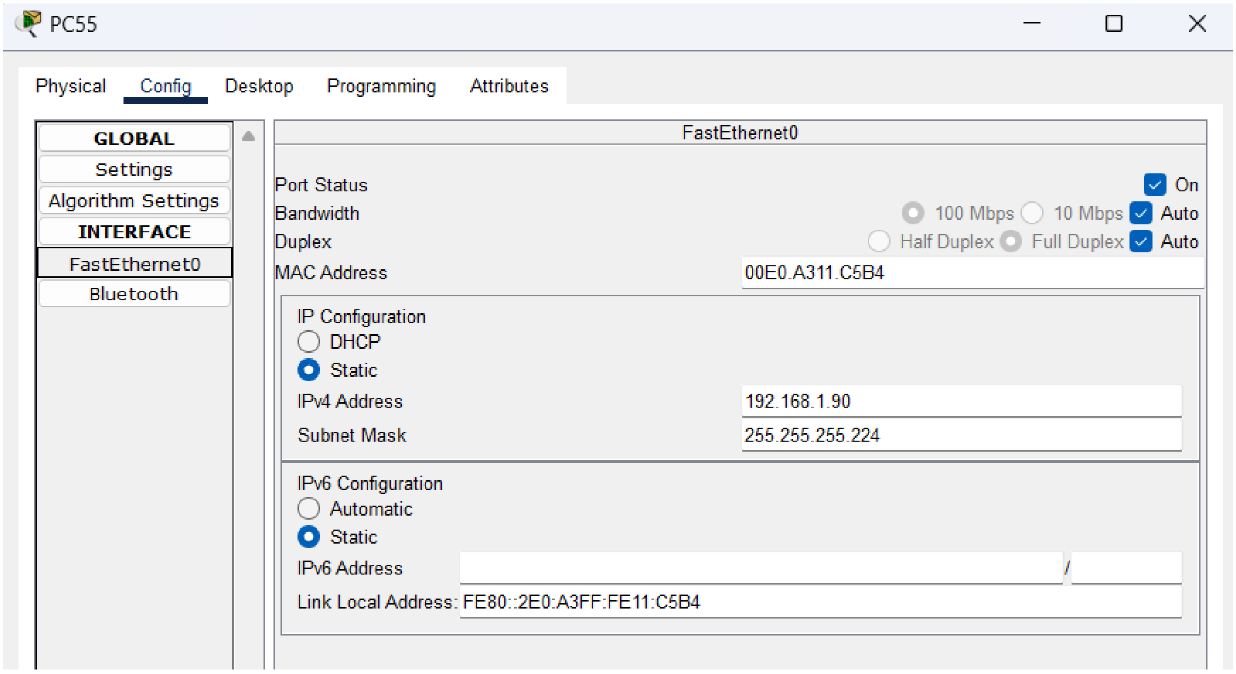
Configurations for PC31 in the Networking Lab:



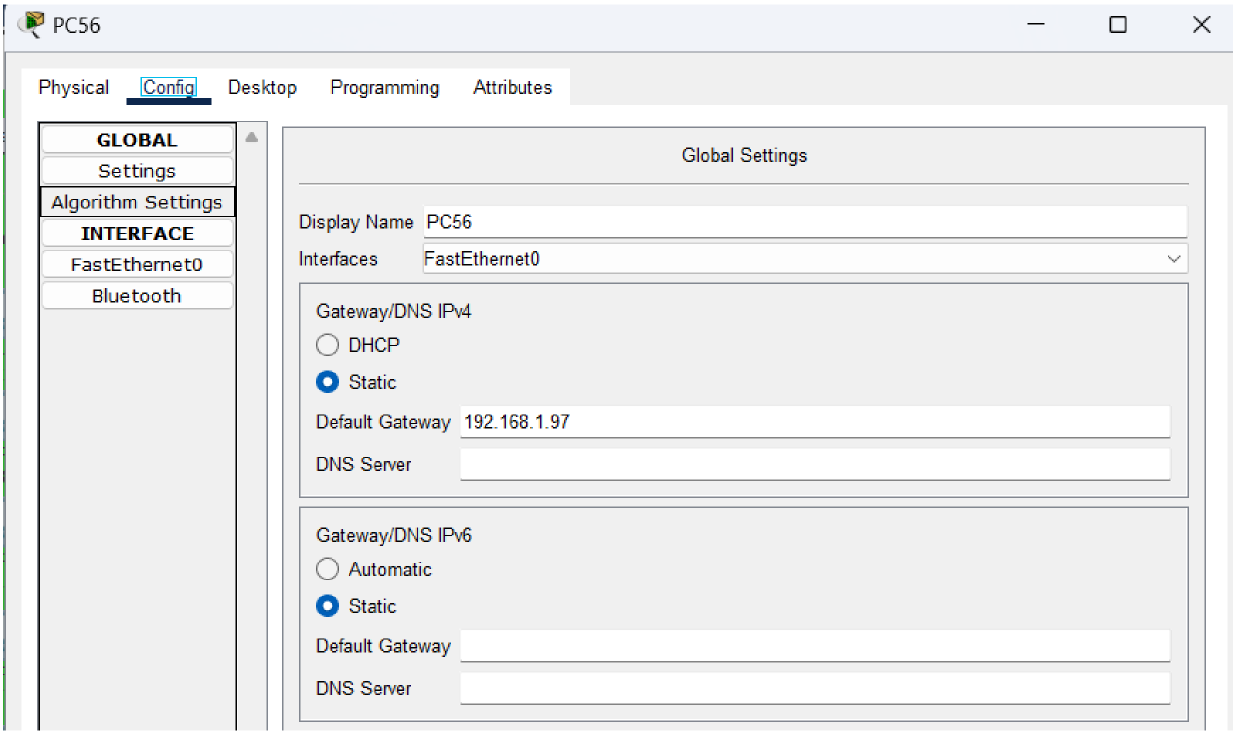


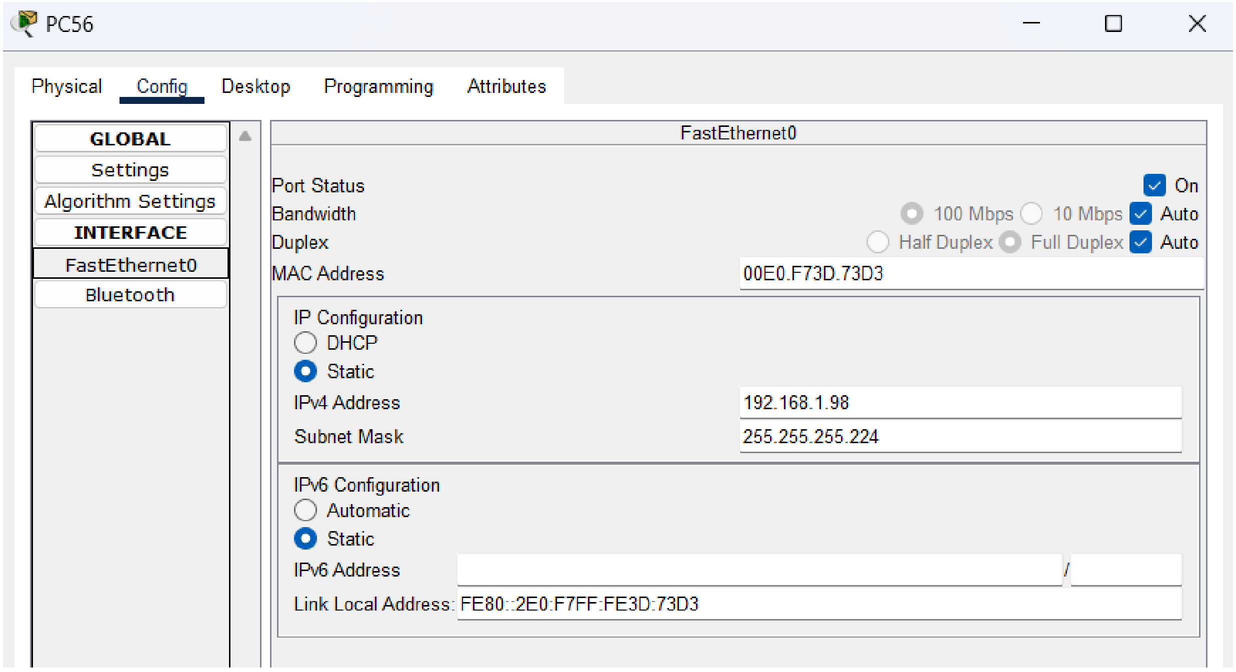
Configurations for PC 55 in the Networking Lab:



