



Assignment Networking

L. Sachintha Prabodhi Liyanage – Networking – HND Computing –
Batch – 05 | RAT/A – 004133
ESOFT METRO COLLEGE | BATCH – 05

Acknowledgment

I would like to express my sincere gratitude to my lecturer Mr. P. Pavithra Piyumal, for their invaluable guidance and support throughout the course. Their expertise and passion for the subject have inspired me to strive for excellence.

I would also like to thank my family and friends for their unwavering love and encouragement, which has kept me motivated during this challenging time. Without their support, I would not have been able to complete the assignment. Once again, thank you to everyone who has helped me on this journey.

Thank you very much...!

Table of Contents

Acknowledgment	1
Table of Contents	2
List of Figures	5
List of Tables	9
Activity 01	10
1.1 The existing system at VividZone	10
1.2 An Explanation of	11
1.2.1 What is Network	11
1.2.1.1 Network Principles	12
1.2.1.2 Data Communication	12
1.2.1.3 Data Flow	12
1.2.2 Network System Types	13
1.2.2.1 Peer-to-peer	13
1.2.2.2 Client-Server	14
1.2.3 Types of Networks	15
1.2.3.1 LAN - Local Area Network	16
1.2.3.2 WAN – Wide Area Network	16
1.2.3.3 SAN – Storage Area Network	17
1.2.3.4 CAN - Controller Area Network	18
1.2.3.5 PAN - Personal Area Network	19
1.2.3.6 VPN - Virtual Private Network	19
1.2.4 Standards	20
1.2.5 Network Models	22
1.2.5.1 The OSI Model	22
1.2.5.2 The TCP/IP Model	25
1.2.5.3 Differences between the OSI and TCP/IP models	26
1.2.5.4 Similarities between ISO OSI Model and TCP/IP Model	27
1.2.6 Protocols	28
1.2.7 Network Topologies	30
1.2.7.1 Physical Topology	30
1.2.7.2 Logical Topology	36
1.2.8 Transmission Medium	37

1.2.8.1	Wired Media	37
1.2.8.2	Wireless Media	40
1.2.9	Bandwidth.....	40
1.2.9.1	Bandwidth Requirements.....	41
1.2.9.2	Latency.....	41
1.2.10	Effectiveness of network systems.....	41
1.2.11	Networking Devices	42
1.2.11.1	Hub.....	42
1.2.11.2	Switch.....	42
1.2.11.3	Router.....	43
1.2.11.4	Bridge.....	43
1.2.11.5	Gateway.....	44
1.2.11.6	Modem	44
1.2.11.7	Repeater.....	45
1.2.11.8	Access Point.....	45
1.2.11.9	Firewall.....	46
1.2.12	Types of Servers	47
1.2.12.1	Web Server.....	47
1.2.12.2	File Server	47
1.2.12.3	Database Server.....	48
1.2.12.4	Server Selection Requirement.....	48
1.2.12.5	Server Brands Documentation	49
1.2.13	Workstation	50
1.2.14	Networking Software.....	51
1.2.14.1	Client Software.....	51
1.2.14.2	Server Software	51
1.2.14.3	Software Firewall	51
1.2.15	Benefits of Computer Networking	52
1.2.16	Constraints of Computer Networking.....	53
Activity 02	54
2.1	Blueprint of LAN	54
2.1.1	Technical Requirements.....	54
2.1.2	Proposed Topology	54
2.1.3	BYOD (Bring Your Own Device) policies.....	56

2.2	Selection of Accessories, Quality of Services and Security Requirements	56
2.2.1	Dell Precision Tower 7920 Workstation.....	56
2.2.2	Cisco Aironet 3800 Series Access Point.....	57
2.2.3	Cisco ISR 4000 Series Router.....	58
2.2.4	Cisco Catalyst 9300 Series Switches	59
2.2.5	HP EliteDesk 800 G6 Desktop PC.....	59
2.2.6	HP LaserJet Pro MFP M521dn	60
2.2.7	AmazonBasics RJ45 Cat-5e Ethernet Patch Cable	61
2.3	Redesigned Network of Enclave Films	61
2.4	IP Allocation Table	62
2.5	Install & configure network services and applications of your choice	63
2.6	Conduct a test and evaluate the design to meet the requirements and analyses user feedback	66
2.7	Suggest a maintenance schedule to support the networked system	71
Activity 03	72
3.1	Implement a networked system based on a prepared design	72
3.1.1	PC Configuration	72
3.1.2	Switch Configuration	76
3.1.3	Router Configuration	79
3.2	Conduct verification & Analyse test results against expected outcomes.....	83
3.2.1	Ping	83
3.2.2	Traceroute	112
3.2.3	Telnet	113
3.2.4	SSH	117
3.2.5	Ipconfig	121
3.3	Explore system's capabilities for device growth and communication	129
Harvard Referencing	131

List of Figures

Figure 1 Network	11
Figure 2 Data flow	13
Figure 3 Peer-to-Peer	14
Figure 4 Client-Server.....	14
Figure 5 Local Area Network	16
Figure 6 Wide Area Network.....	17
Figure 7 Storage Area Network	18
Figure 8 Controller Area Network	18
Figure 9 Personal Area Network.....	19
Figure 10 Virtual Area Network	20
Figure 11 OSI Model	23
Figure 12 TCP/IP Model.....	25
Figure 13 Ring Topology	32
Figure 14 Bus Topology	33
Figure 15 Star Topology	34
Figure 16 Mesh Topology.....	35
Figure 17 Hybrid Topology	36
Figure 18 Coaxial Cable	38
Figure 19 Unshielded Twisted Pair Cable	39
Figure 20 Shielded Twisted Pair Cable	39
Figure 21 Fibber Optics Cable.....	40
Figure 22 Hub	42
Figure 23 Switch	43
Figure 24 Router	43
Figure 25 Bridge	44
Figure 26 Gateway.....	44
Figure 27 Modem.....	45
Figure 28 Repeater.....	45
Figure 29 Access Point	46
Figure 30 Firewall.....	46
Figure 31 Types of Servers	47

Figure 32 Blueprint of LAN	54
Figure 33 Dell Precision Tower 7920 Workstation	57
Figure 34 Cisco Aironet 3800 Series Access Point	58
Figure 35 Cisco ISR 4000 Series Router	58
Figure 36 Cisco Catalyst 9300 Series Switches.....	59
Figure 37 HP EliteDesk 800 G6 Desktop PC	60
Figure 38 HP LaserJet Pro MFP M521dn.....	61
Figure 39 AmazonBasics RJ45 Cat-5e Ethernet Patch Cable	61
Figure 40 Redesign Network	62
Figure 41 VMware Workstation Pro Setup	64
Figure 42 VMware End User License Agreement.....	64
Figure 43 Custom Setup.....	65
Figure 44 Installation of VMware Workstation Pro	65
Figure 45 VMware Installation Complete	66
Figure 46 User Feedback Form - i	67
Figure 47 User feedback form - ii.....	68
Figure 48 User feedback form - iii.....	69
Figure 49 User feedback form - iv	70
Figure 50 PC Configuration (Sales).....	72
Figure 51 PC Configuration (General Office & Manager's).....	73
Figure 52 PC Configuration (Administration).....	73
Figure 53 PC Configuration (Accounts)	74
Figure 54 PC Configuration (Customer & Reception Area)	74
Figure 55 PC Configuration (Media Development & Storage).....	75
Figure 56 PC Configuration (Office).....	76
Figure 57 Switch Configuration (Naming VLANs)	77
Figure 58 Show VLANs	78
Figure 59 Switch Configuration (Naming VLANs)	78
Figure 60 Show VLANs	79
Figure 61 Router Configuration (Building A)	80
Figure 62 Shows the IP route (Building A)	81
Figure 63 Router Configuration (Building B)	81
Figure 64 shows the IP route (Building B)	82
Figure 65 Test case pinging from Sales Department to General Office & Manager's	84

Figure 66 Test case pinging from Sales Department to Administration Department.....	84
Figure 67 Test case pinging from Sales Department to Accounts Department.....	85
Figure 68 Test case pinging from Sales Department to Customer & Reception Area	86
Figure 69 Test case pinging from Sales Department to Media Development & Storage..	87
Figure 70 Test case pinging from Sales Department to Office.....	88
Figure 71 Test case pinging from General Office & Manager's to Sales Department	88
Figure 72 Test case pinging from General Office & Manager's to Administration Department.....	89
Figure 73 Test case pinging from General Office & Manager's to Accounts Department	90
Figure 74 Test case pinging from General Office & Manager's to Customer & Reception Area.....	90
Figure 75 Test case pinging from General Office & Manager's to Media Development & Storage	91
Figure 76 Test case pinging from General Office & Manager's to Office.....	92
Figure 77 Test case pinging from Administration to Sales Department.....	92
Figure 78 Test case pinging from Administration to General Office & Manager's	93
Figure 79 Test case pinging from Administration to General Accounts Department	94
Figure 80 Test case pinging from Administration to General Customer & Reception Area	94
Figure 81 Test case pinging from Administration to Media Development & Storage.....	95
Figure 82 Test case pinging from Administration to Office.....	96
Figure 83 Test case pinging from Accounts to Sales Department.....	96
Figure 84 Test case pinging from Accounts to General Office & Manager's.....	97
Figure 85 Test case pinging from Accounts to Administration.....	98
Figure 86 Test case pinging from Accounts to Customer & Reception Area	98
Figure 87 Test case pinging from Accounts to Media Development & Storage	99
Figure 88 Test case pinging from Accounts to Office	99
Figure 89 Test case pinging from Customer & Reception Area to Sales Department	100
Figure 90 Test case pinging from Customer & Reception Area to General Office & Manager's	101
Figure 91 Test case pinging from Customer & Reception Area to Administration	101
Figure 92 Test case pinging from Customer & Reception Area to Accounts	102
Figure 93 Test case pinging from Customer & Reception Area to Media Development & Storage	103

Figure 94 Test case pinging from Customer & Reception Area to Office	103
Figure 95 Test case pinging from Media Development & Storage to Sales Department	104
Figure 96 Test case pinging from Media Development & Storage to General Office & Manager's	105
Figure 97 Test case pinging from Media Development & Storage to Administration....	105
Figure 98 Test case pinging from Media Development & Storage to Accounts	106
Figure 99 Test case pinging from Media Development & Storage to Customer & Reception Area.....	107
Figure 100 Test case pinging from Media Development & Storage to Office	107
Figure 101 Test case pinging from Office to Sales Department.....	108
Figure 102 Test case pinging from Office to General Office & Manager's.....	109
Figure 103 Test case pinging from Office to Administration.....	110
Figure 104 Test case pinging from Office to Accounts	110
Figure 105 Test case pinging from Office to Customer & Reception Area	111
Figure 106 Test case pinging from Office to Media Development & Storage	111
Figure 107 Displays traceroute (Building A).....	112
Figure 108 Displays traceroute (Building B).....	113
Figure 109 Telnet (Building A)	114
Figure 110 Result of telnet (Building A)	115
Figure 111 Telnet (Building B).....	116
Figure 112 Result of telnet (Building B)	117
Figure 113 SSH (Building A)	118
Figure 114 Result of SSH (Building A).....	119
Figure 115 SSH (Building B)	120
Figure 116 Result of SSH (Building B).....	121
Figure 117 Displays ipconfig for Sales Department PC	122
Figure 118 Displays ipconfig for General Office & Manager's Department PC	123
Figure 119 Displays ipconfig for Administration Department PC	124
Figure 120 Displays ipconfig for Accounts Department PC	125
Figure 121 Displays ipconfig for Customer & Reception Area Department PC.....	126
Figure 122 Displays ipconfig for Media Development & Storage Department PC	127
Figure 123 Displays ipconfig for Office Department PC	128

List of Tables

Table 1 Network System Comparison	15
Table 2 IEEE Standards	21
Table 3 Differences OSI & TCP/IP Model	27
Table 4 Bandwidth Measurement	41
Table 5 Server Brands Documentation	50
Table 6 List of Hardware Devices	56
Table 7 IP Allocation Table	63
Table 8 Maintenance Schedule	71

Activity 01

1.1 The existing system at VividZone

Enclave Films is a well-known film production company that offers high-quality videos for download through the VividZone website. Recently, the Enclave Films management decided to merge with VividZone by adding more efficient staff and equipment to improve their services. However, the Enclave Films organization has experienced growth without a proper plan, which has proven to be a disadvantage for the company.

To improve its network infrastructure, Enclave Films should consider upgrading its Ethernet connection from Cat5e to Cat6e, which is faster and more efficient. Alternatively, they could use wireless connections, but Cat6e Ethernet is preferred due to its better system requirements and less likelihood of tangled wires.

Enclave Films should also avoid a flat network configuration, which can lead to security issues. Since the company has grown significantly after merging with Vivid Zone, a larger network system like WAN with better security measures would be more appropriate. Having minimal redundancy could result in the loss of important data in the event of a system failure, so the company should consider having a backup system.

Although there is a small wireless LAN occasionally used by managers and guests in Building B, this can also lead to security issues. Managers may have private information stored on their laptops that could be viewed by guests. Enclave Films could opt for a wired network instead since it is a smaller network and does not necessarily require a wireless connection, which would improve the speed in the area.

1.2 An Explanation of

1.2.1 What is Network

Computer networking refers to interconnected computing devices that can exchange data and share resources. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.

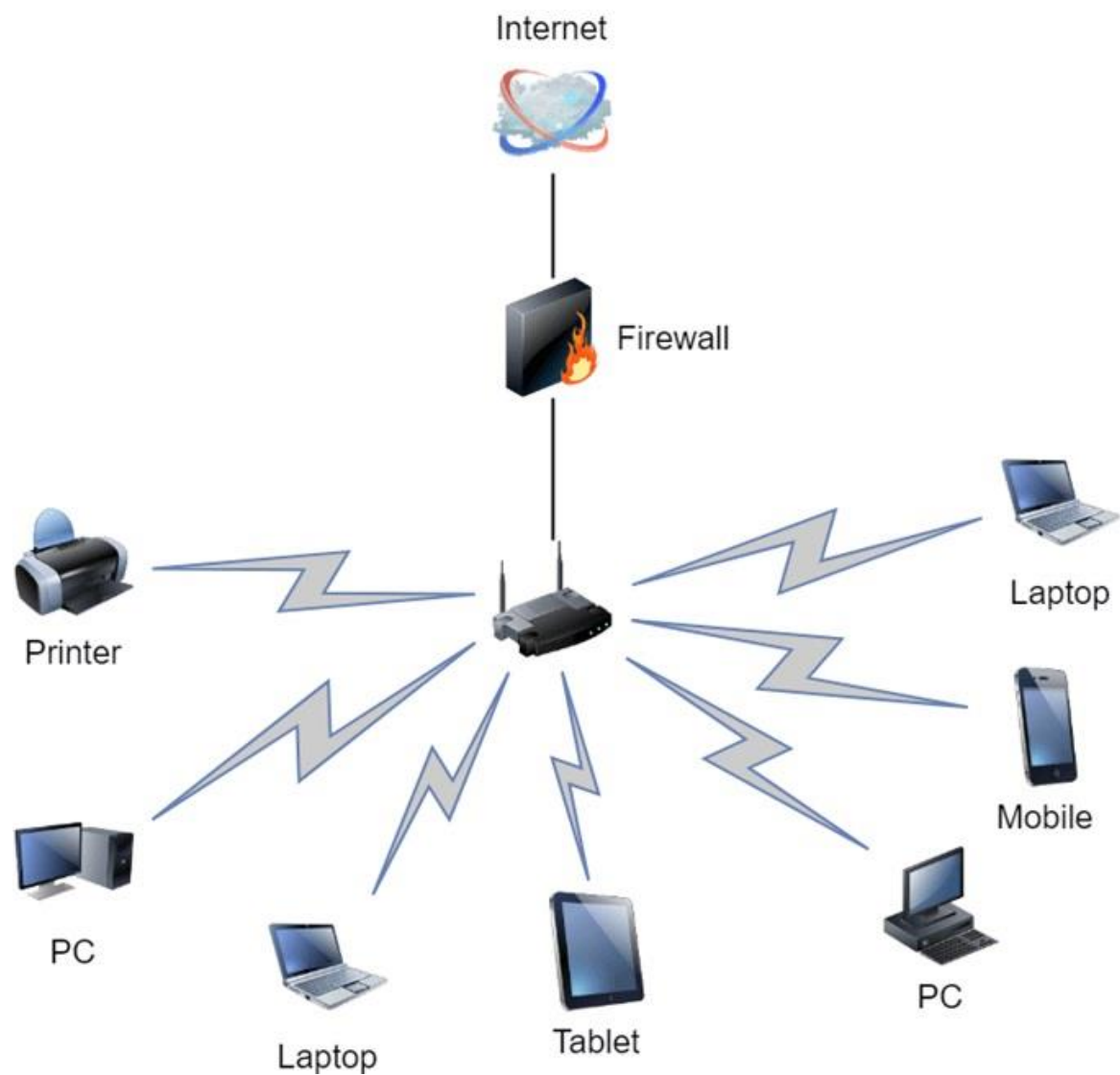


Figure 1 Network

1.2.1.1 Network Principles

Computer networks have changed the way we communicate with each other and the world around us. Networking has made our world much smaller over the past 20 years. The Internet consists of many large networks interconnected throughout the globe using standardized communication methods and values. There are systems in place everywhere to help out in our daily lives, which are connected through the Internet.

1.2.1.2 Data Communication

Sharing data between two or more devices can also be called data communication. For successful data communication, we should have the following parties on our network.

- **Sender:** The computer or the device that contains the data that we can send.
- **Receiver:** The computer or device that receives or can get data.
- **Transmission Medium:** The medium (wired or wireless) that we can use to send our data or receive our data is called transmission media.
- **Message:** The data that we communicate between computers or devices.
- **Protocols:** A set of rules that all the parties of the communication agreed on called protocols.