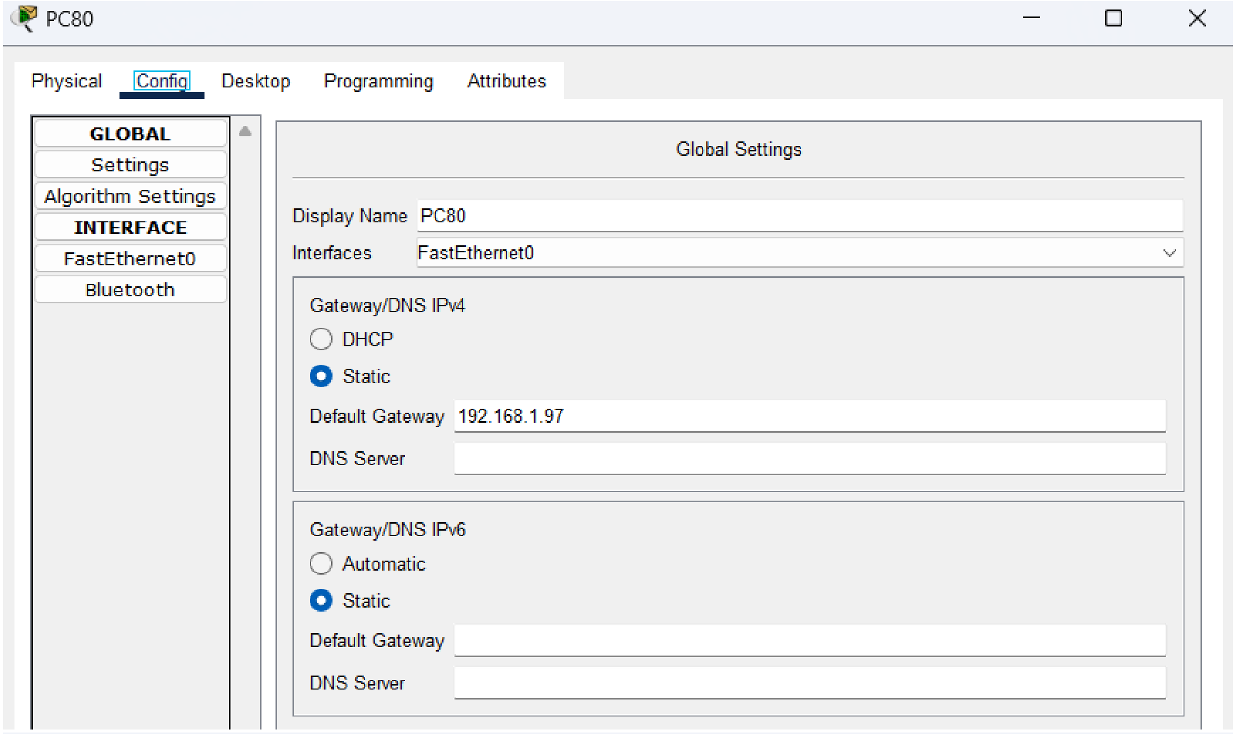


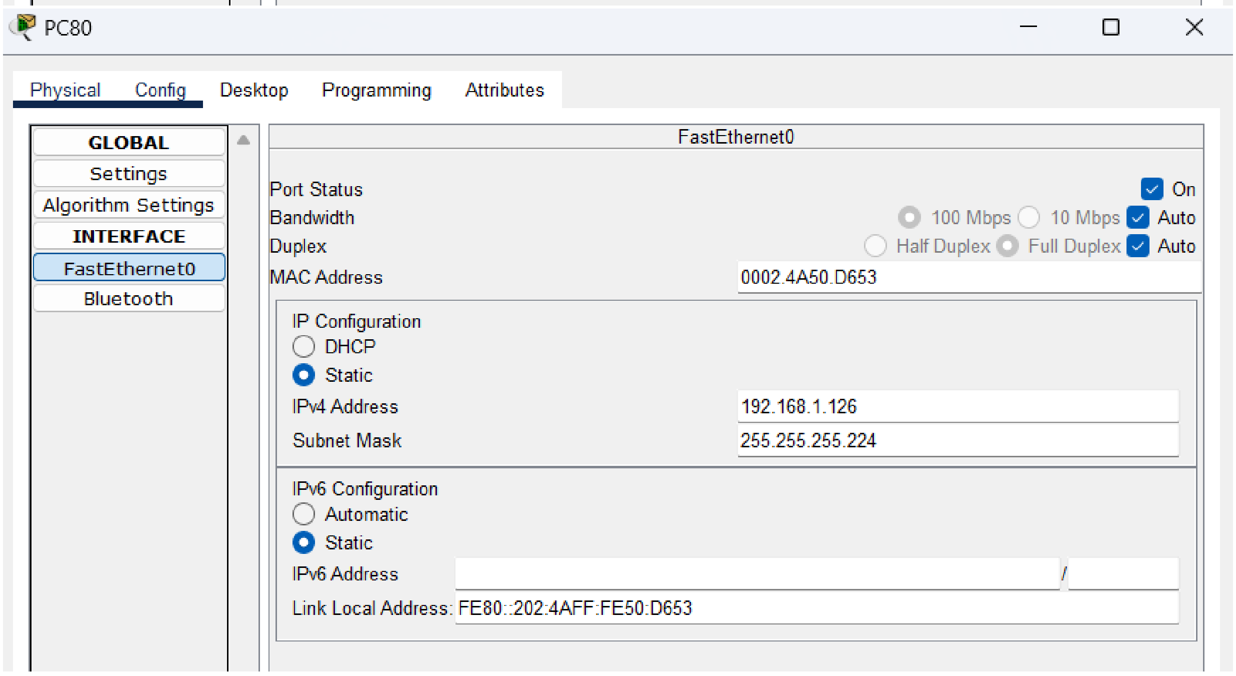
Configurations for PC 56 in the Database Lab:



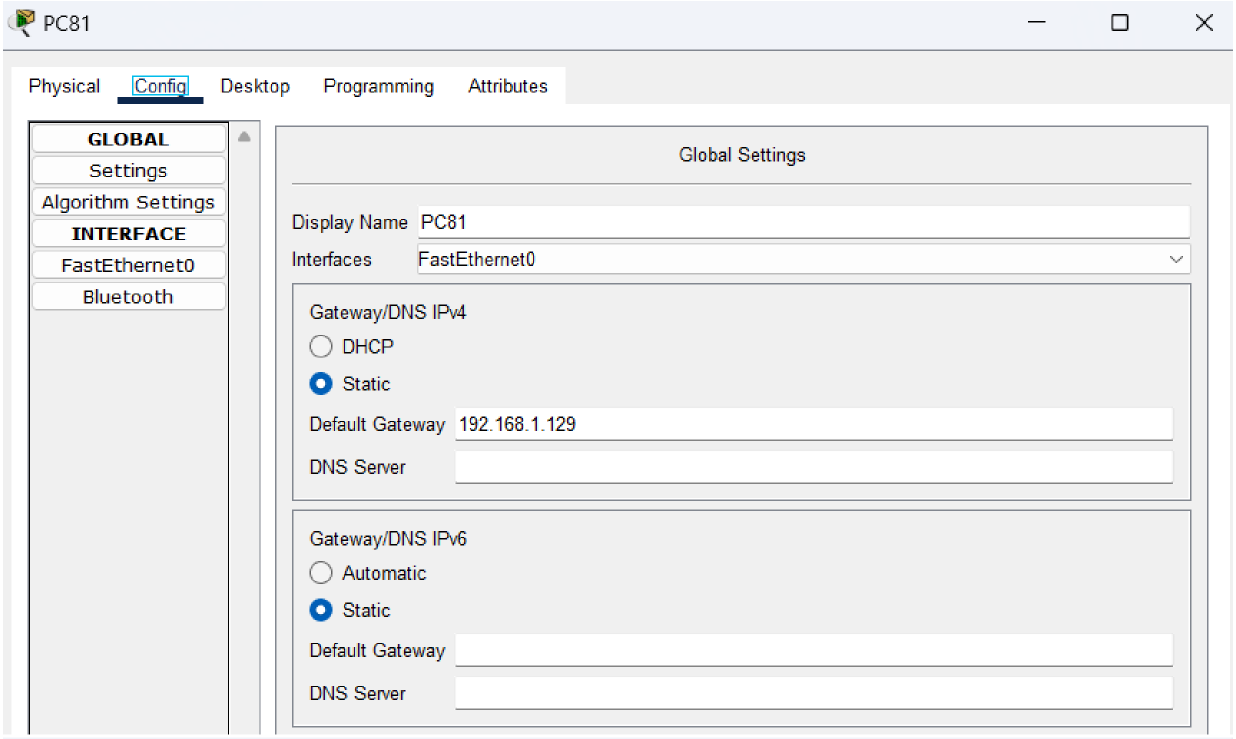


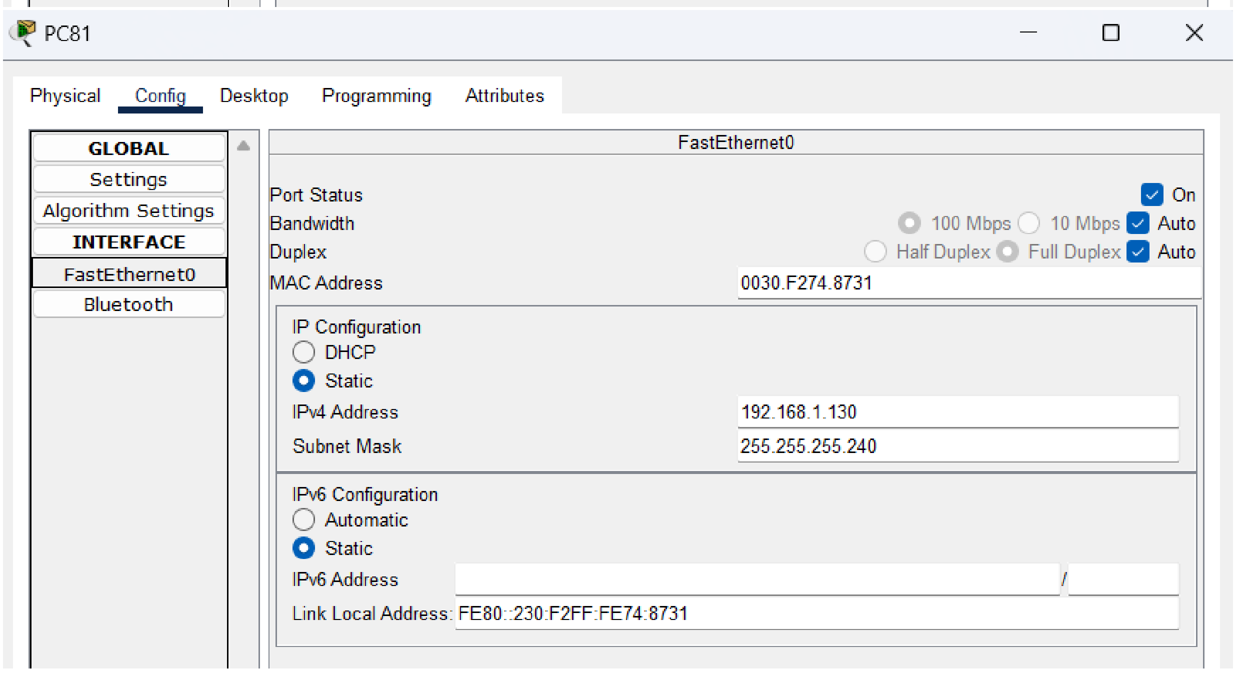
Configurations for PC 80 in the Database Lab:



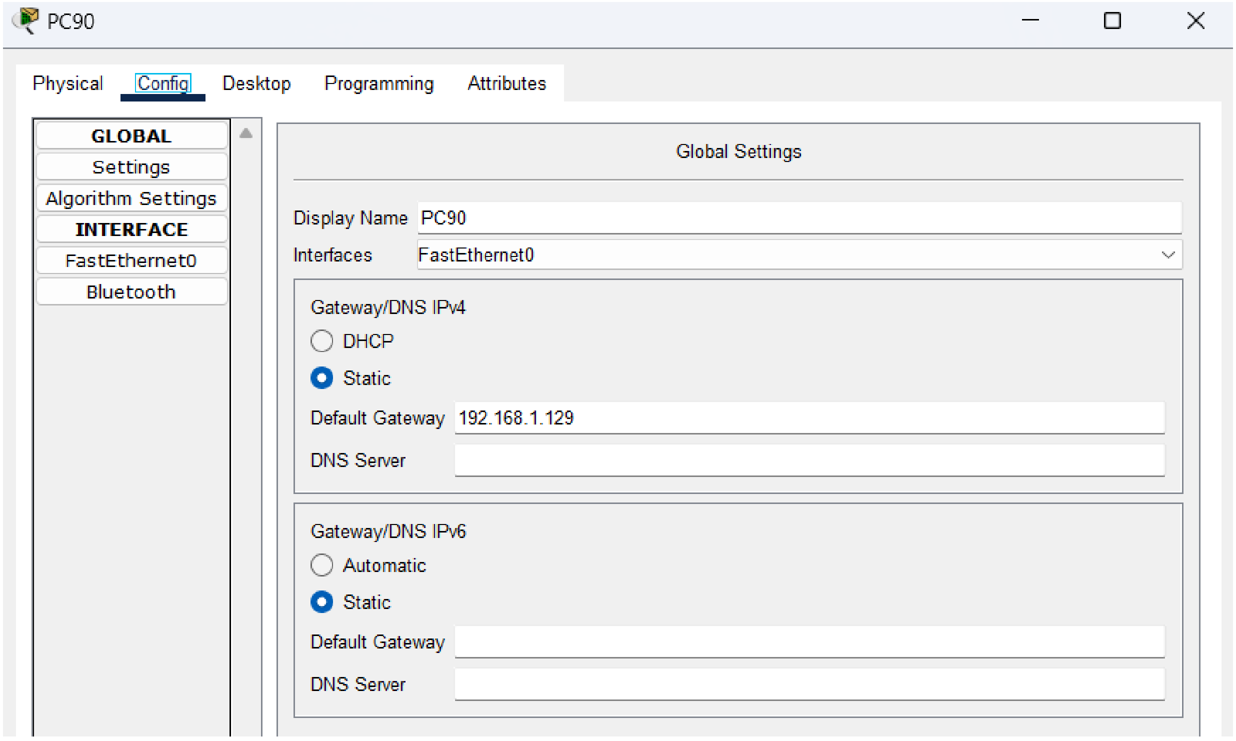


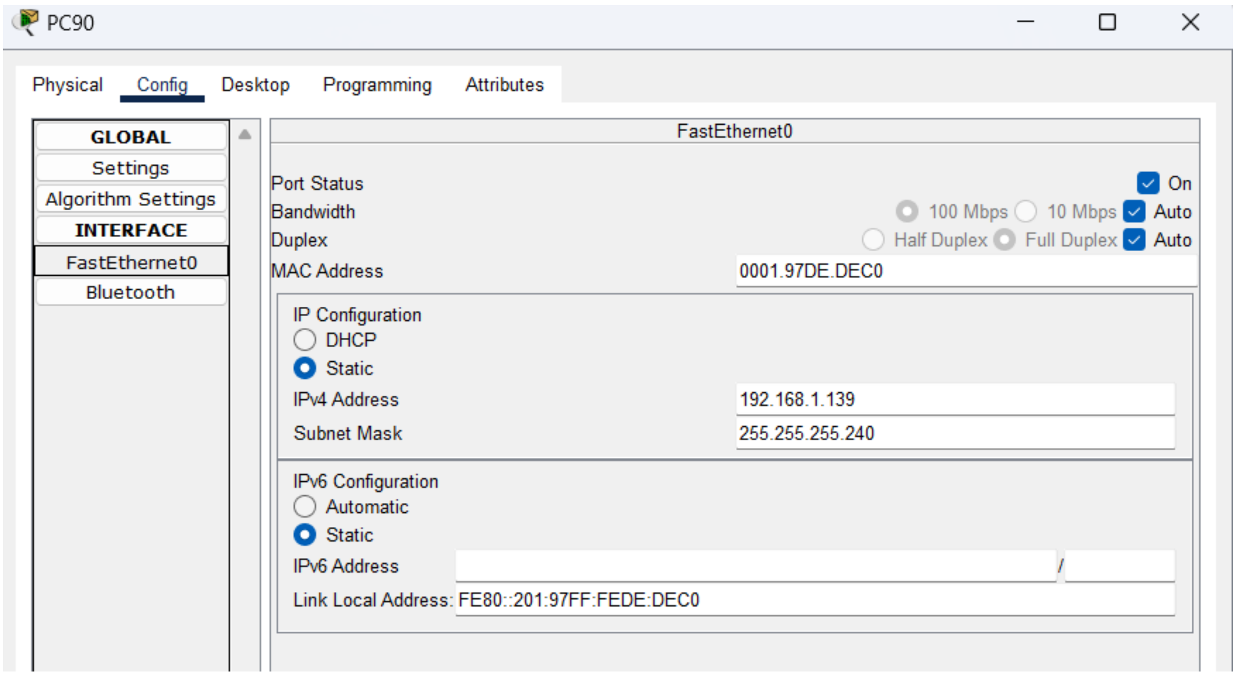
Configurations for PC81 in the Digital Forensics Lab:





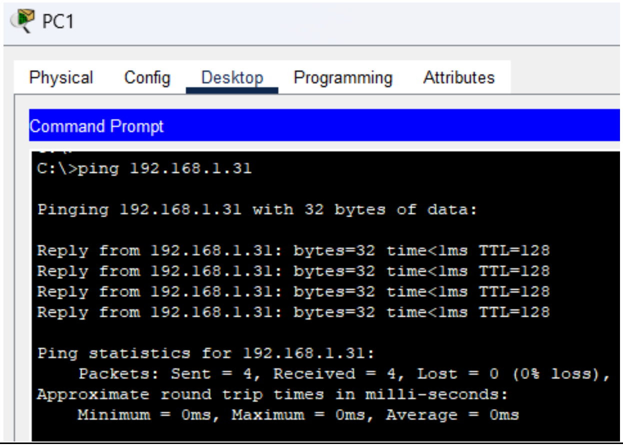
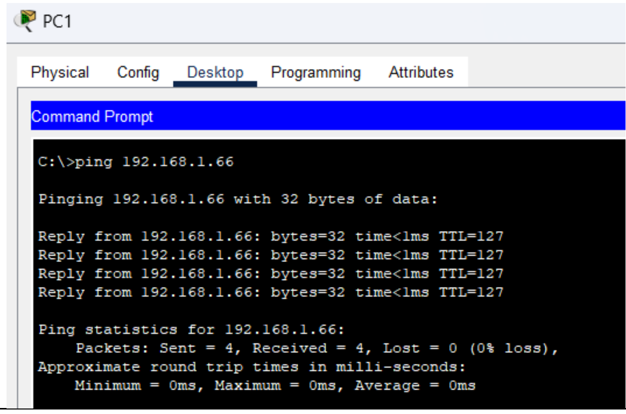
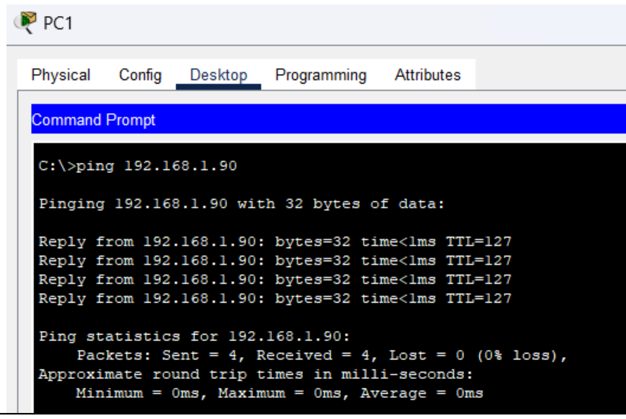
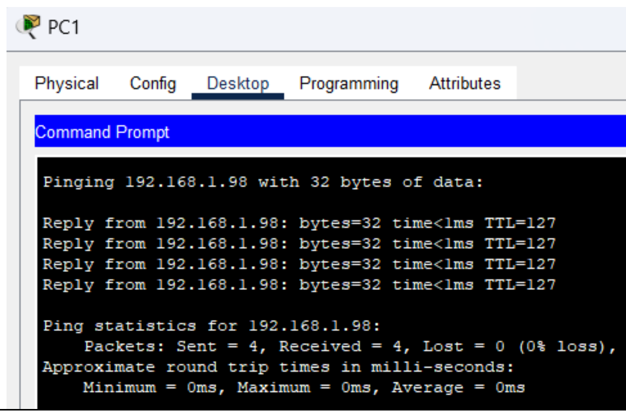
Configurations for PC90 in the Digital Forensics Lab:

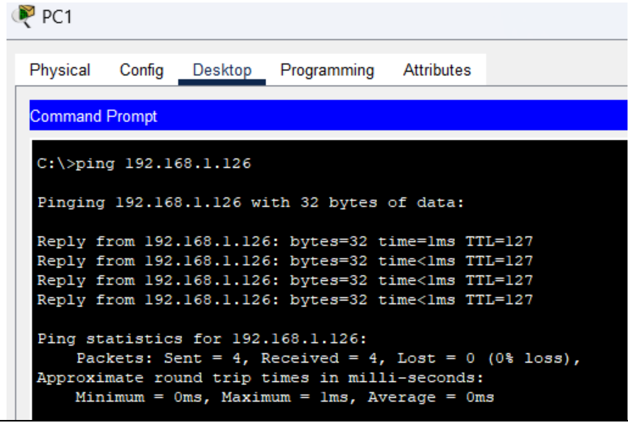
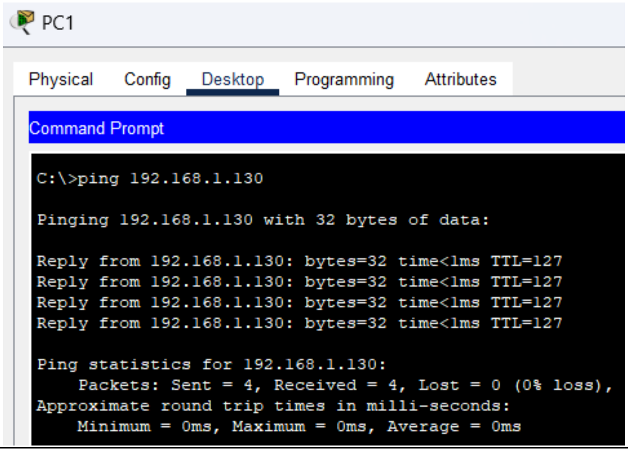
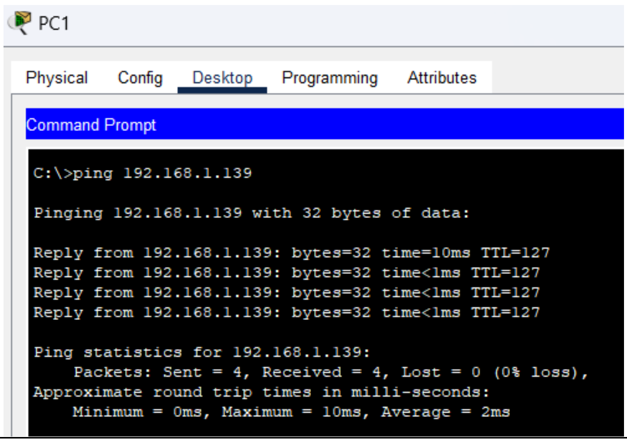




Ping Testing:

Table: Showing testing with command ping to every PC from source PC1.

Source	Destination	Screenshot
(PC1) 192.168.1.2	(PC30) 192.168.1.31	
(PC1) 192.168.1.2	(PC31) 192.168.1.66	
(PC1) 192.168.1.2	(PC55) 192.168.1.90	
(PC1) 192.168.1.2	(PC56) 192.168.1.98	

(PC1) 192.168.1.2	**(PC80) 192.168.1.126**	
(PC1) 192.168.1.2	**(PC81) 192.168.1.130**	
(PC1) 192.168.1.2	**(PC90) 192.168.1.139**	