1.2.1.3 Data Flow

The term transmission mode defines the direction of data flow between two linked devices. The manner or way in which data is transmitted from one place to another is called Data Transmission Mode. There are three ways for transmitting data from one location to another.

- **Simplex**

On the simplex method, you will only be able to send or receive data.

E.g.: TV remote, Keyboard

- **Half duplex**

On half-duplex, you will be able to send data and also receive data. But you will not be able to send and receive data at the same time.

E.g.: Walkie-talkie

- **Full duplex**

On full-duplex, you will be able to send data and receive data, and also you will be able to do this at the same time.

E.g.: Telephone

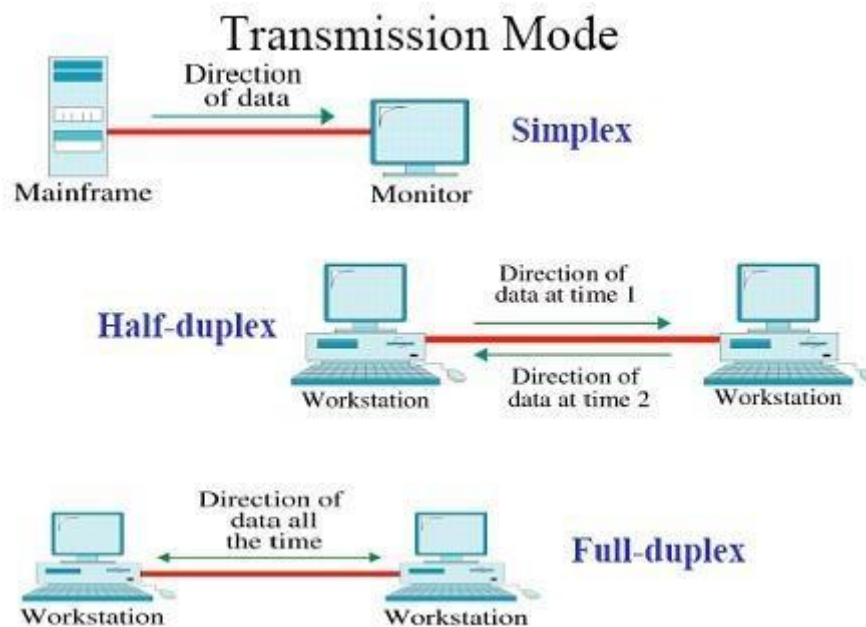


Figure 2 Data flow

1.2.2 Network System Types

1.2.2.1 Peer-to-peer

A peer-to-peer network is a simple network of computers where each node acts as a server and shares an equal workload, allowing for the sharing of large amounts of data.

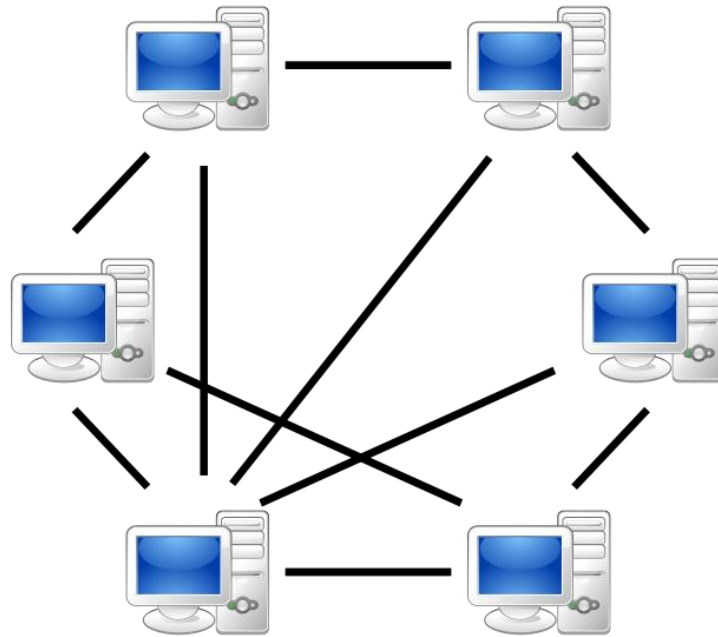


Figure 3 Peer-to-Peer

1.2.2.2 Client-Server

Client-server networking is a computer networking model that uses both client hardware devices and servers for specific functions.

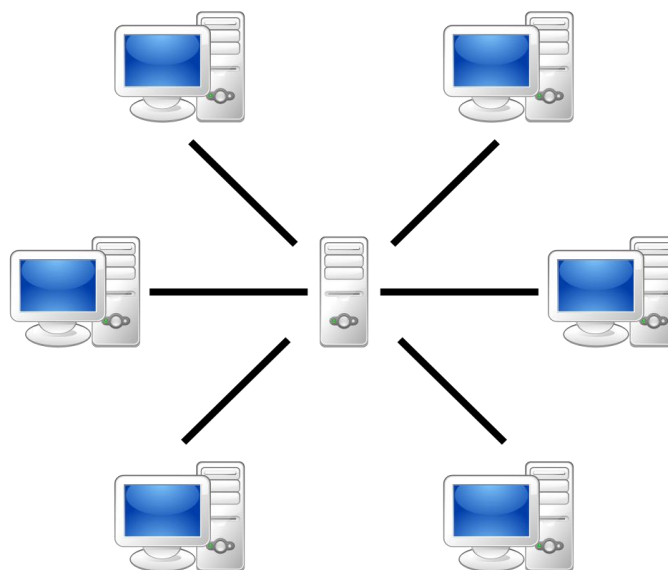


Figure 4 Client-Server

Peer-to-peer	Client-Server
Easy to set up	Difficult to set up
Less expensive to install	More expensive to install
Can be implemented on a wide range of operating systems	A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
More time-consuming to maintain the software being used (as computers must be managed individually)	Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	High levels of security are supported, all of which are controlled by the server. Such measures prevent the deletion of essential system files or the changing of settings
Ideal for networks with less than 10 computers	No limit to the number of computers that can be supported by the network
Does not require a server	Requires a server/ PC running a server operating system
Demands a moderate level of skill to administer the network	Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

Table 1 Network System Comparison

1.2.3 Types of Networks

A computer network is an interconnected system of devices that share information, data, and resources, with different levels of access and connectivity. Network types are classified based on purpose and size; types of networks are as follows.

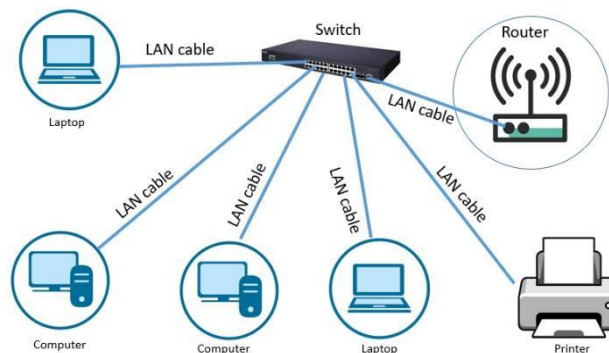
- LAN - Local Area Network

- WAN – Wide Area Network
- SAN – Storage Area Network
- CAN - Controller Area Network
- PAN - Personal Area Network
- VPN - Virtual Private Network

1.2.3.1 LAN - Local Area Network

A local area network is a network that we can create in a small or limited geographical area. This type of local area network is suitable for the location where we have to create a network with a small number of computers.

Local area networks are controlled by local network administrators and can transfer data with high speed and bandwidth.



Local Area Network

Figure 5 Local Area Network

1.2.3.2 WAN – Wide Area Network

A network located in a very large geographical area. The Internet can be called as largest wide area network in the world. But remember that wide area networks are a relatively slower network that has lower bandwidth than local area network. Also, wide area networks are costlier and more complex network types with more opportunities for the users.

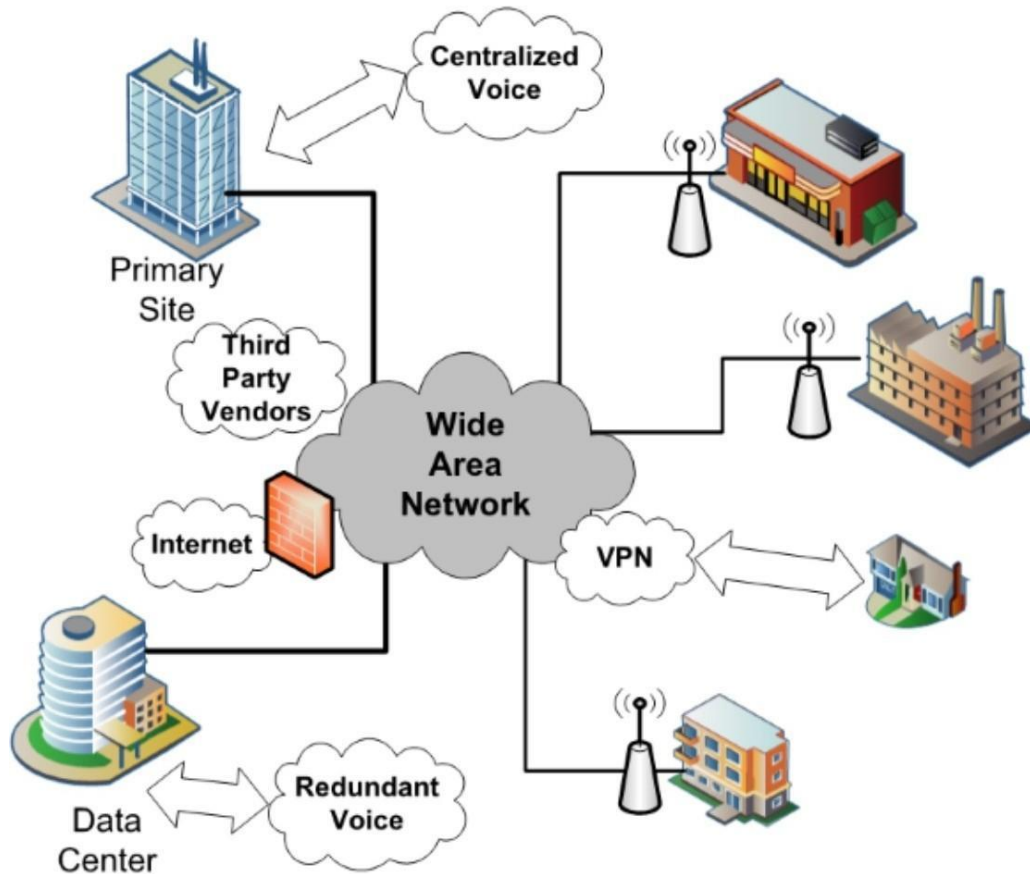


Figure 6 Wide Area Network

1.2.3.3 SAN – Storage Area Network

A network that enables network users to access storage devices with high speed can be called a Storage Area Network. This type of network allowed users to store their data on public storage but privately.

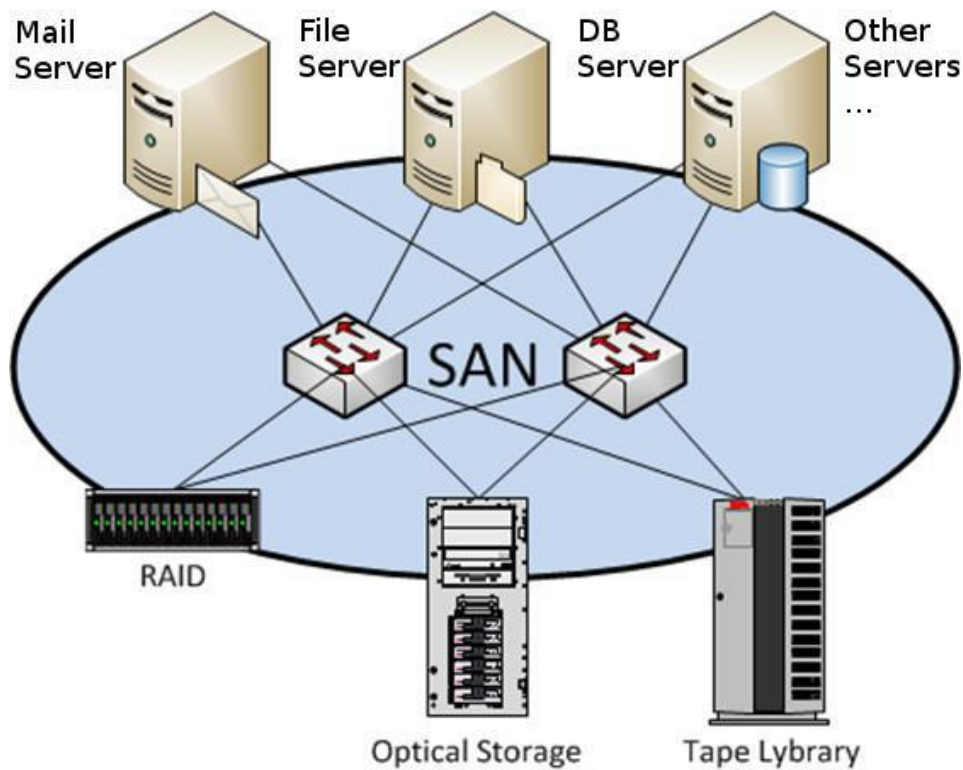
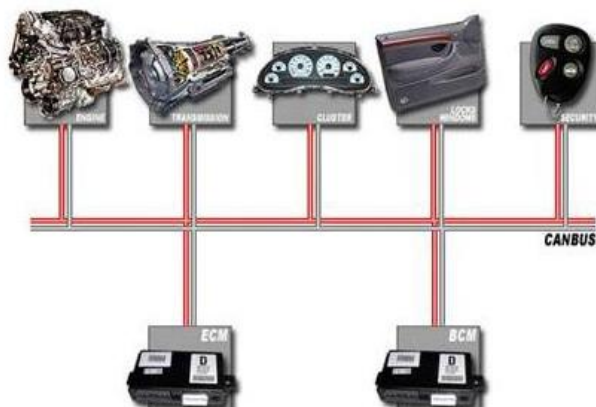


Figure 7 Storage Area Network

1.2.3.4 CAN - Controller Area Network

This network type can also be called a bus network. On this network type, some controlled devices or computers can connect to the network. Most private companies use this type of controller area network.



Controller Area Network (CAN)

Figure 8 Controller Area Network

1.2.3.5 PAN - Personal Area Network

A personal area network (PAN) connects electronic devices within a user's immediate area, ranging from a few centimetres to a few meters. It can be wired or wireless, and devices can exchange data with each other, but only the computer can connect directly to the Internet.

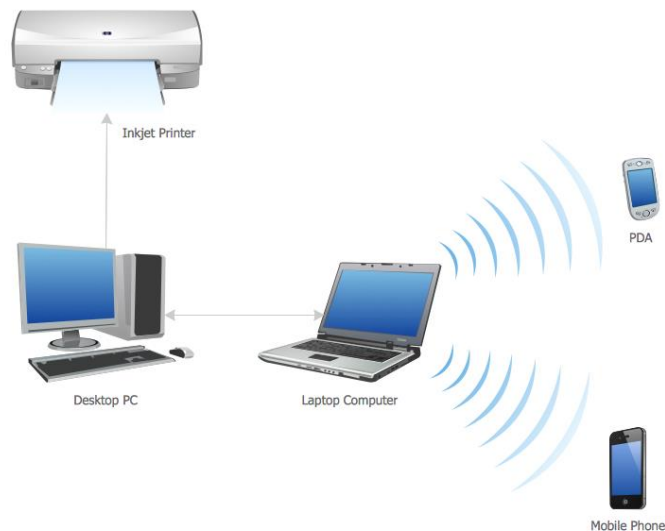


Figure 9 Personal Area Network

1.2.3.6 VPN - Virtual Private Network

Virtual private networks (VPNs) provide online privacy by creating an encrypted connection from a device to a network. They use tunnelling protocols to encrypt sensitive data from a sender, transmit it, and then decrypt it at the receiver's end, providing a high level of privacy.

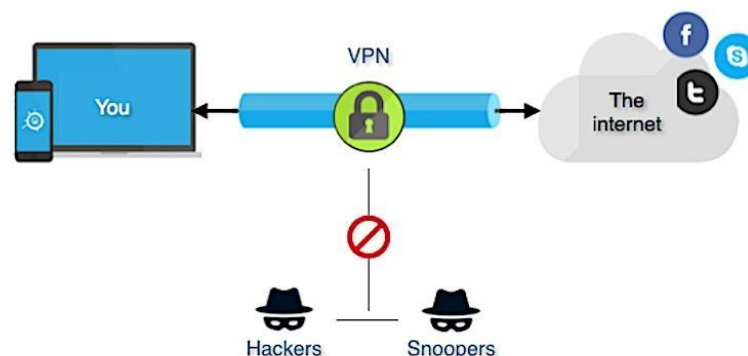


Figure 10 Virtual Area Network

1.2.4 Standards

Networking standards provide technical requirements, specifications, and guidelines to ensure devices, equipment, and software are suitable for their intended purpose.

- **American National Standards Institute (ANSI)**

ANSI is the coordinating organization for the U.S. national system of standards, accepting standards developed by other organizations and publishing them as American standards.

- **Institute of Electrical and Electronics Engineers (IEEE)**

IEEE is a global association and organization that works to standardize the electrical and electronic development industry.

IEEE 802	LAN/MAN
IEEE 802.1	Standards for LAN/MAN bridging and management and remote media access control (MAC) bridging.
IEEE 802.2	Standards for Logical Link Control (LLC) standards for connectivity.
IEEE 802.3	Ethernet standards for Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.4	Standards for token passing bus access.
IEEE 802.24	Standards for Logical Link Control (LLC) standards for connectivity.

IEEE 802.5	Standards for token ring access and communications between LANs and MANs.
IEEE 802.6	Standards for information exchange between systems.
IEEE 802.7	Standards for broadband LAN cabling.
IEEE 802.8	Fiber optic connection.
IEEE 802.9	Standards for integrated services, like voice and data.
IEEE 802.10	Standards for LAN/MAN security implementations.
IEEE 802.11	Wireless Networking- “Wi-Fi”
IEEE 802.12	Standards for demand priority access method.
IEEE 802.14	Standards for cable television broadband communications.
IEEE 802.15.1	Bluetooth
IEEE 802.15.4	Wireless Sensor/ Control Networks – “ZigBee”
IEEE 802.15.6	Wireless Body Area Network (BAN) – (e.g. Bluetooth low energy)
IEEE 802.16	Wireless Networking – “WiMAX”

Table 2 IEEE Standards

- **International Organization for Standardization (ISO)**

ISO is a worldwide federation of national standards bodies that collaborate to develop and promote international standards.

- **World Wide Web Consortium (W3C)**

W3C Recommendations are consensus-building guidelines that have been endorsed by W3C Members and the Director and are similar to standards published by other organizations.

- **Internet Engineering Task Force (IETF)**

The Internet Engineering Task Force is a standards organization responsible for the Internet protocol suite.

1.2.5 Network Models

Using a formal model allows us to deal with various aspects of Networks abstractly, in the same way, that we would use a computer program to model a real-life network. Both models are based on the concept of layering - where layers of data are placed on top of each other and interact to form a network.

The two major networking models are as follows:

- OSI Model
- TCP/IP Model

1.2.5.1 The OSI Model

The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization. The OSI provides a standard for different computer systems to be able to communicate with each other. It is based on the concept of splitting up a communication system into seven abstract layers.

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer

6. Datalink Layer
7. Physical Layer

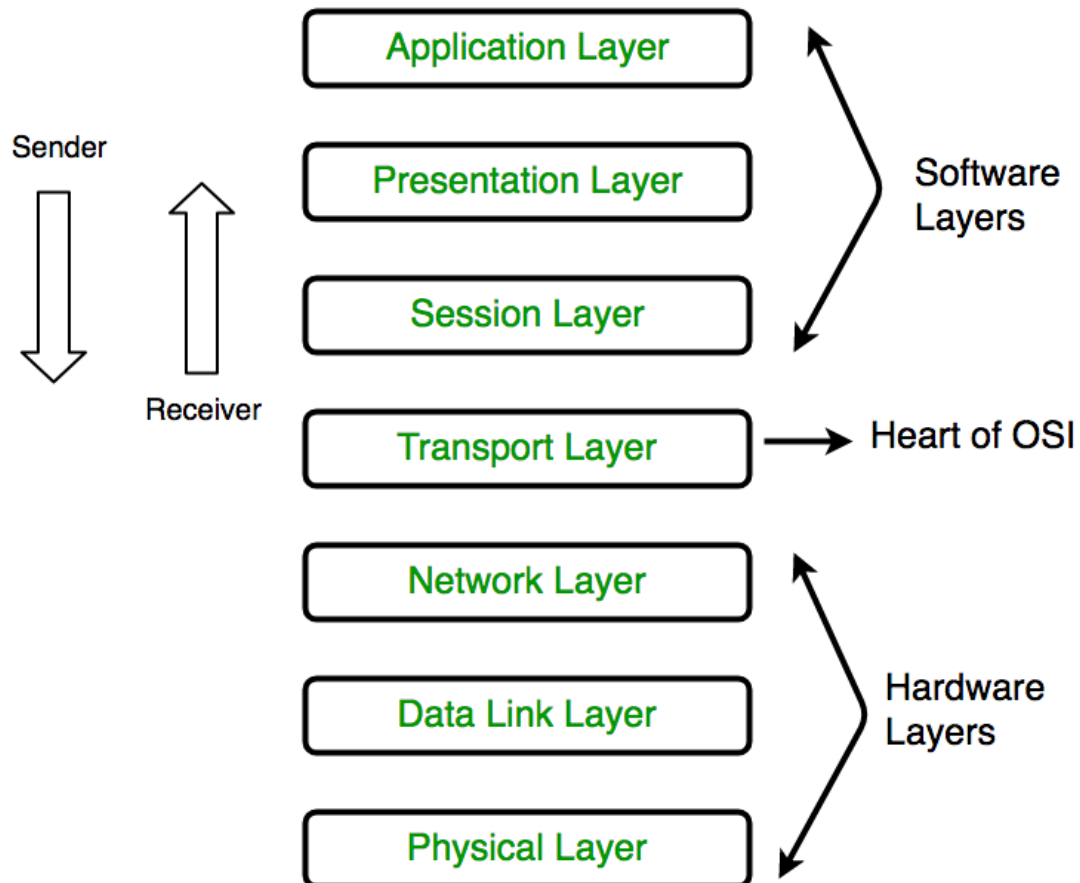


Figure 11 OSI Model

1. Application Layer

The application layer is the layer that allows software applications to communicate with each other and interact with data from the user. It is responsible for the protocols and data manipulation that the software relies on to present meaningful data to its users.

2. Presentation Layer

The presentation layer is responsible for the translation, encryption, and compression of data. It's responsible for translating incoming data into a syntax that the application

layer of the receiving device can understand. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

3. Session Layer

The session layer is the layer responsible for opening and closing communication between two devices. It ensures that the session stays open long enough to transfer all the data being exchanged. The session layer synchronizes data transfer with checkpoints, in the case of a crash or disconnection.

4. Transport Layer

The transport layer is responsible for the End-to-End Delivery of the complete message. It receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control. The transport layer also provides acknowledgment of the successful data transmission and re-transmits the data if an error is found.

5. Network Layer

The network layer is the layer between the transport layer and the data layer. It is responsible for facilitating data transfer between two different devices on different networks. The network layer also finds the best physical path for the data to reach its destination, or routes, known as routing.

6. Datalink Layer

The physical layer transmits and expects confirmations for separately obtained and delivered outlines. This layer establishes a consistent layer between two hubs and manages the system's traffic authority. The major function of this layer is to guarantee error-free data transfer from one hub to the next.

7. Physical Layer

The physical layer is responsible for the transmission and collection of unstructured, raw data over the system. It defines the requisite transmission voltages and information speeds. It converts digital/simple bits into electrical or optical signals. In addition, information encoding is performed in this layer.

1.2.5.2 The TCP/IP Model

The TCP/IP model is the Transmission Control Protocol/Internet Protocol Model. This model is a part of the network designed specifically for overseeing efficient and error-free transmission of data. The model works on a four-layered architecture model, where each layer implicitly the required network protocols on the data to be transmitted. These four layers are as follows.

1. Application/Process Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Link Access Layer

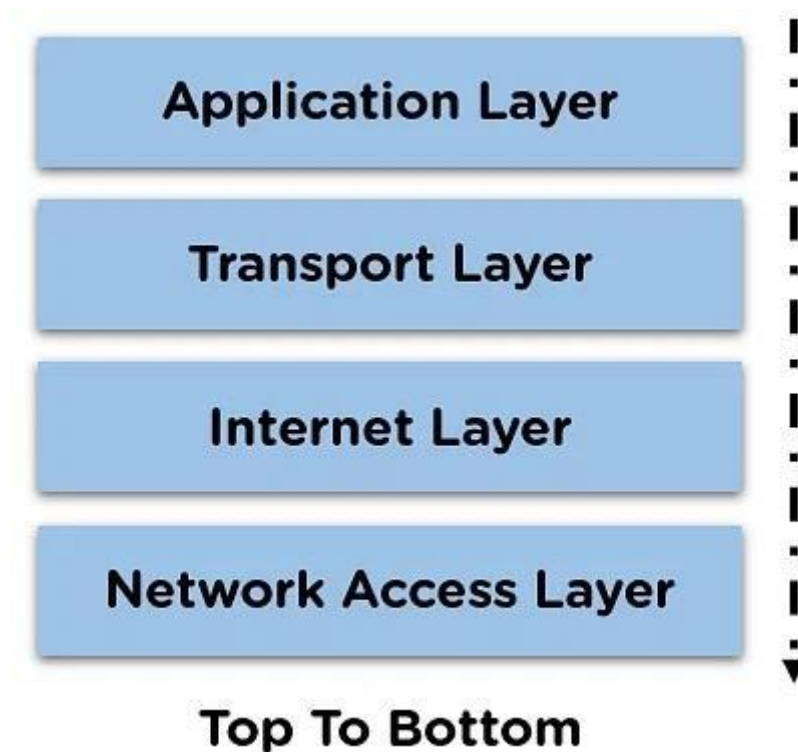


Figure 12 TCP/IP Model

1. Application/Process Layer

The application layer maintains a smooth connection between the application and the user for data exchange. It offers various feats such as remote handling of the system,

e-mail services, etc. Some of the protocols used in this layer are HTTP, SMTP, FTP, and LDAP.

2. Host-to-Host/Transport Layer

The Transport layer is responsible for the proper transmission of data over the communication channel. This layer establishes a network connection between the source and destination system. It also performs the task of maintaining the data, i.e., to be transmitted without error. The protocols used in this layer are TCP, User Datagram Protocol, and Data Flow Control Protocol.

3. Internet Layer

The Internet layer enacts protocols related to the transmission of data over the network modes. This layer is responsible for specifying the path that the data packets will use for transmission. Some of the protocols applied in this layer include the Address Resolution Protocol (ARP) and the Data Transport Protocol (DTP).

4. Network Link Access Layer

The network Access Layer is responsible for transmitting and receiving data over the physical medium of the network, such as a wire or wireless connection. Devices use it to establish connections with other devices on the network and transmit and receive data. For example, a phone may use the Network Access Layer to connect to a wireless network and send and receive phone calls and texts.

1.2.5.3 Differences between the OSI and TCP/IP models

OSI Model	TCP/IP Model
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI has 7 layers.	TCP/IP has 4 layers.
OSI is less reliable.	TCP/IP is more reliable.
OSI has strict boundaries.	TCP/IP does not have very strict boundaries.

OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI uses different session and presentation layers.	TCP/IP uses both the session and presentation layer in the application layer itself.
OSI developed a model and then a protocol.	TCP/IP developed protocols then model.
In the OSI model, the transport layer provides assurance delivery of packets.	The transport layer in TCP/IP does not provide assurance delivery of packets.
Connectionless and connection-oriented services are provided by the network layer in the OSI model.	TCP/IP model network layer only provides connectionless services.
While in the OSI model, Protocols are better covered and are easy to replace with the technology change.	Protocols cannot be replaced easily in TCP/IP model.

Table 3 Differences OSI & TCP/IP Model

1.2.5.4 Similarities between ISO OSI Model and TCP/IP Model

- Both TCP/IP are logical models.
- Architectural models have a stack of protocols arranged in every layer.
- Both TCP/IP defines standards for networking.
- Both TCP/IPs provide a framework for creating and implementing networking standards and devices.
- Both TCP/IPs divide the network communication process into making their layers.
- In Both TCP/IP model's manufacturer allows making sets of devices and network components that can co-exist and work with the devices and components that are made by the other manufacturers.
- In both TCP/IP models, a single layer defines a particular functionality and set standards for that functionality only.
- Both the TCP/IP models simplify their troubleshooting process by dividing the layer's complex functions into simpler components of the layer.
- Instead of defining the already defined standards and protocols in both the TCP/IP models. For example, the Ethernet standards were already defined by IEEE before

proceeding to create these models. So instead of defining them again in both the models of IEEE Ethernet standards.

1.2.6 Protocols

A protocol is a set of rules that allow electronic devices to communicate with each other, including what data may be transmitted, commands used, and how data transfers are confirmed. There are different types of protocols and different uses of the protocol.

IP – Internet Protocol

The internet protocol (IP) address is used to identify each device on a network uniquely. In modern networking, there are two types of IP addresses: IP v4 and IP v6. IP v4 addresses are 32 bits (4 bytes) long, while IP v6 addresses are 128 bits (16 bytes). On IP version 6, there is a risk of the internet getting stuck, so scientists developed a new IP version called IP version 6. The size of the IP address space is much larger than IP version 4, and all devices, services, and servers are ready to use it.

FTP – File Transfer Protocol

FTP (File Transfer Protocol) is a network protocol for transferring files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. It is used to transfer files behind the scenes for other applications, such as banking services, and to download new applications.

SSH – Secure Shell

SSH is a cryptographic network protocol that allows two computers to communicate and share data over an insecure network. It provides strong password authentication and

encrypted communication over an insecure channel and is used by network administrators to manage systems and applications remotely.

HTTP – Hyper Text Transfer Protocol

HTTP is a protocol used to access data on the World Wide Web, transferring data in plain text, hypertext, audio, video, and so on. It is similar to FTP, but uses only one connection and carries data in a MIME-like format.

HTTPS - Hypertext Transfer Protocol Secure

HTTPS is a secure extension of HTTP that encrypts data sent between a website and a web browser. It is supported by various web browsers and should be used for login credentials.

SMTP - Simple Mail Transfer Protocol

SMTP is a set of communication guidelines that allow the software to transmit electronic mail over the Internet. It is used to set up communication rules between servers and to handle errors such as incorrect email addresses.

TCP - Transmission Control Protocol

TCP and IP are the set of networking protocols that enable computers to connect over the Internet, with TCP managing the reliability of the rails and IP managing the addressing and forwarding of data.

UDP – User Datagram Protocol

UDP is used for real-time or high-performance applications that don't require data verification or correction and are commonly used for Remote Procedure Call (RPC) applications.

ARP – Address Resolution Protocol

ARP is a network protocol used to find out the hardware (MAC) address of a device from an IP address, allowing the sending device to send a packet to the receiving device. These four types of Address Resolution Protocols are as follows,

- Proxy ARP
- Gratuitous ARP
- Reverse ARP (RARP)
- Inverse ARP

Telnet

Telnet is a popular client-server program that allows users to log on to a remote computer by providing a connection to the remote computer in such a way that a local terminal appears to be on the remote side.

1.2.7 Network Topologies

The methods that we can use to connect two or more computers can be called network topologies. On a network, you will be able to use two main types of topologies called,

- Physical Topology
- Logical Topology

1.2.7.1 Physical Topology

A network that we laid out physically can be called a physical topology. When you are creating a network, you have to connect each computer to the other by using network devices and cables. When you connect computers or devices on a network you will be able to use the following main network topologies.

- Ring Topology
- Bus Topology
- Star Topology

- Mesh Topology
- Hybrid Topology

1.2.7.1.1 Ring Topology

Ring topology is a topology that is extended by using the line topology. In this ring topology same method that we use online topology will use.

On this network, each computer will connect with two computers on both sides of the network. Then each computer can use two connections with each network. This will enable the network to keep some computers off while two computers transfer data. But still, the network might need to keep some computers on to transfer data.

Same as the line topology on this network also flows data from other computers. Therefore, those computers can access data that we transfer so data privacy will be minimum on this network.

Advantages of Ring Topology

- Since data flows in one direction, the chance of a packet collision is reduced
- A network server is not needed to control network connectivity
- Devices can be added without impacting network performance
- Easy to identify and isolate single points of failure
- Better suited for high-traffic environments than a bus topology

Disadvantages of Ring Topology

- All data traveling over the network must pass through each device on its way to its destination, which can reduce performance
- If one device fails, the entire network is impacted
- Can be difficult to architect the necessary cabling
- More expensive to implement than a bus topology

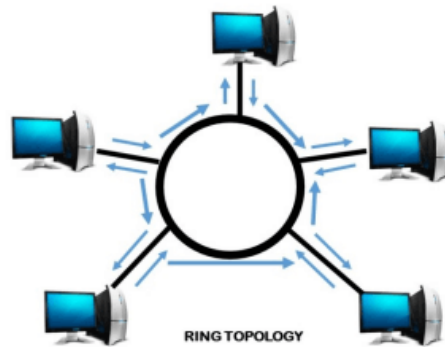


Figure 13 Ring Topology

1.2.7.1.2 Bus Topology

On this bus topology, the network contains a backbone cable that other computers can connect. Then any computer can transfer data directly to the other computer without data transferring through the other computers. Therefore, on a bus topology network, you don't have to keep other computers on to work with the network. But if the backbone cable is damaged or fails the network going to be down. So, on this network, it will be better to protect the backbone cable.

On this network type the privacy of the data that you transfer might not be possible. On each end of the backbone cable, we use a terminator to remove additional data from the backbone cable.

Advantages of Bus topology

- Low cost
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.
- No need to purchase any additional devices such as a switch and hub.

Disadvantages of Bus topology

- The entire network shuts down if there is a break in the main cable.

- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down. (Difficult to troubleshoot).

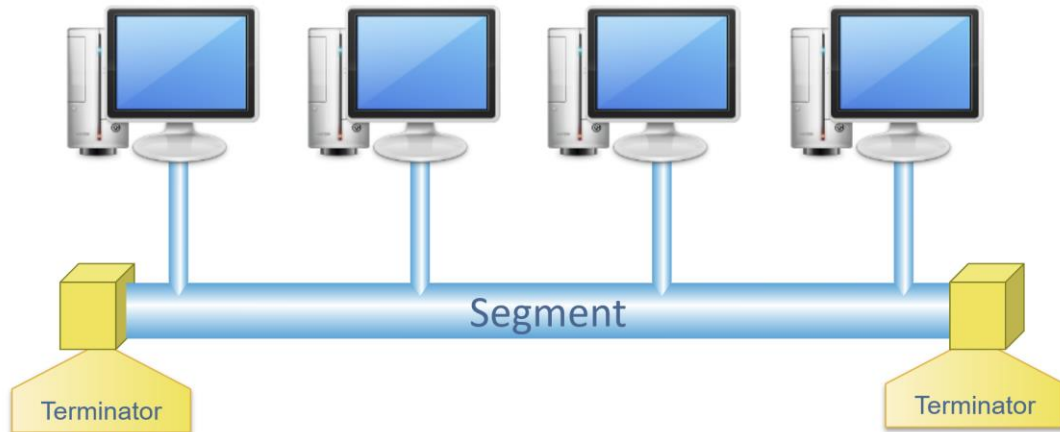


Figure 14 Bus Topology

1.2.7.1.3 Star Topology

On star topology we use a central device called a hub/switch each computer on the network will connect with the hub by using a direct cable. This topology will be the same as the bus topology. But without a backbone cable, the backbone cable will replace by the hub. In modern networking, we use this star topology.