3. Evaluation:

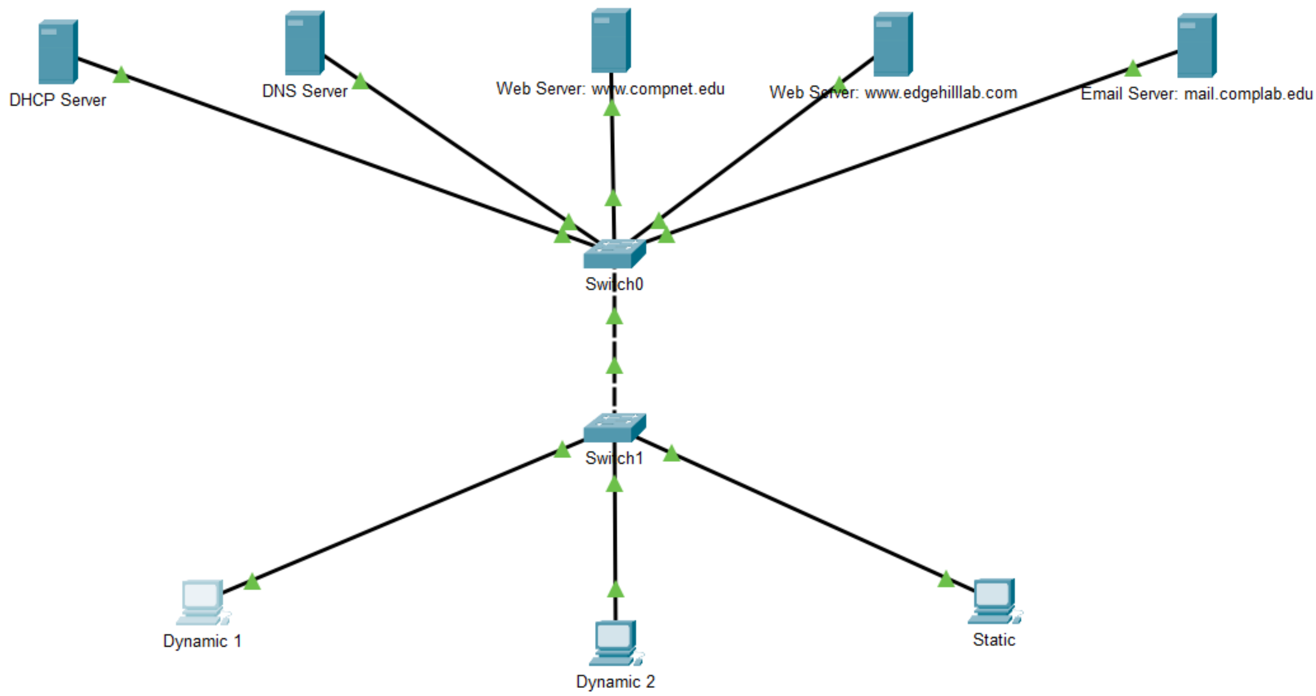
Overall, the network meets the lab's requirements, and although not all the devices are connected, I have simulated this by connecting the hosts to the opposite ends of IP address ranges. All the testing works and meets the requirements with no errors between testing the different hosts.

5. Lab Report 4: Application

5.1 Introduction

In this lab, I set up three PCs with two dynamic IP addresses and one with static. These PCs were connected to a network of different types of servers through two switches. These include two Email, a Web server, a DNS server and a DHCP server. Finally, after setting up the network, I documented my setup testing.

5.2 Answer to Questions

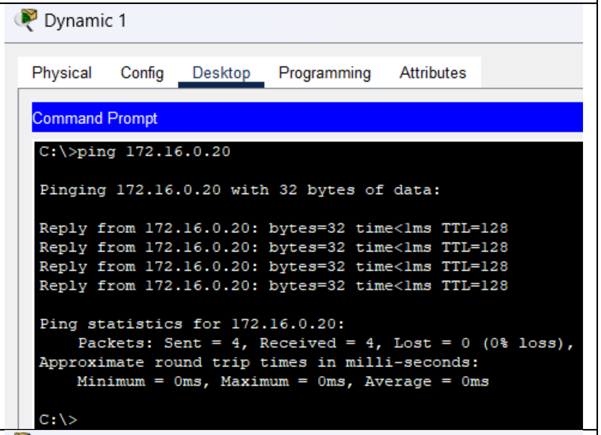
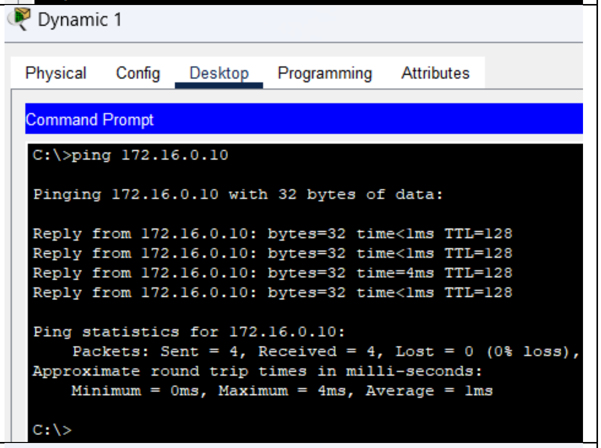
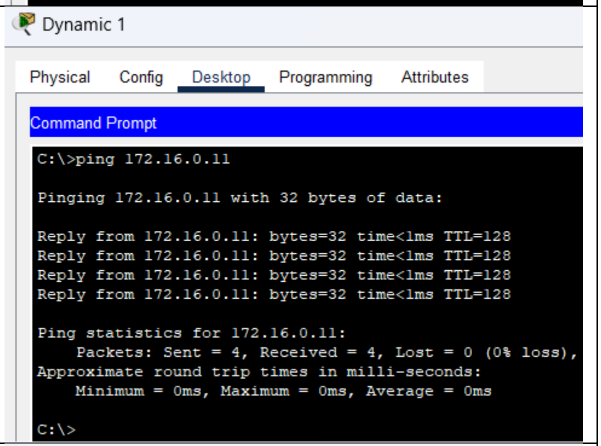
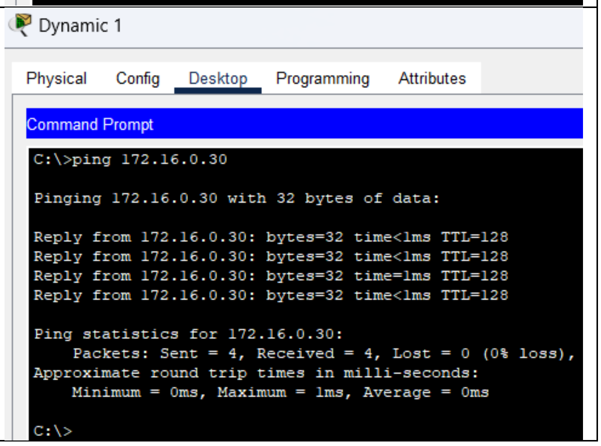


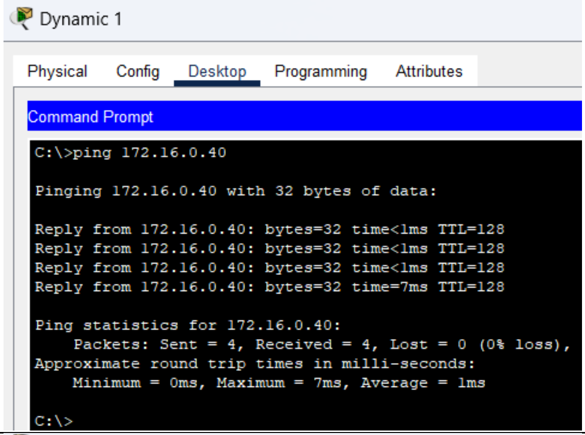
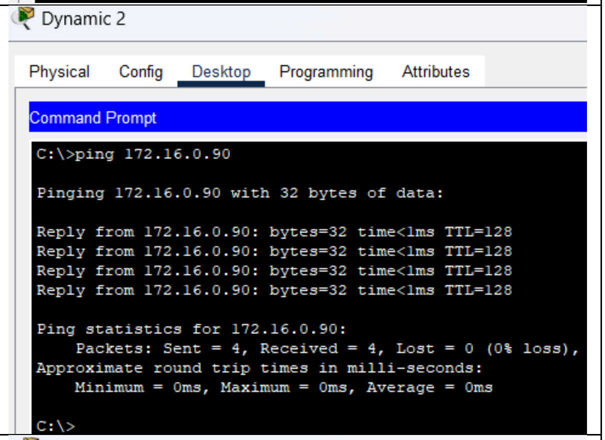
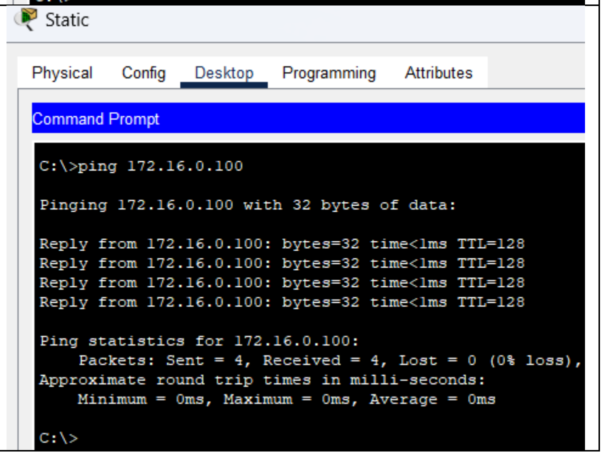
Questions – Verify Connectivity

Question 1: Ping (ICMP)

Ping is a simple echo query and response message which is used to see if another device is reachable over the network. A successful ping means both devices are able to communicate and are reachable. When a ping request is sent, it sends data packets across the network, usually four, unless specific parameters state otherwise, and once the packets are received, they are counted; if any are lost, a packet loss is calculated (Goralski, 2017).