Advantages of Star Topology

- It is easy to install and maintains.
- Can easily add and remove nodes to and from the network without affecting the network (scalability).
- If need to add another workstation with a star topology we can simply connect that system as an unused part of the hub.
- If any node fails, other nodes are not affected.

Disadvantages of Star Topology

- This type of network depends upon the central hub. If the hub fails the entire network is failed. (But hub troubleshooting is easier than bus topology)
- Each computer is directly connected to the hub through a cable, so it becomes costlier.

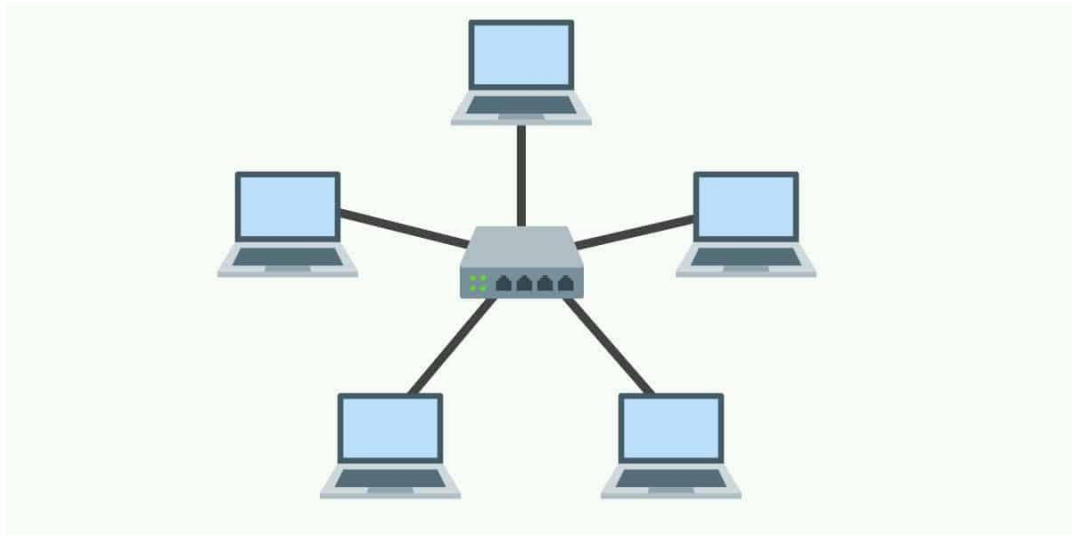


Figure 15 Star Topology

1.2.7.1.4 Mesh Topology

On this mesh topology, each computer will connect with each computer or as much as computers on the network. Internet uses this type of topology.

Advantages of Mesh Topology

- Provides redundant paths between devices.
- The network can be expanded without disruption to current users.

Disadvantages of Mesh Topology

- Requires more cable than the other LAN topologies.
- Complicated implementation.

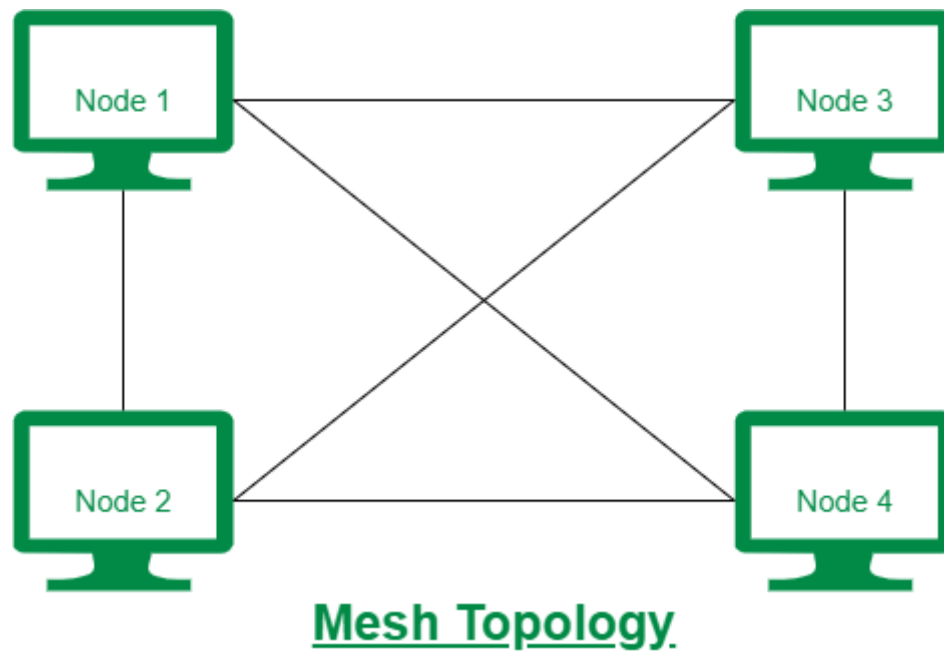


Figure 16 Mesh Topology

1.2.7.1.5 Hybrid Topology

Hybrid topology is a combination of two or more network topologies, depending on deployment and requirements. Tree topology is an example of a hybrid topology.

Advantages of Hybrid Topology

- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
- Error detecting and troubleshooting is easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

Disadvantages of Hybrid Topology

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.

- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.

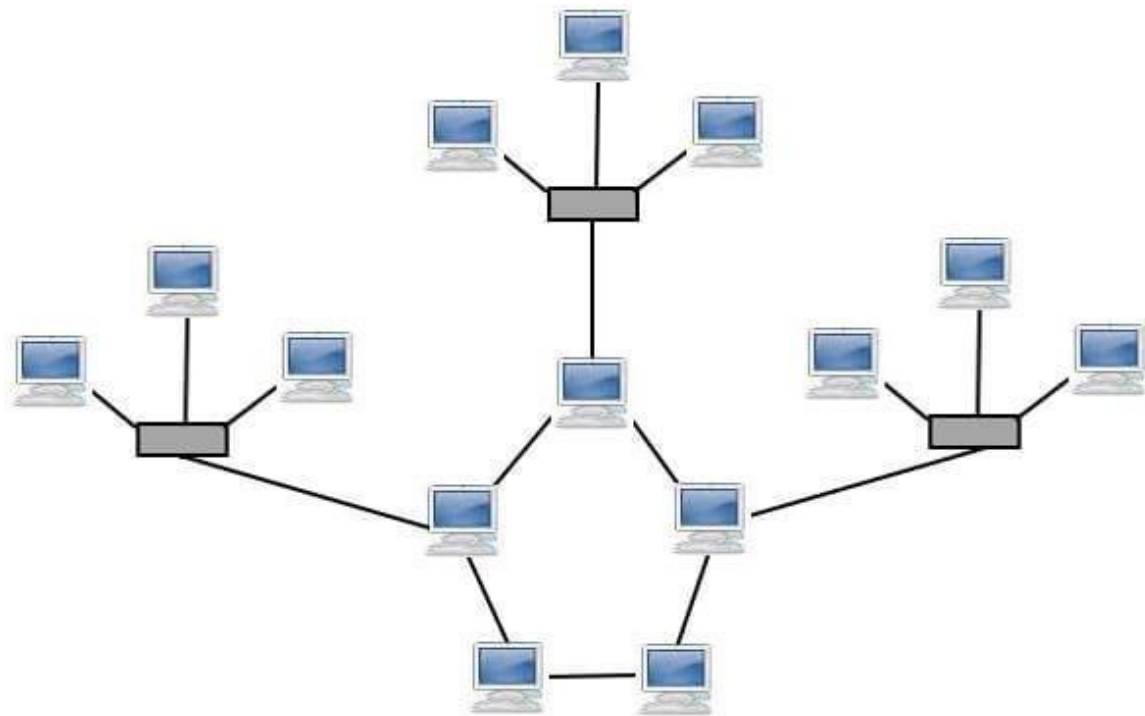


Figure 17 Hybrid Topology

1.2.7.2 Logical Topology

Logical Topology is the transmission of data over physical topology, independent of node arrangements, and ensures optimal flow control. These three types of logical topologies are as follows,

- Ethernet
- Virtual LAN
- Token Ring

1.2.7.2.1 Ethernet

Ethernet is a popular physical layer LAN technology that provides a good balance between speed, cost, and ease of installation, making it an ideal networking technology for most computer users.

1.2.7.2.2 Virtual LAN

VLAN is a concept that divides devices logically on layer 2, allowing for the creation of small-size sub-networks which are easy to handle.

1.2.7.2.3 Token Ring

Token ring topology is a structure of data communication between computers in a ring formation, where one host is connected to two adjacent hosts forming a circular structured network. When a host fails to receive a message, it fails the entire ring, and a backup can be made by deploying another ring.

1.2.8 Transmission Medium

The medium or media that we can use to create the communication link can be called transmission media. To transfer data within the network. We can use two main types of transmission media called,

- Wired Media
- Wireless Media

1.2.8.1 Wired Media

Wired media is also called physical media. Because wired media are the physical cables. That we use to transfer data within the network. As physical media, we can use 3 main types of cables,

- Coaxial Cables
- Twisted Pair Cable
- Fiber Optics Cable

1.2.8.1.1 Coaxial Cables

Coaxial cable consists of a core copper cable and another layer of copper mesh. In the earlier age of networking, this coaxial cable is the most common network cable type. But at the current network systems, the use of coaxial cable will be minimum. But security camera to the Digital Video Recorder (DVR).

Coaxial cables can transfer data at high speeds of up to 100m. Also, the cost of a coaxial cable will be very low.

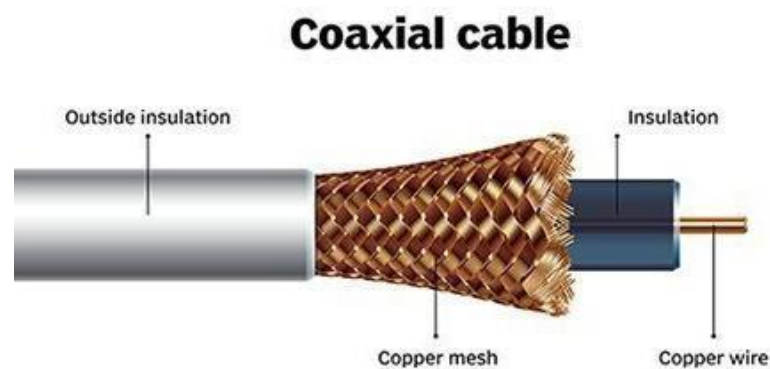


Figure 18 Coaxial Cable

1.2.8.1.2 Twisted Pair Cable

A cable consists of 8 cables that have twisted as pairs to create 4 twisted pairs cables as twisted pair cables. On modern networking, you will able to use two twisted pairs called,

- **Unshielded Twisted Pair Cable – UTP**

Unshielded twisted pair cables will not have any protection to protect the cable and data transfer from external forces. But you will able to use this cable the same as other cables. UTP cables can transfer data at very high speeds up to 40ms. Also, the cost of the cable will be minimum.

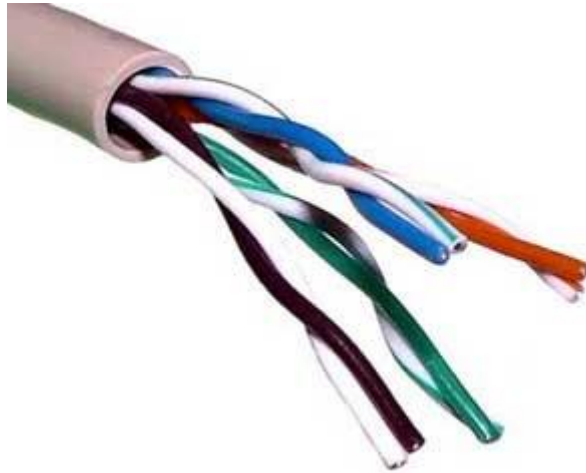


Figure 19 Unshielded Twisted Pair Cable

- **Shielded Twisted Pair Cable - STP**

On a Shielded twisted pair cable, there will be the protection you will be able to protect data from external forces. Therefore, you will be able to transfer data with high speeds up to 1000Mbps. Also, by using STP cable you will be able to send data up to 100ms. The purchasing cost of the cable will be more than coaxial and UTP cables.

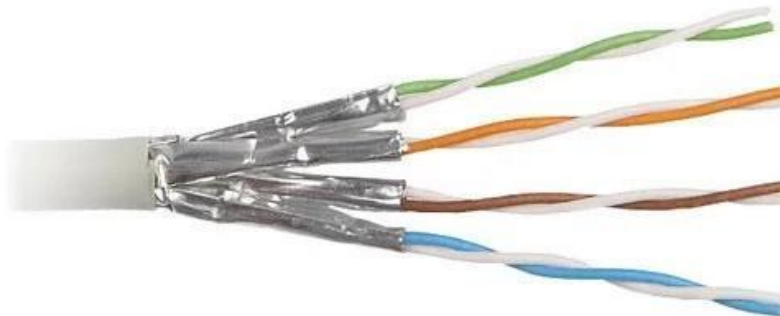


Figure 20 Shielded Twisted Pair Cable

Fiber Optics Cable

Fiber optic cables contain very thin cables made of glass or fiber. On these cables, we use light to transfer data. Therefore, the data transfer speed will be very high and able to transfer data with very high bandwidth. But the cost of fiber optic cables is very higher

than other cables. Most internet connections are shared through fiber optic cables all over the world.

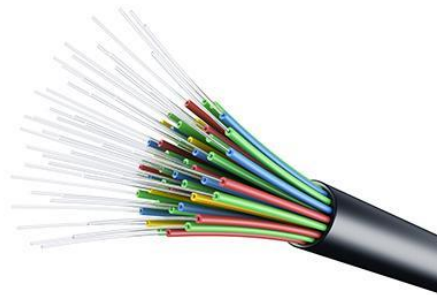


Figure 21 Fiber Optics Cable

1.2.8.2 Wireless Media

In wireless transmission methods, we can use radio signals to transfer data between devices. Other than radio signals we can use infrared lights to transfer data between infrared devices.

To transfer data, we can use 3 main types of wireless transmission media that use radio signals.

- WIFI
- Bluetooth
- Satellite

All these methods use radio signals. But on a Wi-Fi connection, you will be able to transfer up to 72 Mbps for a range of 40 m s. On Bluetooth transfer speed will be around 1Mbps for a maximum of 15 Ms.

Satellite connections will be able to transfer a longer range of area through the radio signals. But for the satellite connections whether the situation may affect data transfer.

1.2.9 Bandwidth

Network bandwidth is the maximum capacity of a wired or wireless communications link to transmit data in a given amount of time. Networking bandwidth is measured in bits, kilobits, megabits, or gigabits.

1.2.9.1 Bandwidth Requirements

Bandwidth is the amount of data that can be transferred in a given amount of time. As well as an important factor in determining the quality and speed of a network or internet connection and is now denoted with metric prefixes such as Mbps, Gbps, or Tbps.

The bandwidth requirements and utilization of web cameras and other meeting activities will vary depending on the make and model of the camera, resolution, frames per second (FPS) setting, active cameras, and users.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	Bps	1bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 kbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 kbps = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 kbps = 1,000,000,000,000 bps = 10^{12} bps

Table 4 Bandwidth Measurement

1.2.9.2 Latency

Latency is the time difference between the moment when a transaction is committed on the master and the moment when it is committed on a subordinate. It includes query run time, transfer time, WAN bandwidth, speed, and utilization.

1.2.10 Effectiveness of network systems

Networking is a fast and reliable way to share information and resources within a business, allowing for file sharing, resource sharing, sharing a single Internet connection, and increased storage solutions.

Network systems help employees improve communication, reduce errors, and deliver better services by allowing access to common databases and storing data in back-ups.

1.2.11 Networking Devices

Network devices enable communication and interaction between hardware on a computer network.

1.2.11.1 Hub

Hubs connect multiple computer networking devices, act as repeaters, and send data packets to all connected devices. They operate at the Physical layer of the Open Systems Interconnection (OSI) model. Hubs connect multiple computer networking devices, act as repeaters, and send data packets to all connected devices. They operate at the Physical layer of the Open Systems Interconnection (OSI) model.



Figure 22 Hub

1.2.11.2 Switch

Switches improve network efficiency and communication between hubs, routers, and other network devices.



Figure 23 Switch

1.2.11.3 Router

The router is an intelligent network device that can be configured to act as packet-filtering firewalls and ACLs, as well as divide networks into subnetworks, facilitating a zero-trust architecture.



Figure 24 Router

1.2.11.4 Bridge

The bridge is used to connect hosts or network segments, regulate traffic, filter packets, and filter frames.



Figure 25 Bridge

1.2.11.5 Gateway

Gateway devices facilitate interoperability between different technologies by translating messages.



Figure 26 Gateway

1.2.11.6 Modem

A modem converts digital signals into analogy signals, then converts them back to digital.



Figure 27 Modem

1.2.11.7 Repeater

A repeater amplifies a signal to cover a longer distance.



Figure 28 Repeater

1.2.11.8 Access Point

An access point is a network device that connects a variety of network devices, with a built-in antenna, transmitter, and adapter, and can be configured manually or remotely.



Figure 29 Access Point

1.2.11.9 Firewall

A firewall is a hardware device that monitors and controls network traffic based on security rules, protecting internal networks from unauthorized access and threats. It is commonly deployed in corporate networks, data centres, and homes to enhance security. Firewalls analyse packets and determine whether to allow or block them based on configured policies.



Figure 30 Firewall

1.2.12 Types of Servers

A server is a piece of computer hardware or software that provides functionality for other programs or devices, known as clients.



Figure 31 Types of Servers

1.2.12.1 Web Server

Web servers provide hosting, which is the renting of space required to publish Web pages on the Internet. Apache, Microsoft's IIS, and Nginx are the most popular web servers. A web Server is used to efficiently use the computer and is made up of numerous software packages.

1.2.12.2 File Server

File Servers are modern and capable of mapping networked files onto drives, allowing users to upload and download shared files.

1.2.12.3 Database Server

Database servers are used to store data in groups, such as MySQL, MariaDB, Microsoft SQL, Oracle Database, and MS-SQL. They should exist on their own for security as if a hacker gains access to the main web server, they will be able to retrieve or modify the data stored in the database.

1.2.12.4 Server Selection Requirement

- **Match the server to your primary need**

A dedicated email server or file-sharing server is an ideal option for improving business email and document management.

- **Buy an affordable server**

Set a budget for a new server and shop around for great deals.

- **Choose best of breed**

Vendor leaders should be chosen to ensure a reputable source and fully supported server for business needs.

- **Buy the right operating system**

Choosing the right operating system is essential for stable applications and server performance.

- **Build in expansion and redundancy**

Businesses should expand their server with hard drives that can be upgraded and RAID configuration to ensure data is not lost.

- **Support and maintenance**

Businesses may need to outsource IT support and maintenance if they don't have onsite IT support.

- **Choose the right cloud service providers**

Small businesses should perform due diligence before signing up for cloud-based servers to ensure security.

1.2.12.5 Server Brands Documentation

Brand-Model			Specifications	Extra Features	Price
Cisco	USC	C-Series	up to two 4th Gen Intel Xeon Scalable CPUs, with up to 52 cores per socket	Up to 3 PCIe 4.0 slots or up to 2 PCIe 5.01 slots, plus a modular LAN on the motherboard (mLOM) slot	Starting at price of 3,699 USD
			32 DDR5 DIMM slots: 16, 32, 64, and 128 GB up to 4800 MT/s (Memory)	Up to 10 x 2.5-inch SAS and SATA HDDs, SSD, and NVMe drives, with the option of up to 4 direct-attach NVMe drives	
IBM	Power	System S922	The Power S922 server supports two processor sockets, offering 10-core or 20-core typical 2.9 to 3.8 GHz (max), or 8-core or 16-core typical 3.4 to 3.9 GHz (max), or 4-core typical 2.8 to 3.8 GHz (max) POWER9 configurations in a 19-inch	Up to 10 x 2.5-inch NVMe PCIe SSDs (all direct-attach PCIe Gen4x4)	37,222 USD
				Dual M.2 SATA/NVMe SSDs with HW RAID support	

	rack-mount, 2U (EIA units) drawer configuration. All the cores are active.		
Dell PowerEdge R710	Quad-core or six-core Intel® Xeon® processor 5500 and 5600 series Up to 288GB (18 DIMM slots): 1GB/2GB/4GB/8GB/16GB DDR3 up to 1333MT/s	Hot-plug hard drive options: 2.5" SAS SSD, SATA SSD, SAS (15K, 10K), nearline SAS (7.2K), SATA (7.2K) 3.5" SAS (15K, 10K), nearline SAS (7.2K), SATA (7.2K)	399 USD

Table 5 Server Brands Documentation

After server comparison and review, the Enclave website has selected the Cisco USC C-Series as the data server. In addition, the Dell PowerEdge R710 has been chosen as the backup server.

1.2.13 Workstation

Workstations are specialized computers for scientific or technical applications, connected to a local area network and multi-user operating system.

The inter-dependence of workstation hardware with relevant networking software

- Workstations can be used independently of mainframes, with applications installed and stored on hard drives.
- Workstations are attached to the network and processed after loading programs and data from servers, and files are stored back on the server to be used by other workstations.
- The server may be dedicated, non-dedicated, workstation, or DOS-based.

- Network interface cards act as translators, allowing computers to communicate with each other using the specified protocol.

1.2.14 Networking Software

Network software is software for networking that helps network administrators gain complete control over their IT infrastructure, monitor network health, measure performance, anticipate potential outages, take proactive decisions, and resolve network faults. It is important to invest in efficient computer network software platforms to ensure network optimization.

1.2.14.1 Client Software

A client is a computer or program that relies on sending a request to another program or computer hardware or software to access a service made available by a server.

E.g.: - Client Operating System

1.2.14.2 Server Software

Server software is used to interact with a server's hardware infrastructure, such as the processor, memory, storage, input/output (I/O), and other communication ports.

E.g.: - Server Operating System

1.2.14.3 Software Firewall

Firewalls protect any network-connected device and can be deployed as software, hardware, or virtual.

1.2.15 Benefits of Computer Networking

Networking and internet access have enabled users to share both hardware and software resources quickly and efficiently, lowering the cost of providing network solutions. This has enabled businesses to stay connected to their networks and students to access unlimited resources.

Some of the key benefits of computer networking are as follows;

- **Resource sharing:** Computer networking allows multiple users to share resources such as printers, scanners, and data files, making it easier to collaborate and work together.
- **Increased efficiency:** Computer networking enables users to communicate and share data more quickly and easily, which can increase productivity and efficiency in the workplace.
- **Remote access:** With computer networking, users can access resources and data from remote locations, making it easier to work from home or when traveling.
- **Cost savings:** By sharing resources and data, computer networking can help organizations save money on hardware, software, and other IT expenses.
- **Improved communication:** Computer networking enables users to communicate with each other more effectively through email, instant messaging, and video conferencing, regardless of their physical location.
- **Scalability:** Computer networking can easily scale to accommodate an organization's growing needs, allowing it to expand without significant infrastructure changes.

Overall, computer networking has revolutionized the way we work and communicate, providing numerous benefits to individuals and organizations alike.

1.2.16 Constraints of Computer Networking

While computer networking has many benefits, there are also several constraints that can affect its effectiveness. Here are some of the key constraints of computer networking:

- **Security:** Computer networks are vulnerable to security threats, such as hacking and malware attacks, which can compromise data and systems. Maintaining network security requires constant monitoring and updates to security protocols.
- **Reliability:** Network downtime or failures can result in lost productivity and revenue. Network components, such as routers and switches, need to be maintained and upgraded regularly to ensure reliable performance.
- **Bandwidth limitations:** Network bandwidth can become a bottleneck when multiple users are accessing the network simultaneously. This can result in slow data transfer speeds and reduced performance.
- **Compatibility:** Networking components and protocols need to be compatible to work together effectively. If incompatible components are used, data transfer speeds can be reduced, and the network may not function correctly.
- **Complexity:** Computer networks require specialized knowledge and skills to set up and maintain. This can make networking challenging for small organizations or individuals without dedicated IT staff.

Overall, computer networking can be a powerful tool, but it is not without its constraints. Addressing these constraints requires ongoing monitoring and maintenance, as well as careful planning and implementation of networking infrastructure.

Activity 02

2.1 Blueprint of LAN

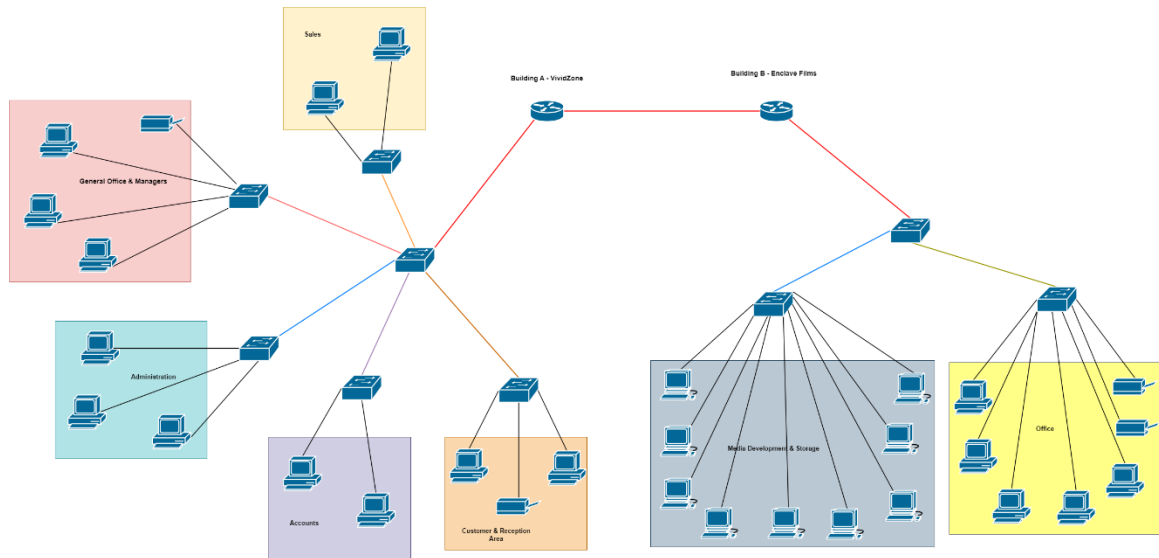


Figure 32 Blueprint of LAN

2.1.1 Technical Requirements

Enclave Movie Company has decided to enhance and secure its existing network infrastructure to modern-day standards. The provided diagram illustrates the company's fundamental network setup. Building A will house twelve desktop computers and two printers, which will be interconnected via a LAN, positioned between the two buildings. Building B's network is composed of nine high-performance workstations, five office PCs, and two printers. There is a total of nine switches, all connected to two routers. Additionally, a wireless access point has also been installed and there are a few project managers with laptops in the B building. There are eight departments and VLAN are assigned to each department.

2.1.2 Proposed Topology

After carefully considering the recommendations of networking peers and conducting thorough research, we have decided to implement a star topology for the company's networks.

Characteristics of Star Topology:

- High-speed connections
- Flexibility in network design
- High reliability
- Ease of maintenance

Advantages of Star topology:

- Individual nodes require dedicated cables, simplifying management and maintenance.
- Any failures can be easily identified as they only impact a single user or system.
- The star topology facilitates efficient data transfer with excellent throughput rates.

List of Hardware devices:

Quantity	Description	Brand	Model
9	High-performance workstations	Dell	Dell Precision Tower 7920 Workstation
1	Wireless access point (Wi-Fi router)	Cisco	Cisco Aironet 3800 Series Access Point
2	Router	Cisco	Cisco ISR 4000 Series Router
9	Switches	Cisco	Cisco Catalyst 9300 Series Switches
17	Desktop PC	HP	HP EliteDesk 800 G6 Desktop PC

4	Printers	HP	HP LaserJet Pro MFP M521dn
-	Cables (CAT5)	AmazonBasics	AmazonBasics RJ45 Ethernet Cable Cat-5e Patch

Table 6 List of Hardware Devices

2.1.3 BYOD (Bring Your Own Device) policies

To ensure secure usage of company networks and premises, all employees and guests are required to register their personal phones, laptops, tablets, and electronic devices. Additionally, an enforced acceptable use policy is in place for accessing the company's Wi-Fi. This policy aims to prevent unauthorized individuals from disrupting the reasonable and private use of the company's networking services.

2.2 Selection of Accessories, Quality of Services and Security Requirements

2.2.1 Dell Precision Tower 7920 Workstation

Enclave Films requires a reliable and secure network infrastructure for its movie production and delivery. The Dell Precision Tower 7920 Workstation should meet these security requirements by providing robust security features, supporting Quality of Service (QoS) for video applications, offering redundancy and high availability options, facilitating network monitoring, and offering fast and reliable connectivity capabilities. Enclave Films also needs a connection to VividZone, which requires high-speed interfaces and industry-standard networking protocols. These features will help meet Enclave Films' security requirements and ensure the quality of services needed for their network infrastructure.



Figure 33 Dell Precision Tower 7920 Workstation

2.2.2 Cisco Aironet 3800 Series Access Point

The Cisco Aironet 3800 Series Access Point is an ideal choice for Enclave Films' network upgrade due to its high-performance wireless connectivity, QoS for video applications, high network availability and redundancy, advanced security features, and scalability and manageability. The Access Point offers reliable and high-speed wireless connectivity, enhancing coverage and capacity for project managers and guests. It also prioritizes video traffic for optimal performance, ensuring uninterrupted streaming and low-latency performance. The access point also supports dual-band operation, multiple radios, and redundant power options, ensuring uninterrupted wireless connectivity even in hardware or power failures. Additionally, the Access Point offers robust security features, including integrated Intrusion Detection System (IDS)/IPS, Secure Sockets Layer (SSL) encryption, and support for WPA3 protocols.

The Cisco DNA Centre centralized management platform simplifies configuration and troubleshooting, allowing Enclave Films to efficiently manage and expand its wireless network as business requirements evolve. Overall, the Cisco Aironet 3800 Series Access Point is a compelling solution for Enclave Films' network upgrade, meeting their specific requirements for video production and distribution.



Figure 34 Cisco Aironet 3800 Series Access Point

2.2.3 Cisco ISR 4000 Series Router

The Cisco ISR 4000 Series Router is a versatile and powerful router suitable for Enclave Films' network upgrade. It supports virtual LAN functionality, allowing for logical segmentation of the network, enabling better network security and traffic management. The router can handle an 80% increase in data traffic, ensuring efficient processing and WAN optimization. It offers fast and reliable connections to VividZone, ensuring efficient content delivery. The router supports redundant link options, redundancy, and high availability, ensuring network availability and minimizing downtime.

It also offers robust security features, including threat defence, encryption, and access control mechanisms. The router also supports QoS features for video applications, ensuring low latency, minimal packet loss, and a smooth streaming experience. Overall, the Cisco ISR 4000 Series Router is a robust and scalable solution that can support Enclave Films' network consolidation and enhancement efforts.



Figure 35 Cisco ISR 4000 Series Router

2.2.4 Cisco Catalyst 9300 Series Switches

Enclave Films should choose Cisco Catalyst 9300 Series Switches based on their network requirements and criteria. These switches offer advanced VLAN capabilities, such as VLAN segmentation, VLAN trunking, and high performance. They handle increased data traffic, provide high-speed connectivity, and offer buffering and queuing mechanisms. They also offer network redundancy and high availability, with redundant power supplies, redundant uplinks, and protocols like Hot Standby and Rapid Spanning Tree Protocol. The switches support QoS for video applications, including traffic classification and marking, traffic shaping and policing, and network monitoring and security features. These switches provide centralized management and network monitoring capabilities, ensuring a robust and efficient network infrastructure for Enclave Films' operations.



Figure 36 Cisco Catalyst 9300 Series Switches

2.2.5 HP EliteDesk 800 G6 Desktop PC

The HP EliteDesk 800 G6 Desktop PC is the ideal choice for Enclave Films' network due to its high-performance computing capabilities, connectivity options, reliability, security features, and space-efficient form factors. It offers powerful processors, ample memory and storage, and dedicated graphics processing for smooth video editing, rendering, and graphic-intensive tasks. The PCs also provide Ethernet and USB ports, expansion slots, and display connectivity, ensuring seamless integration with network infrastructure and peripherals. Additionally, the EliteDesk 800 G6 offers robust build quality, security features, remote management, and various form factors, including compact and small form factors, allowing flexibility in deployment and optimizing space utilization in Enclave Films' offices. Overall, the HP EliteDesk 800 G6 Desktop PC meets Enclave Films'

requirements for media development, editing, and storage while ensuring productivity and data protection.



Figure 37 HP EliteDesk 800 G6 Desktop PC

2.2.6 HP LaserJet Pro MFP M521dn

The HP LaserJet Pro MFP M521dn is a multifunction printer that offers print, copy, scan, and fax functions, allowing Enclave Films to produce professional documents, reports, and marketing materials. It offers high-quality laser printing, fast copying, scanning, and faxing capabilities. The printer offers high print speeds, fast copy speeds, seamless network connectivity, and compatibility with mobile printing technologies. It also offers duplex printing and scanning capabilities, reducing paper usage and improving scanning efficiency. The printer also provides efficient document handling and paper capacity, with an Automatic Document Feeder (ADF) and generous paper capacity. The printer supports Enclave Films' document management needs, ensuring high-quality output, seamless integration into the network, and improved productivity.



Figure 38 HP LaserJet Pro MFP M521dn

2.2.7 AmazonBasics RJ45 Cat-5e Ethernet Patch Cable

Enclave Films' network upgrade requires accessories like the AmazonBasics RJ45 Cat-5e Ethernet Patch Cable to meet security requirements, quality of service (QoS), redundancy, high availability, fast and reliable connections, and wireless network access needs. Network security is crucial for protecting against unauthorized access, data breaches, and intellectual property theft. Quality of service (QoS) for video applications requires high-quality network performance and reliable and high-performance accessories like the AmazonBasics RJ45 Cat-5e Ethernet Patch Cable to ensure consistent and reliable connectivity. Redundant links and technologies are essential for network availability and minimizing downtime. Fast and reliable connections to VividZone are necessary for efficient content delivery, and high-quality Ethernet patch cables contribute to the overall network infrastructure. These accessories play a critical role in establishing a robust and efficient network infrastructure for Enclave Films' operations and its partnership with VividZone.