Table: Showing testing with command ping to all different devices on the network.

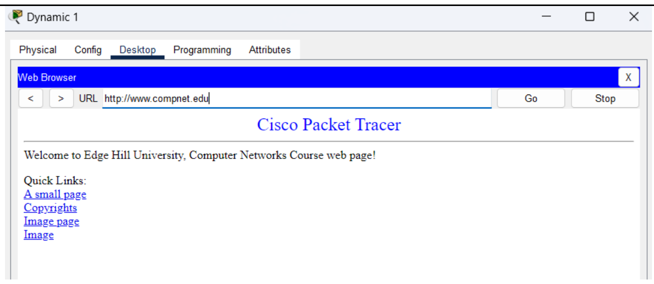
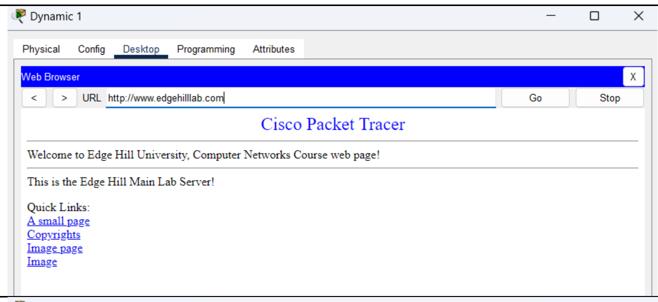
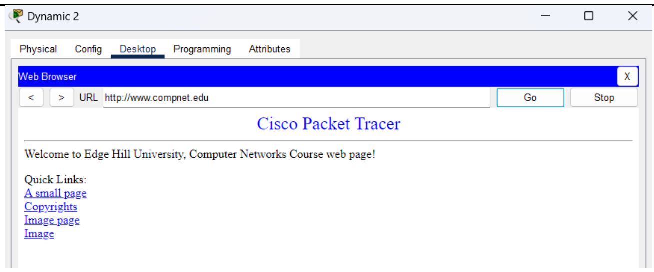
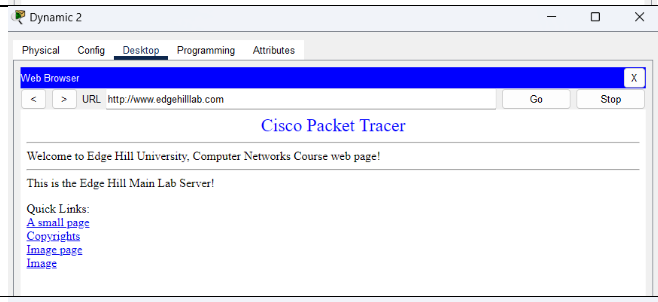
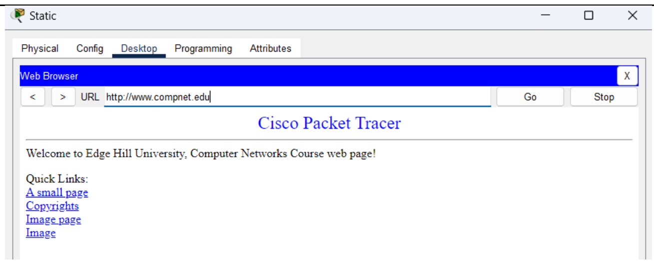
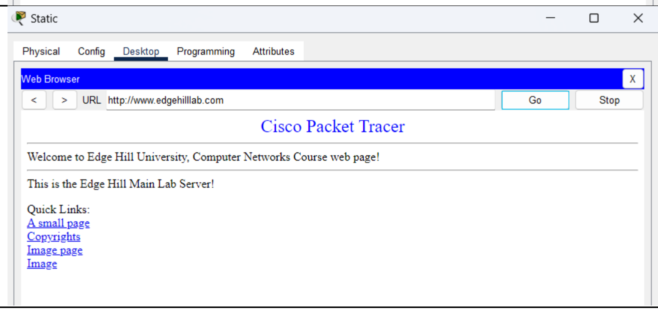
Host	**Receiver**	**Screenshot**
Dynamic 1	172.16.0.20 Web Server: www.compnet.edu	
172.16.0.100 Dynamic 1	172.16.0.10 DCHP Server	
172.16.0.100 Dynamic 1	172.16.0.11 DNS Server	
172.16.0.100 Dynamic 1	172.16.0.30 Web Server: www.edgehilllab.com	

<table>
<tr><td>172.16.0.100
Dynamic 1</td><td>172.16.0.40
Email Server: mail.complab.edu</td><td>
</td></tr>
<tr><td>172.16.0.101
Dynamic 2</td><td>172.16.0.90
Static</td><td>
</td></tr>
<tr><td>172.16.0.90
Static</td><td>172.16.0.100
Dynamic 1</td><td>
</td></tr>
</table>

Question 2: Web Browser (HTTP)

HTTP (HyperText Transfer Protocol) has been the primary standard for communication between web servers and web browsers over the internet since the 1990s. HTTP has improved over time, and the original version, HTTPS, was a simple protocol for transferring raw data across the internet (R. Fielding, 1999).

Table: Showing the client computers using the 2 web servers.

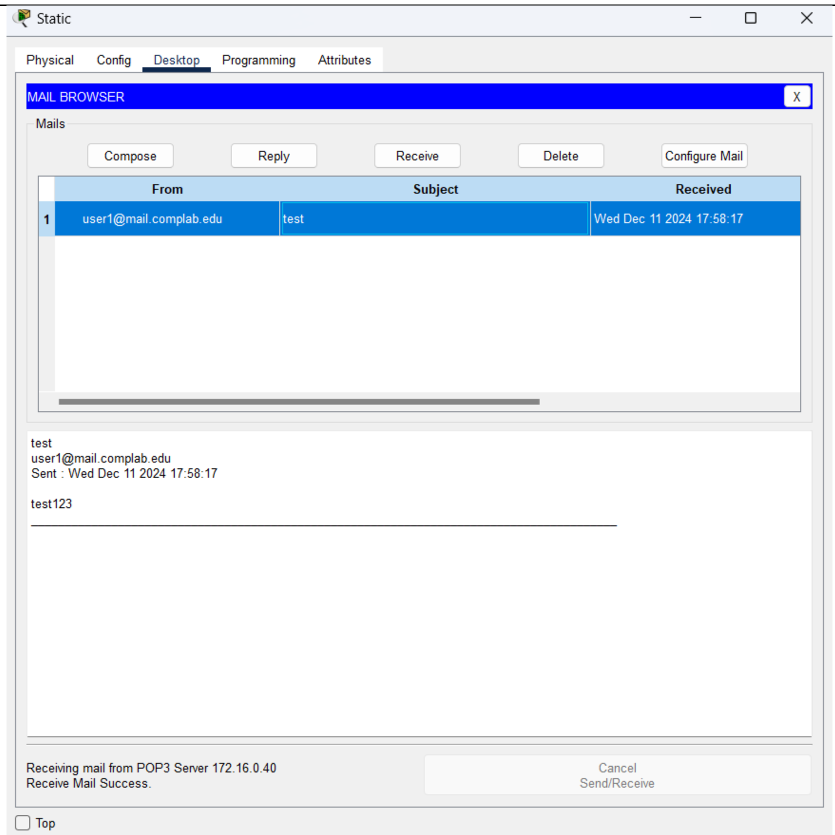
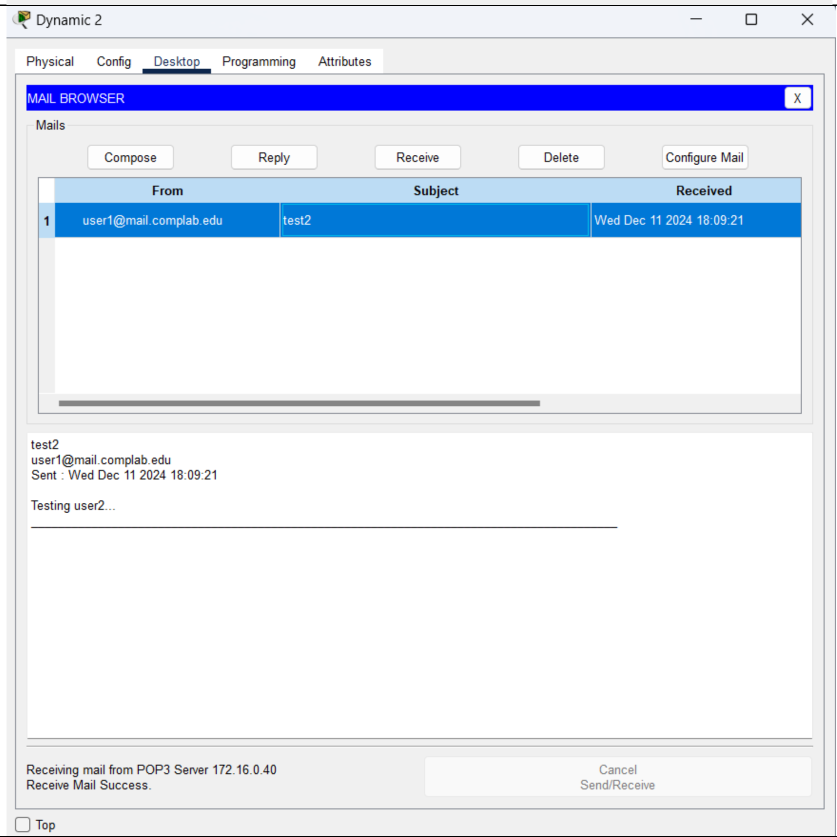
Client Computer	www.compnet.edu	www.edgehilllab.com
Dynamic 1		
Dynamic 2		
Static		

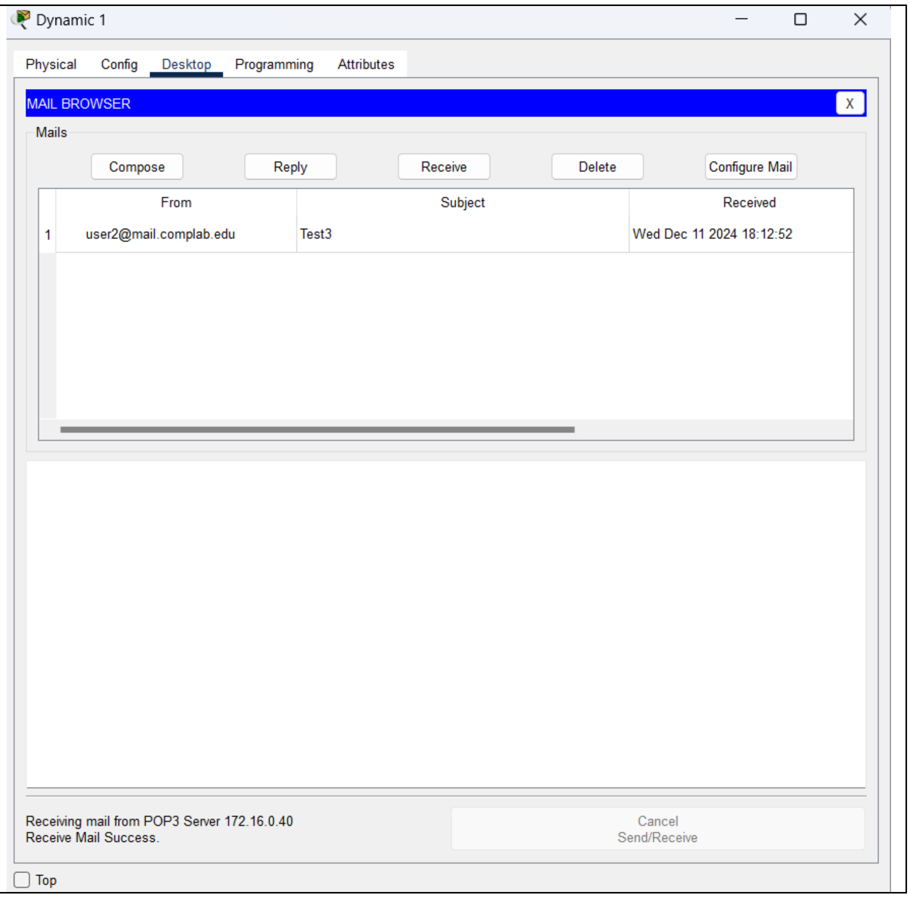
Question 3: Email (SMTP)

SMTP (Simple Mail Transfer Protocol) is a TCP/IP that exchanges data between servers over the network regardless of their underlying hardware or software. While it is not used for receiving data, like POP3, it provides a standardised method for delivering emails to the email provider's server and a separate protocol is used to retrieve that email so the recipient can receive it (Cloudflare, n.d.), (Awati, 2024).

POP3 (Post Office Protocol 3) is the third version of the protocol, POP. The Protocol itself is relatively simple and allows for the download of mail from a server to the client. It also allows the user to view the emails within the mailbox, transfer and delete emails, and log out via server port 110. Because the protocol itself is so simple to set with little configuration, it leaves very little room for error (Heinlein, 2008).

Table: Showing the received email from the email sender.

<table>
<tr><th>Email Sender</th><th>Email Recipient</th><th>Screenshot</th></tr>
<tr><td>Dynamic 1/user1</td><td>Static/user3</td><td>
</td></tr>
<tr><td>Dynamic1/user1</td><td>Dynamic2/user2</td><td>
</td></tr>
</table>

Dynamic2/user2	Dynamic1/user1	

6. Lab Reports 5: Network Security

6.1 Introduction:

In my final lab, I covered the fundamentals of the different types of firewalls and where you would use them. Next, I covered how a firewall examines a packet and what a stateless firewall is. After that, I answered questions about which packets would and wouldn't be received by the server and which IP addresses were for which packets. Finally, I discussed the advantages and disadvantages of application-level proxy compared with packet filtering firewalls, the purpose of the honey pot for catching attackers and why the bastion host needs to be highly secured.

6.2 Answer to Questions:

Activity 1:

1. Is the firewall software or hardware? Could it be a combination of both?

   A firewall can be network-based hardware (physical), host-based (software) or a combination of both. While software firewalls provide adaptable and easy-to-manage firewalls, they do take up resources from other devices. The benefit of hardware firewalls is that this doesn't happen as they are their own hardware entity; however, they usually have a more significant upfront cost (Fortinet, 2024), (Anon., 2024).

2. What data does the firewall monitor?

   A firewall acts as a security guard for a private network from outside traffic, monitoring all incoming and outgoing packets as they must pass through it. A firewall examines each packet, accepts the legitimate packets, and discards the ones which don't meet the firewall configuration (Liu, 2010)

3. John has 5 PCs at home, and he wants to protect all of them. What type of firewall should be used?

   As John is protecting multiple devices on a network, the best-suited firewall would be a physical network-based router firewall. This firewall will work as the first point of defence from the internet to the home network. A physical hardware firewall stops the need to dedicate additional hardware resources and set up software on each computer, as a software firewall would require (McCart, 2024).

4. John has a laptop and uses it in different locations such as work, hotels and home. What type of firewall should be used?

   Because John only needs to protect his laptop, the best firewall would be a host-based software firewall. Software Host-based firewalls use the existing operating system on a device and are simple downloadable software, making an easy setup/maintenance process. (Ot, 2023).

5. In a home network environment where you have 3 PCs, iPads, iPhones and a router. Which of the following is the best option to install a firewall (PC, router, switch) to protect the network?

   The best option to install a firewall is on the router because this is the first entry point to the local network and, therefore, protects all the other devices within the local network.

6. In the lab, one of the computers has been infected by malware by an employee using his infected USB. Do you think a firewall can protect the PCs?

   Firewalls are designed to monitor incoming and outgoing traffic; a firewall does not scan for malware via USB to local devices. As the malware is on a USB device, this bypasses the network entirely and defeats the object of a firewall.

Activity 2:

1. What does a packet filtering firewall examine in a packet?

   A packet filter decides if a packet meets the requirements to enter the network. It does this by examining the source and destination of the IP address and port numbers, Data transfer protocols used in transmission, header flags, and the NIC interface (NordLayer, 2024).

2. What does a stateless firewall mean?

   Stateless firewalls are the most basic type of firewall; they rely on rules on the access control list and make decisions based on each packet, not storing any information about each packet state or reason for the connection, only inspecting the information within the packet header to justify if they match the configuration rules (Cobb, 2024).