Figure 39 AmazonBasics RJ45 Cat-5e Ethernet Patch Cable

2.3 Redesigned Network of Enclave Films

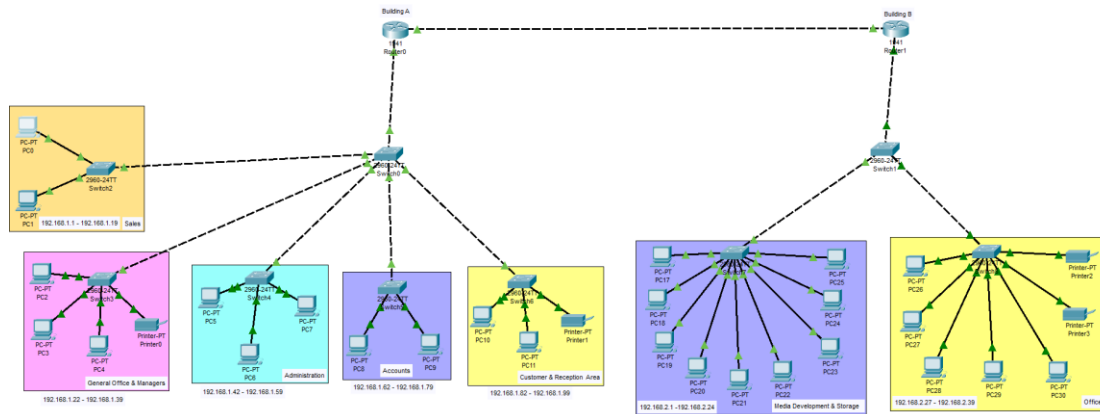


Figure 40 Redesign Network

2.4 IP Allocation Table

Departme nt	Vlan no	Network Ip	B.cast Ip	Gateway Ip	Subnet mask	Usable Ip range
Sales	Vlan 10	192.168.1. 0	192.168.1.2 0	192.168.1.2 54	255.255.255 .0	192.168.1. 1 – 192.168.1. 19
General office & managers	Vlan 20	192.168.1. 21	192.168.1.4 0	192.168.1.2 54	255.255.255 .0	192.168.1. 22 - 192.168.1. 39
Administra tion	Vlan 30	192.168.1. 41	192.168.1.6 0	192.168.1.2 54	255.255.255 .0	192.168.1. 42 – 192.168.1. 59
Accounts	Vlan 40	192.168.1. 61	192.168.1.8 0	192.168.1.2 54	255.255.255 .0	192.168.1. 62 – 192.168.1. 79
Customer &	Vlan 50	192.168.1. 81	192.168.1.1 00	192.168.1.2 54	255.255.255 .0	192.168.1. 82 –

Reception Area						192.168.1.99
Media Development & Storage	Vlan 60	192.168.2.0	192.168.2.25	192.168.2.254	255.255.255.0	192.168.2.1 – 192.168.2.24
Office	Vlan 70	192.168.2.26	192.168.2.40	192.168.2.254	255.255.255.0	192.168.2.27 – 192.168.2.39

Table 7 IP Allocation Table

2.5 Install & configure network services and applications of your choice

VMware Workstation Pro is a 64-bit hosted hypervisor designed for virtualization on Microsoft Windows and Linux endpoint computers. It creates an abstraction layer between software and hardware, managing virtual representations like CPUs, memory, storage, and network adapters. Enterprise-class hypervisors, like VMware ESXi, run directly on the underlying hardware, while endpoint-type hypervisors like VMware Workstation Pro install atop a host OS. Workstation Pro is treated as an application, allowing users to create virtual machines and resources while running as an isolated instance.

I utilized VMware Workstation Pro for virtualization purposes during the Windows installation process. The steps taken for the installation of VMware Workstation Pro are as follows.

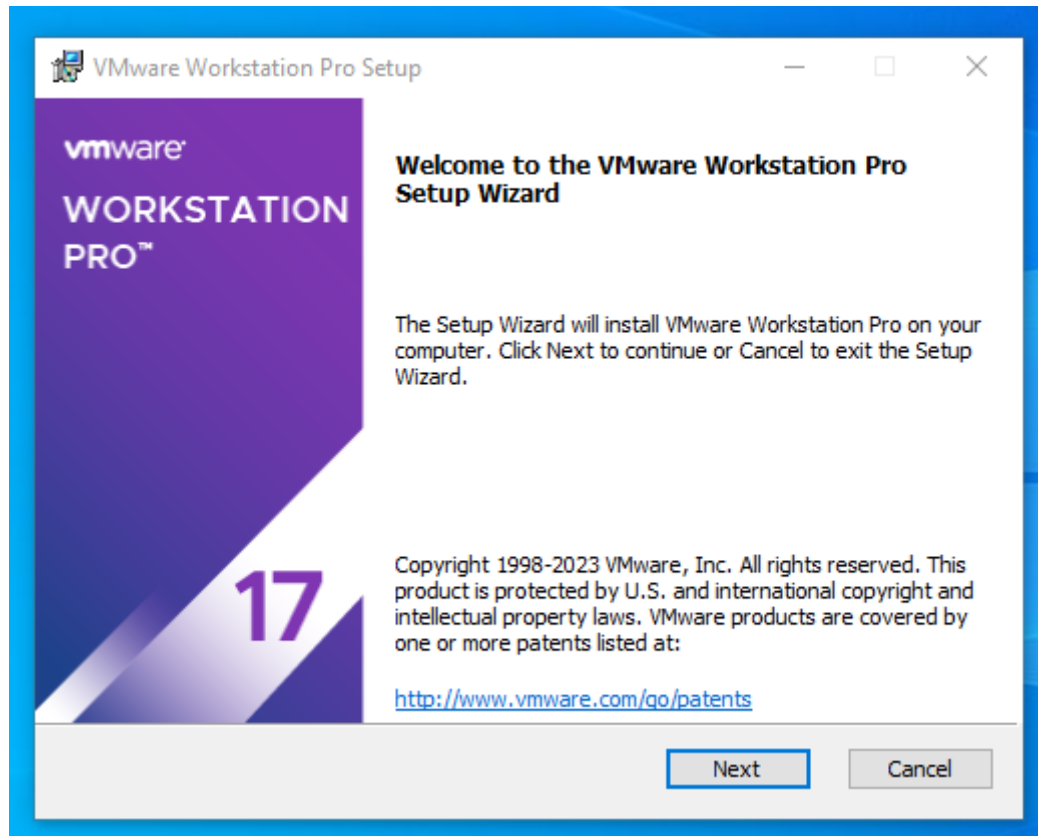


Figure 41 VMware Workstation Pro Setup

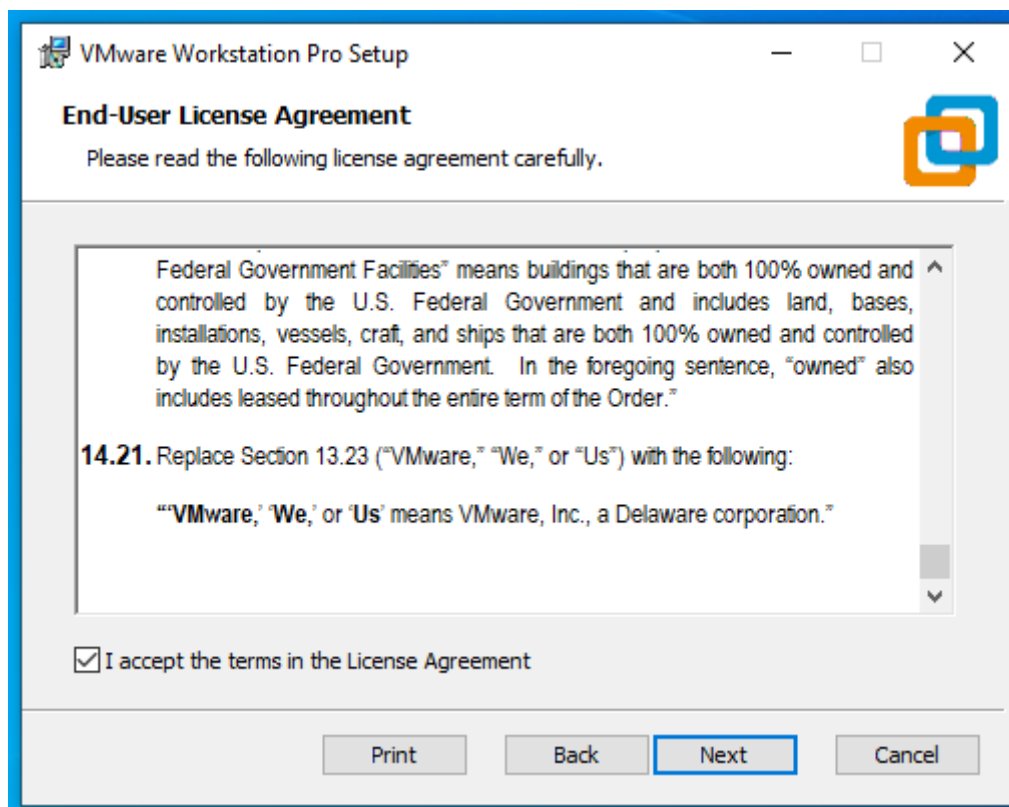


Figure 42 VMware End User License Agreement

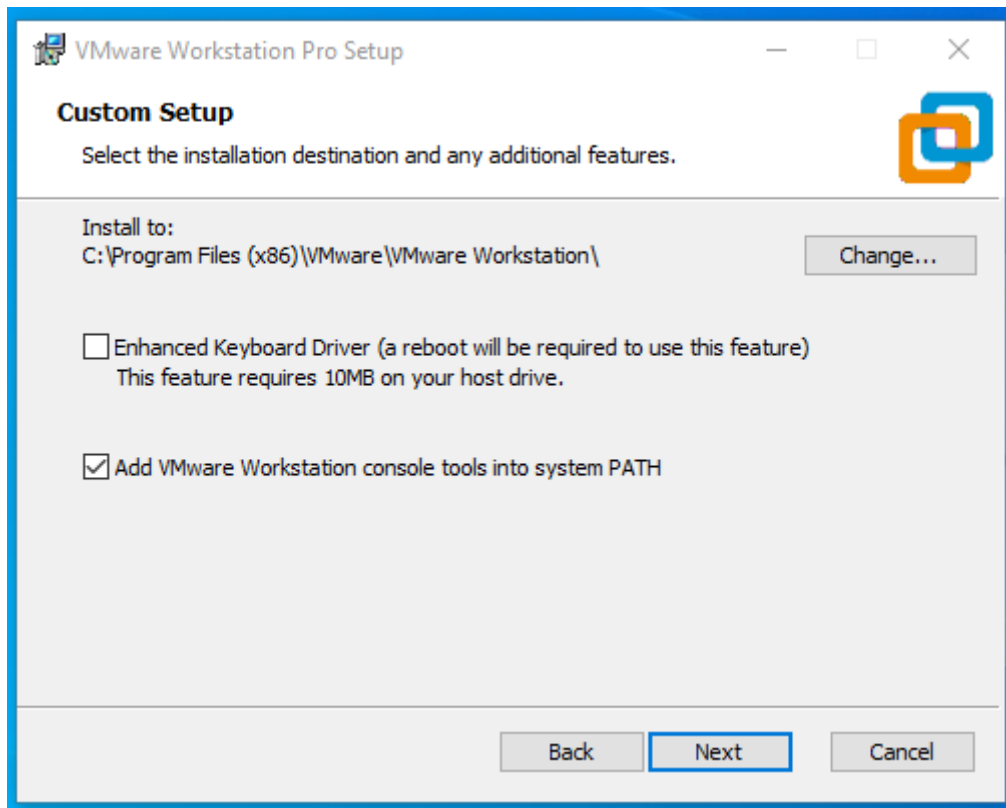


Figure 43 Custom Setup

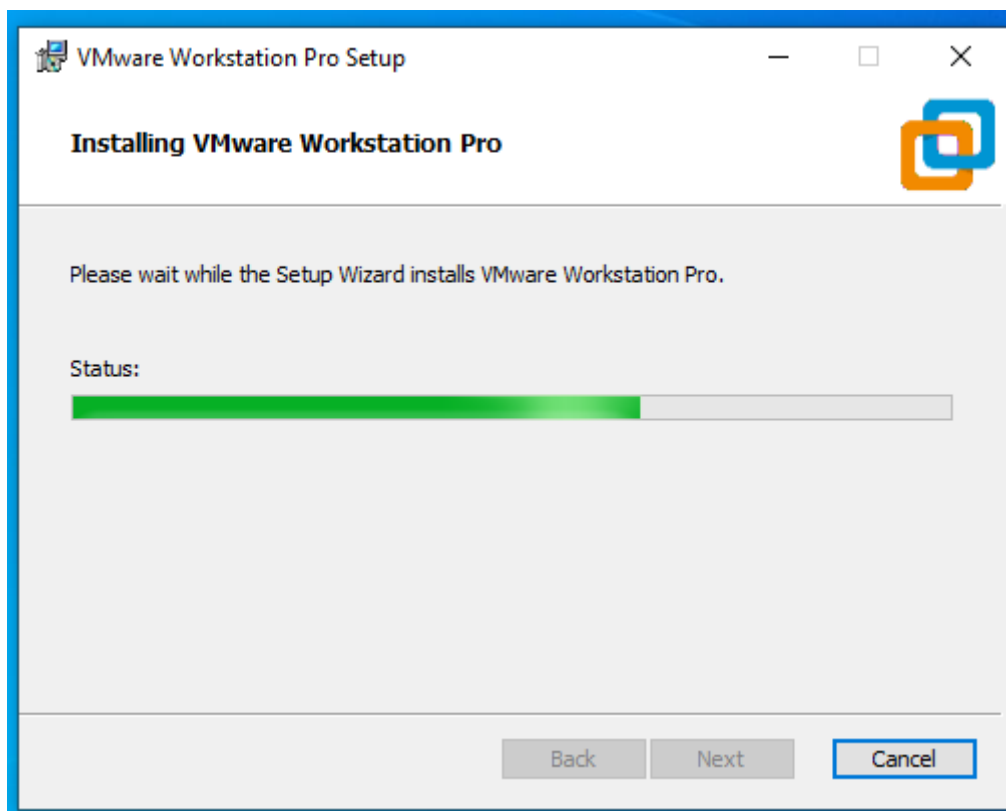


Figure 44 Installation of VMware Workstation Pro

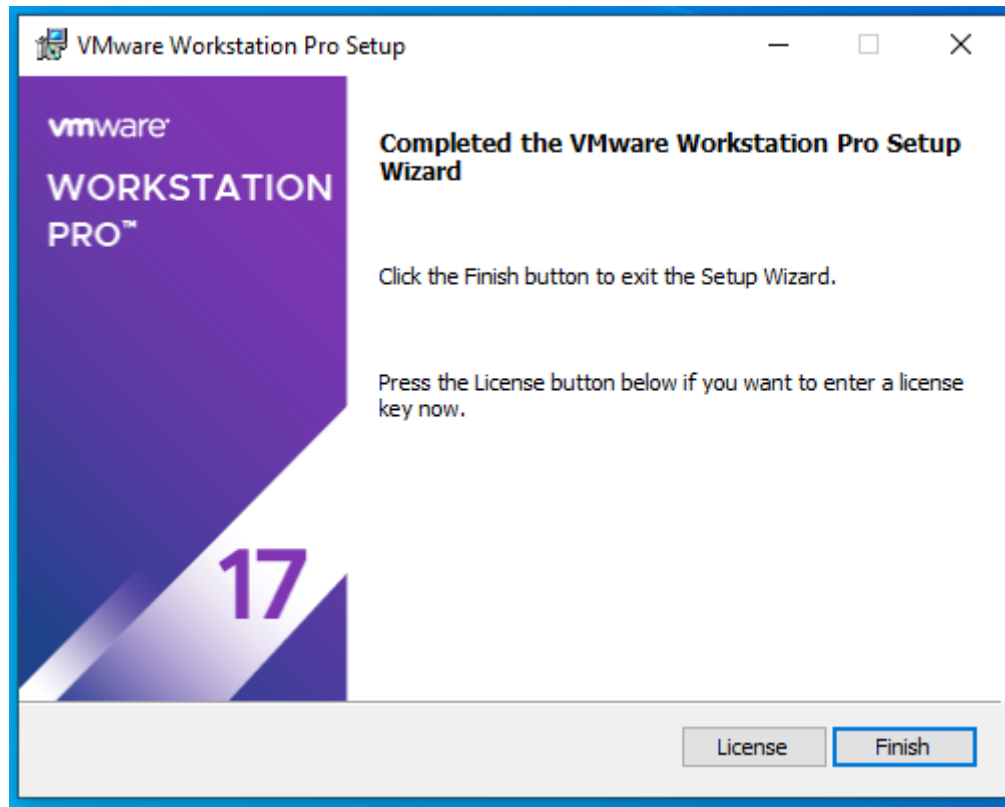


Figure 45 VMware Installation Complete

2.6 Conduct a test and evaluate the design to meet the requirements and analyses user feedback

Enclave Movie Company Network Upgrade Feedback Form

Dear Employee,

We value your feedback regarding the recent network upgrades conducted by Enclave Movie Company. Your input is crucial in assessing the effectiveness of the upgrades and identifying areas for further improvement. Please take a few moments to complete this feedback form based on your experience before and after the network upgrades.

Ispliyanage3128@gmail.com [Switch account](#)

Not shared

* Indicates required question

How satisfied are you with the overall performance of the network after the redesign?

☐ Very good
☐ Good
☐ Not so good
☐ Bad

How would you rate the Wi-Fi connections in both buildings?

☐ Very good
☐ Ok
☐ Not so good
☐ Very bad

Figure 46 User Feedback Form - i

How would you rate the speed and responsiveness of the network for your day-to-day tasks?

☐ Excellent

☐ Good

☐ Fair

☐ Poor

How would you rate the security and security features implemented?

☐ Good

☐ Ok

☐ Not so good

☐ Very bad

Did the network meet your requirements for data transfer and file sharing among departments?

☐ Yes

☐ No

Figure 47 User feedback form - ii

How is our maintenance service?

☐ Excellent

☐ Good

☐ Average

☐ Poor

Were there any noticeable delays or bottlenecks while accessing network resources or the internet?

☐ Yes

☐ No

☐ Maybe

Comment Suggestions

Your answer

Name *

Your answer

Figure 48 User feedback form - iii

Were there any noticeable delays or bottlenecks while accessing network resources or the internet?