3. Does the packet filter examine the payload of a packet?

   No, the packet header contains information about the packet, including the IP source and destination address, the protocol and the port number. In contrast, the packet payload only includes the data to be transferred (Wright, 2023).

Activity 3:

1. What are the IP addresses of the client and server?

   Client: 192.168.51.50
   Server: 172.16.3.4

2. What is the source IP, source port, destination IP and destination port of the first packet?

Source IP: 192.168.51.50
Source Port: 3264
Destination IP: 172.16.3.4
Destination Port: 1525

3. Who sent the first packet? Client or server? Did the packet pass?

   The Client sent the first packet, and the first packet passed because a packet had been sent back to the Client.

4. What is the source IP, source port, destination IP and destination port of the second packet? Find the matching numbers between packet 1 and packet 2.

   Source IP: 172.16.3.4
   Source Port: 1525
   Destination IP: 192.168.51.50
   Destination Port: 3264

5. What is the source IP, source port, destination IP and destination port of the third packet? Find the matching and mismatching numbers between packet 1 and packet 3.

   Source IP: 172.16.3.4
   Source Port: 1525
   Destination IP: 192.168.51.50
   Destination Port: 2049
   Mismatching: The Destination Port does not match the source port on packet 1.

6. Why was the last packet blocked? How did the firewall make this decision? Did the firewall have to remember the first packet?

   The firewall remembers the original packet information from the initial packet 1, and because the destination port number for the Client doesn't match the original packet source port, the 3rd packet, in this case, is blocked.

7. Explain why a stateful firewall requires more resources compared to a stateless one.

   A stateful firewall requires more resources due to the recording of information about ongoing network connections. This allows the firewall to make more intelligent decisions about which packets to allow and block (Ot, 2023).

Activity 4:

1. Discuss the advantages and disadvantages of application-level proxy compared with packet filtering firewalls.

   An advantage of Packet Filtering is that they are faster than Application-level at making packet decisions as it doesn't require deep packet inspection; however, a disadvantage is that it is less secure because of the lack of DPI (Ayuya, 2023).

An advantage of Application Level is that they are more secure than a Packet Filtering Firewall as they use deep packet inspection. However, a disadvantage is that because of the DPI, it takes longer to decide on the packet inspection, therefore making them slower (Partida, 2023).

An advantage of Packet Filtering Firewalls is that they are cost-effective and easy to use as they only need one filtering router compared with the application level, which is more expensive. A disadvantage of Packet Filtering Firewalls is that while they are easy to use, they are challenging to set up and lack the logging capabilities of the Application Level (Ayuya, 2023)

An advantage of the Application Level is that they have a simple traffic logging system that records every traffic transaction that goes across the server compared to the Packet Filtering Firewall, which lacks this logging system. A disadvantage of the Application Level is that each protocol in the network needs a proxy application to operate (Partida, 2023).

2. What is the purpose of honeypots?
   Honeypots work by baiting attackers away from the legitimate target, and if the attackers fall for the trap, they can be tracked, and their behaviours are analysed to make future networks more secure by prioritising and focusing on certain weak spots. An example of this could be a port purposely left open to lead the attackers into the trap (Kaspersky, 2024).

3. Explain why the bastion host needs to be highly secured by system administrators compared to other computers in the private networks.

   Bastion host needs to be highly secure as it sits on the edge of the local network and public network, and it decides what can enter and can't. Because it is on the edge of the public network and its purpose is to determine what can join the network, it is a prime target for attackers to try to gain unauthorised access or attempt data breaches. Because of this, administrators need to make sure it is secured (Krysińska, 2024).

References

Anon., 2024. *Hardware Firewalls vs. Software Firewalls.* [Online]
Available at: https://www.paloaltonetworks.co.uk/cyberpedia/hardware-firewall-vs-software-firewall
[Accessed 12 12 2024].

Awati, R., 2024. *What is SMTP (Simple Mail Transfer Protocol)?.* [Online]
Available at: https://www.techtarget.com/whatis/definition/SMTP-Simple-Mail-Transfer-Protocol
[Accessed 11 12 2024].

Ayuya, C., 2023. *What Is a Packet-Filtering Firewall? Is It Right For You?.* [Online]
Available at: https://www.enterprisenetworkingplanet.com/security/packet-filtering-firewall/
[Accessed 12 12 2024].

Chai, W., 2021. *HTTP (Hypertext Transfer Protocol).* [Online]
Available at: https://www.techtarget.com/whatis/definition/HTTP-Hypertext-Transfer-Protocol
[Accessed 26 11 2024].

Cloudflare, n.d. *What is the Simple Mail Transfer Protocol (SMTP)?.* [Online]
Available at: https://www.cloudflare.com/en-gb/learning/email-security/what-is-smtp/
[Accessed 11 12 2024].

Cobb, M., 2024. *Stateful vs. stateless firewalls: Understanding the differences.* [Online]
Available at: https://www.techtarget.com/searchsecurity/answer/How-do-stateful-inspection-and-packet-filtering-firewalls-differ
[Accessed 12 12 2024].

Fortinet, 2024. *What Is A Hardware Firewall? Hardware vs Software Firewalls.* [Online]
Available at: https://www.fortinet.com/uk/resources/cyberglossary/hardware-firewalls-better-than-software
[Accessed 12 12 2024].

GeeksforGeeks, 2024. *How to Calculate a Subnet Mask from IP Address?.* [Online]
Available at: https://www.geeksforgeeks.org/how-to-calculate-a-subnet-mask-from-ip-address/
[Accessed 10 12 2024].

Goralski, W., 2017. *The Illustrated Network : How TCP/IP Works in a Modern Network.* Chantilly: Elsevier Science & Technology.

Heinlein, P. a. H. P., 2008. *The book of IMAP : building a mail server with Courier and Cyrus.* Munich, San Francisco: s.n.

Internet Society, 2015. *TLS Basics.* [Online]
Available at: https://www.internetsociety.org/deploy360/tls/basics/
[Accessed 12 12 2024].

Kaspersky, 2024. *What is a honeypot?.* [Online]
Available at: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot
[Accessed 12 12 2024].

Kerner, S. M., 2021. *Internet Protocol.* [Online]
Available at: https://www.techtarget.com/searchunifiedcommunications/definition/Internet-Protocol
[Accessed 26 11 2024].

Krysińska, J., 2024. *What is a bastion host and does your business need it?.* [Online]
Available at: https://nordlayer.com/blog/bastion-host/
[Accessed 12 12 2024].

Liu, A. X., 2010. Background and Motivation. In: *Firewall Design and Analysis.* Singapore: ProQuest Ebook Central, p. 1.

McCart, C., 2024. *What is a Router Firewall and how does it work?.* [Online]
Available at: https://www.comparitech.com/antivirus/what-is-a-router-firewall/
[Accessed 12 12 2024].

NordLayer, 2024. *What is a packet filtering firewall?.* [Online]
Available at: https://nordlayer.com/learn/firewall/packet-filtering/
[Accessed 12 12 2024].

Ot, A., 2023. *What is a Host-Based Firewall?.* [Online]
Available at: https://www.datamation.com/security/what-is-a-host-based-firewall/
[Accessed 12 12 2024].

Ot, A., 2023. *What is a Host-Based Firewall?.* [Online]
Available at: https://www.datamation.com/security/what-is-a-host-based-firewall/
[Accessed 12 12 2024].

Partida, D., 2023. *What Is an Application-Level Gateway? How ALGs Work.* [Online]
Available at: https://www.enterprisenetworkingplanet.com/security/application-level-gateway/
[Accessed 12 12 2024].

R. Fielding, U. I. J. G. C. J. C. M. C. H. F. W. L. M. X. P. L. M. T. B.-L. W., 1999. *Hypertext Transfer Protocol -- HTTP/1.1.* [Online]
Available at: https://www.w3.org/Protocols/HTTP/1.1/rfc2616.pdf
[Accessed 11 12 2024].

Thomas, A., 2014. *Subnetting an IP Address.* [Online]
Available at: https://d12vzecr6ihe4p.cloudfront.net/media/966010/wp-subnetting-an-ip-address.pdf
[Accessed 10 12 2024].

Wright, G., 2023. *packet filtering.* [Online]
Available at: https://www.techtarget.com/searchnetworking/definition/packet-filtering#:~:text=The%20packet%20header%20contains%20information,based%20on%20the%20header%20information.
[Accessed 12 12 2024].

Yasar, K., 2024. *Transmission Control Protocol (TCP).* [Online]
Available at: https://www.techtarget.com/searchnetworking/definition/TCP
[Accessed 26 11 2024].