☐ Yes
☐ No
☐ Maybe

Comment Suggestions

Your answer

Name *

Your answer

Email *

Your answer

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Figure 49 User feedback form - iv

2.7 Suggest a maintenance schedule to support the networked system

System	Maintenance Times	Notice
Hardware Systems	8 am – 8 pm, Sundays, only as needed	will provide 24 - 48 hours' notice when taking down our system.
Network Services	8 am – 8 pm, Sundays, only as needed	will provide 24 - 48 hours' notice when taking down our servers.
Network Devices	7 am – 7 pm, Sundays, once a month.	Will provide notification via email 48 hours before service.
Server Maintenance	12 pm – 12 am, Saturdays, once a month	when a longer downtime is required, will provide 24 - 48 hours notify
Data Backups	6pm, Sundays, once a week	Will be notified via email
Security and Virus protection	once a month, only as needed	48-hour notice to all occupants
Networking & Internet Infrastructure (including wireless system)	5 am - 7.30 am, Thursday	No additional notice.
Telephone	No weekly schedule required	Will provide 24 - 48 hours' notice when taking down the phone/email service.

Table 8 Maintenance Schedule

Activity 03

3.1 Implement a networked system based on a prepared design

The system was structured by isolating the plan to Building A and B, updating PC and Router configurations, adding IP course directions, and enabling remote access. Switch setups were completed, VLANs were named, and VLANs were allocated. IP configurations were given to all divisions. Screenshots demonstrated PC pinging from within, among, and between VLANs. A show directions test was conducted to show all running setups. Follow-up was conducted to monitor bounces transmitted between offices.

3.1.1 PC Configuration

Building A

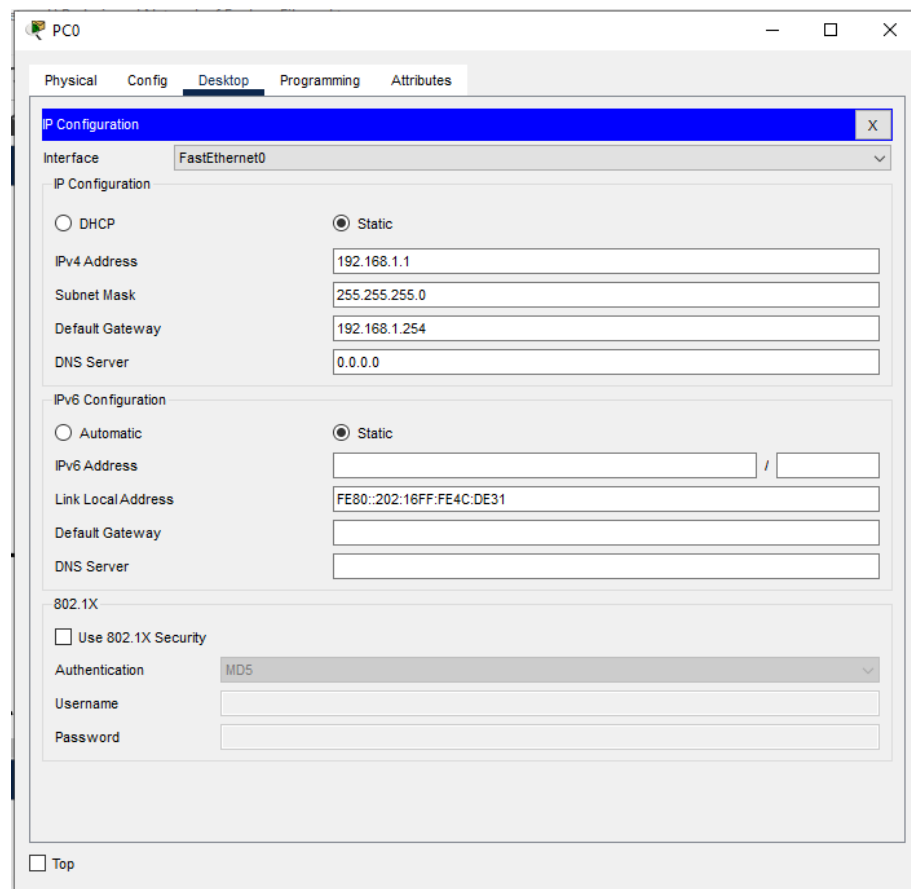


Figure 50 PC Configuration (Sales)

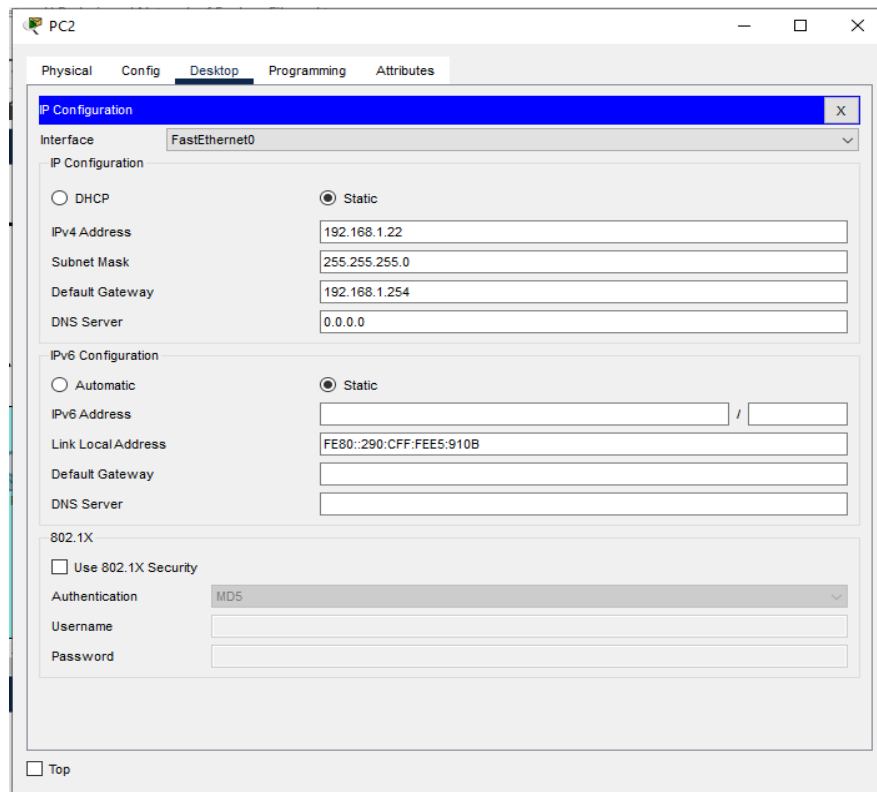


Figure 51 PC Configuration (General Office & Manager's)

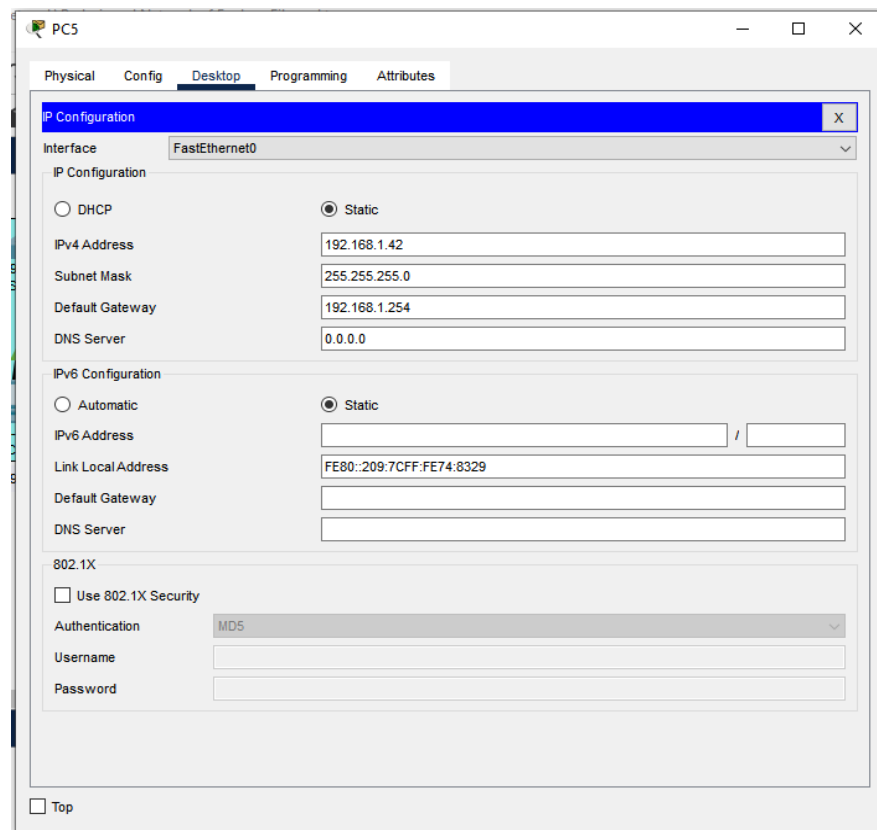
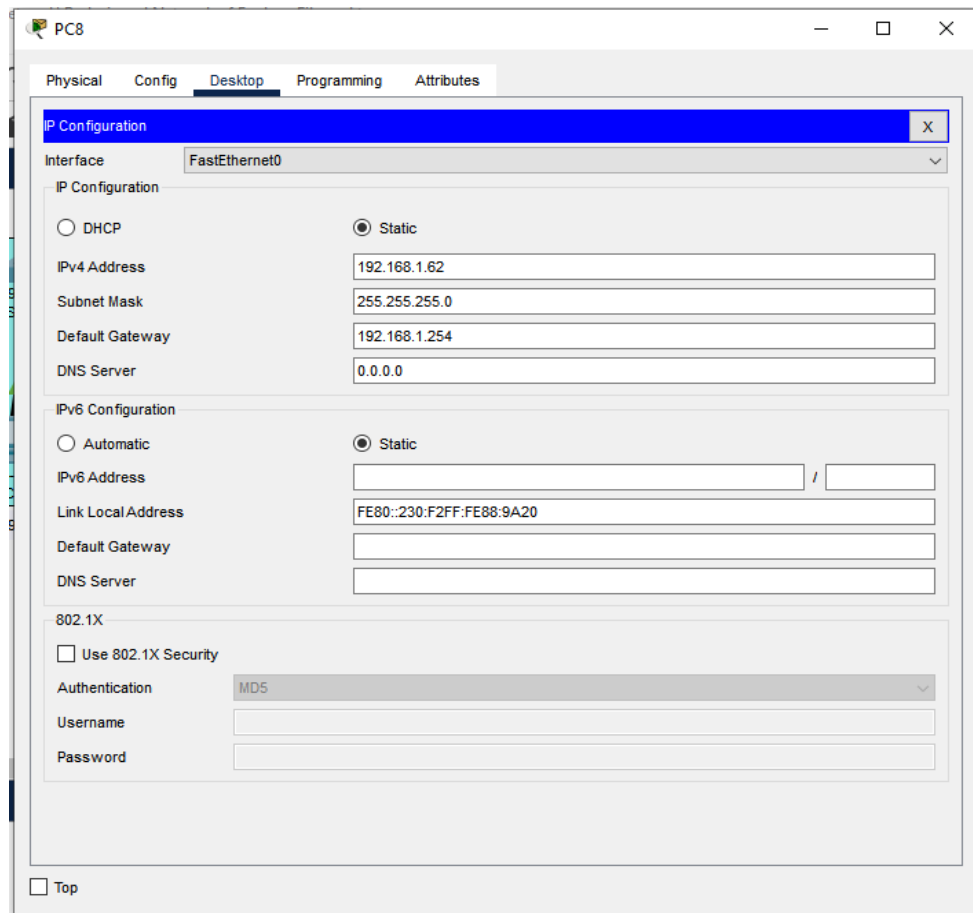


Figure 52 PC Configuration (Administration)



PC8

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.62

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::230:F2FF:FE88:9A20

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

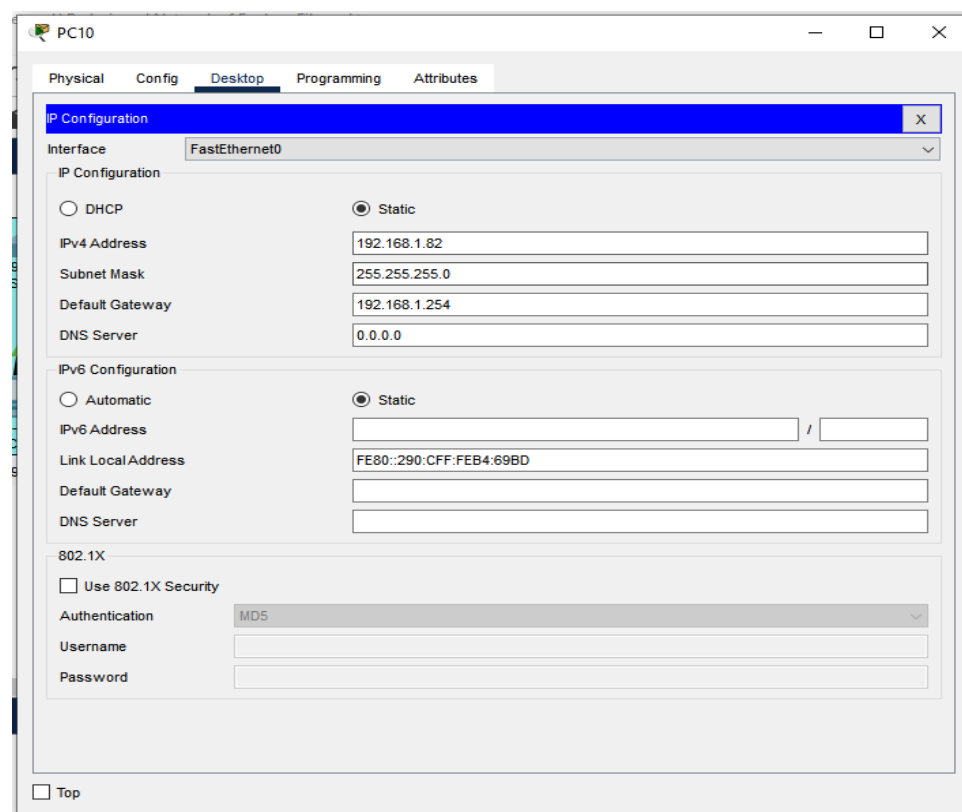
Authentication: MD5

Username:

Password:

☐ Top

Figure 53 PC Configuration (Accounts)



PC10

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.82

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::290:CFF:FE84:69BD

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Figure 54 PC Configuration (Customer & Reception Area)

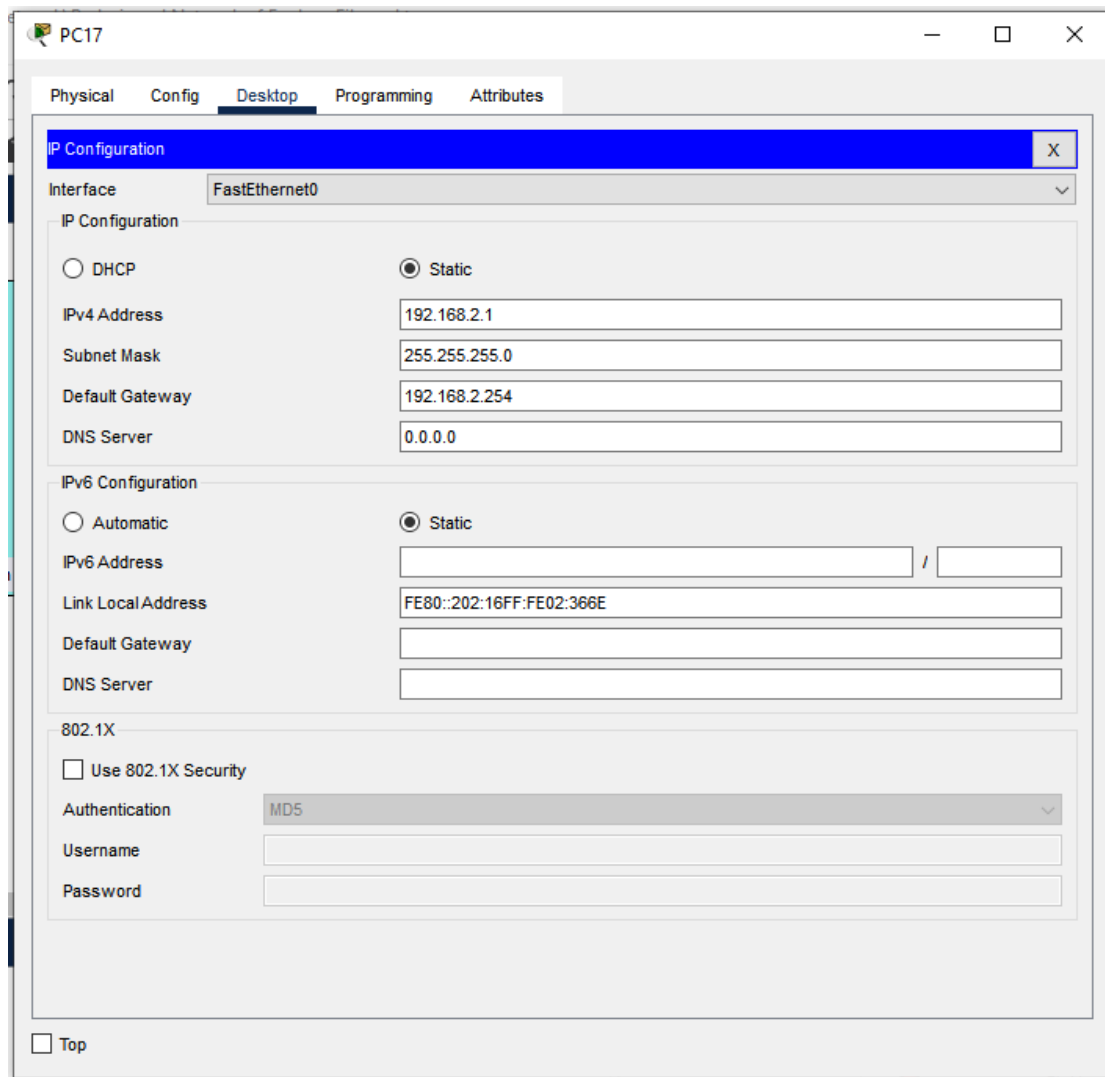
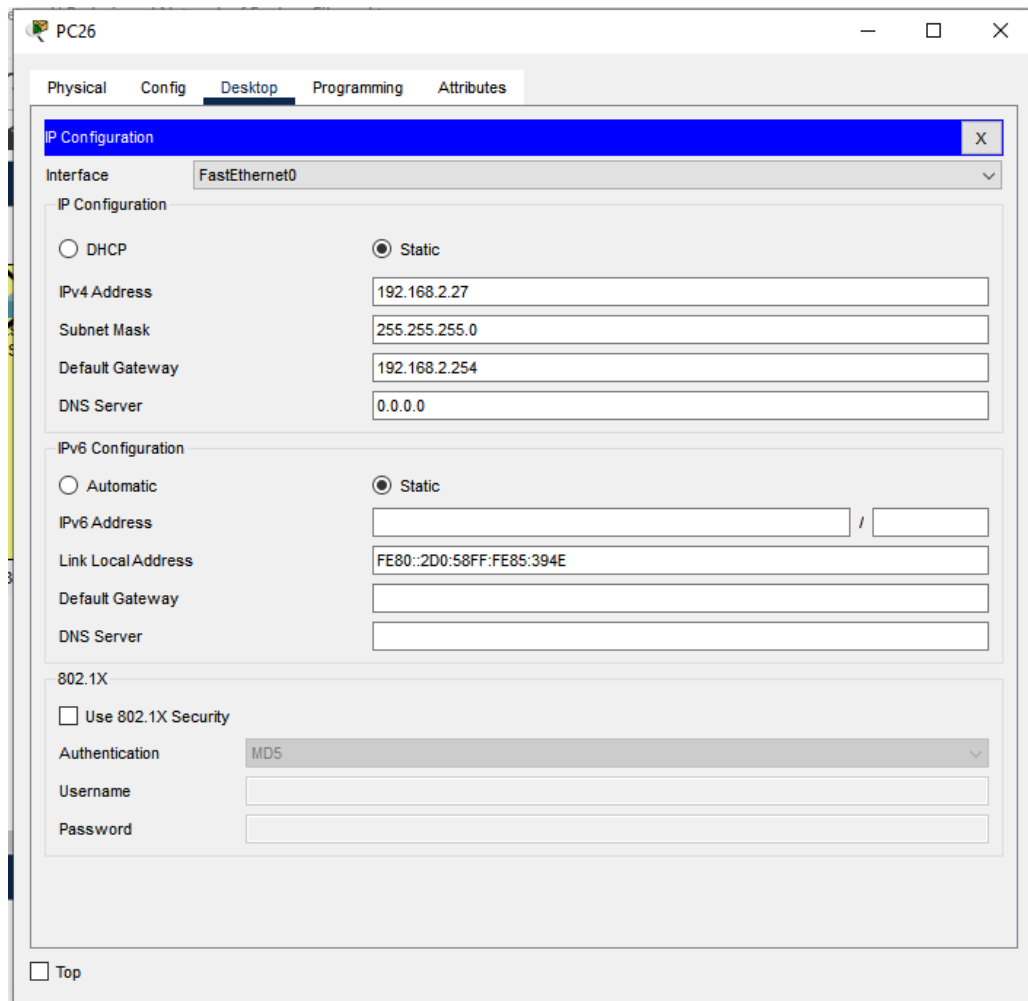


Figure 55 PC Configuration (Media Development & Storage)



The image shows a configuration window for a PC named 'PC26'. The window has four tabs: 'Physical', 'Config', 'Desktop', and 'Attributes'. The 'Desktop' tab is selected. Inside the 'Desktop' tab, there is a sub-tab 'IP Configuration'. The 'Interface' dropdown is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.2.27, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.254, and DNS Server: 0.0.0.0. Under 'IPv6 Configuration', the 'Static' radio button is also selected. The fields are: IPv6 Address (empty), Link Local Address: FE80::2D0:58FF:FE85:394E, Default Gateway (empty), and DNS Server (empty). Under '802.1X', the 'Use 802.1X Security' checkbox is unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty. A 'Top' button is at the bottom left.

Figure 56 PC Configuration (Office)

3.1.2 Switch Configuration

Building A

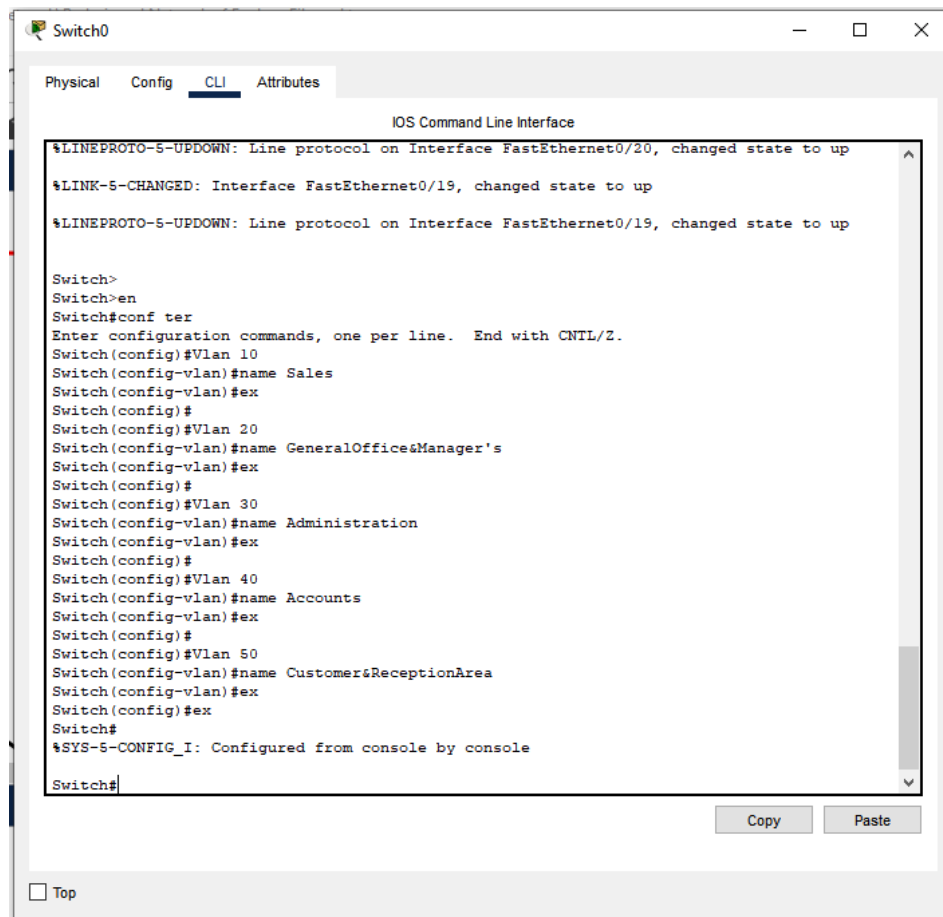


Figure 57 Switch Configuration (Naming VLANs)

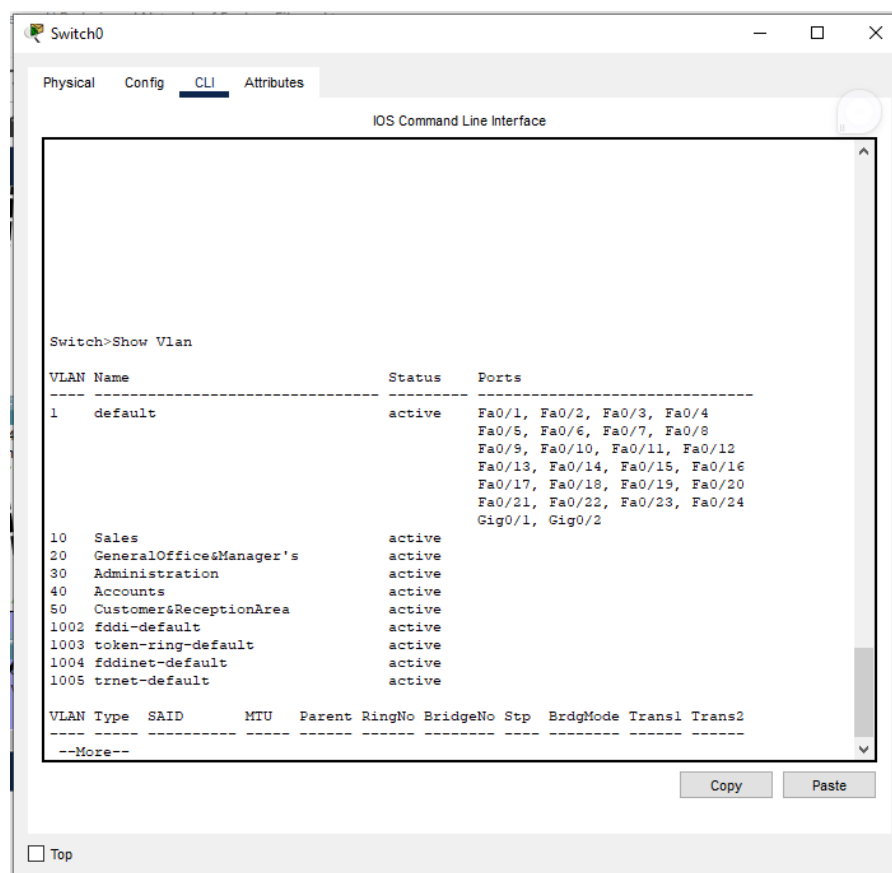


Figure 58 Show VLANs

Building B

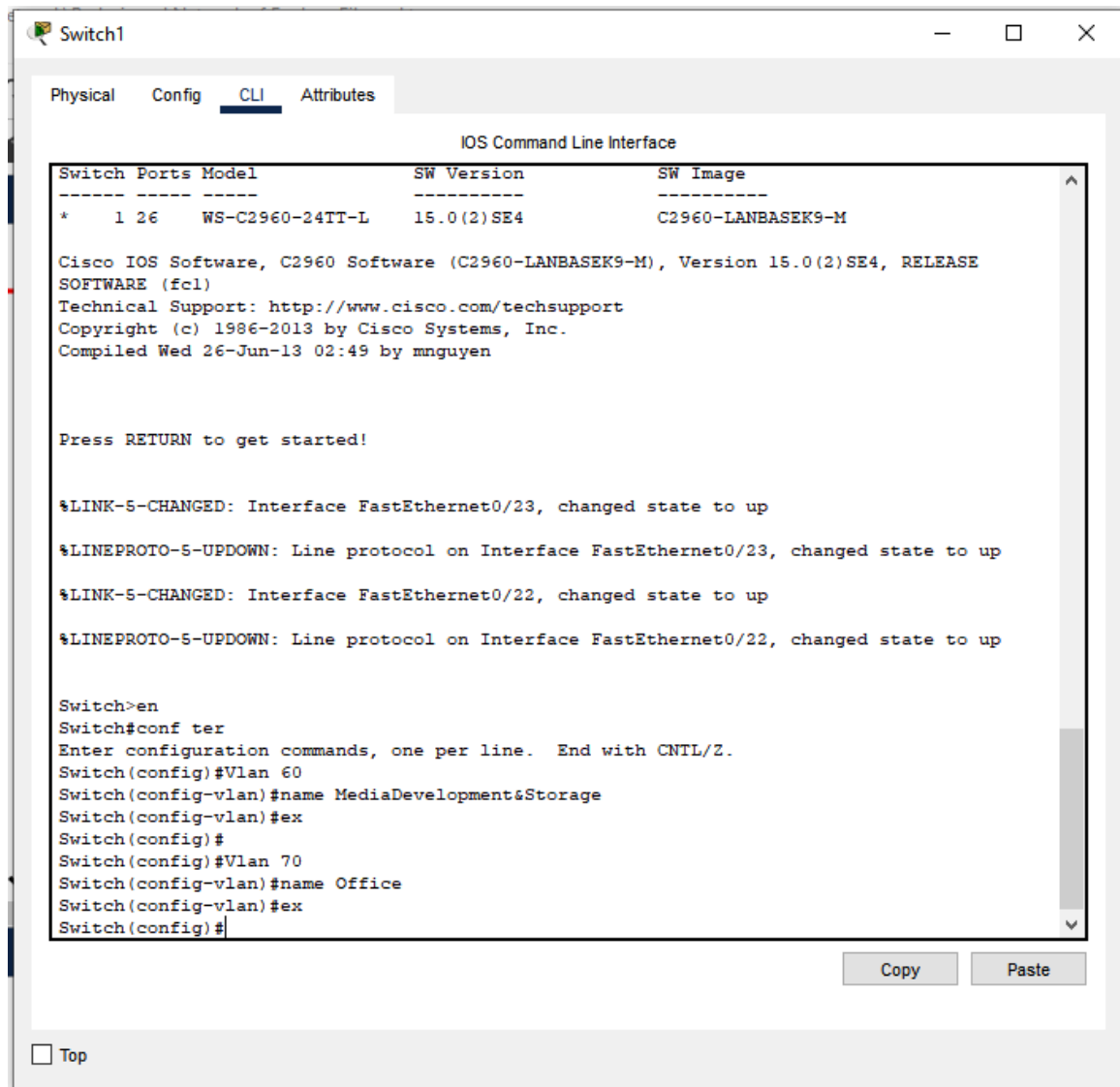


Figure 59 Switch Configuration (Naming VLANs)

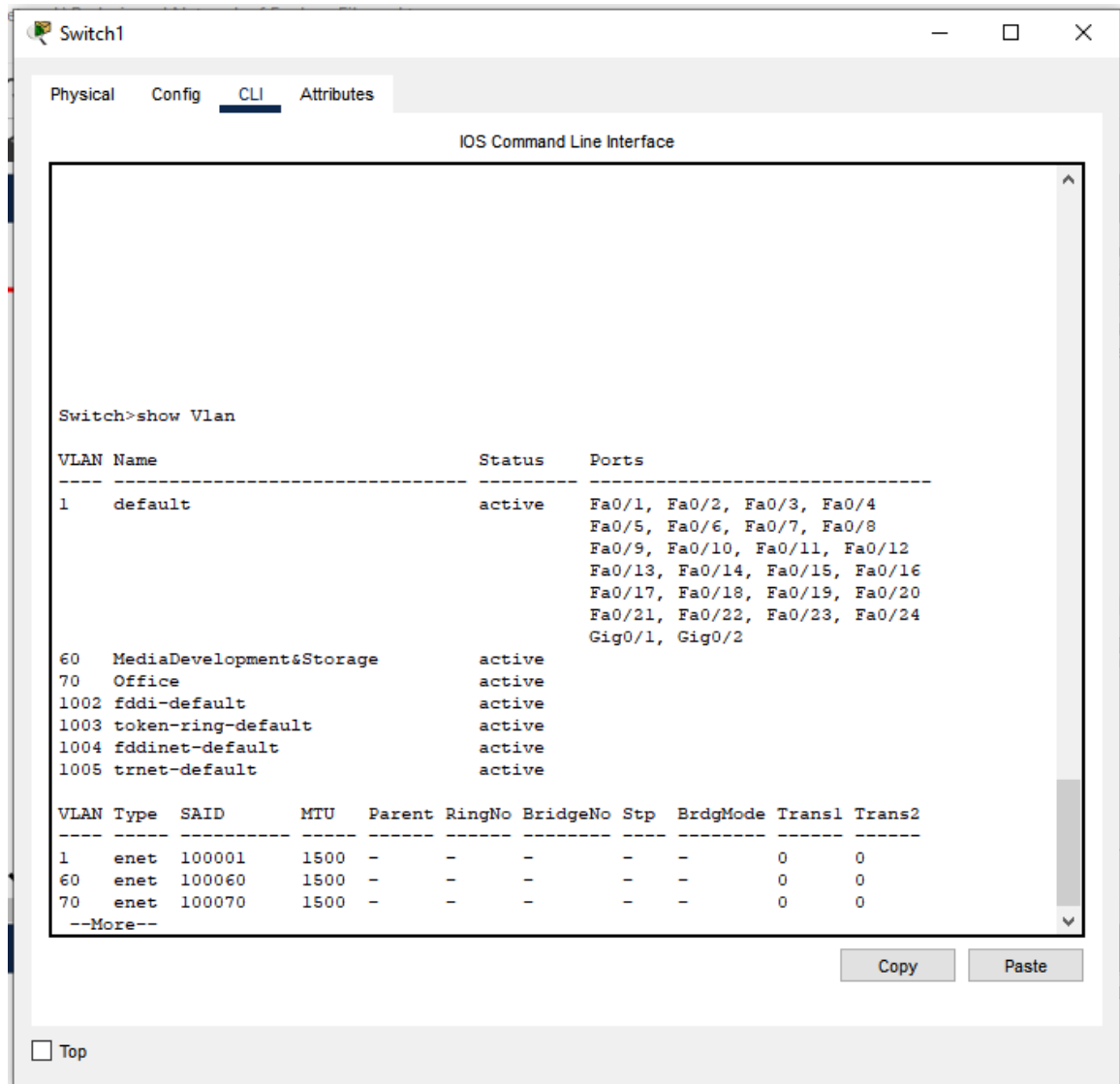


Figure 60 Show VLANs

3.1.3 Router Configuration

Building A

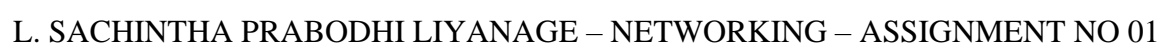


Figure 62 Shows the IP route (Building A)

Building B

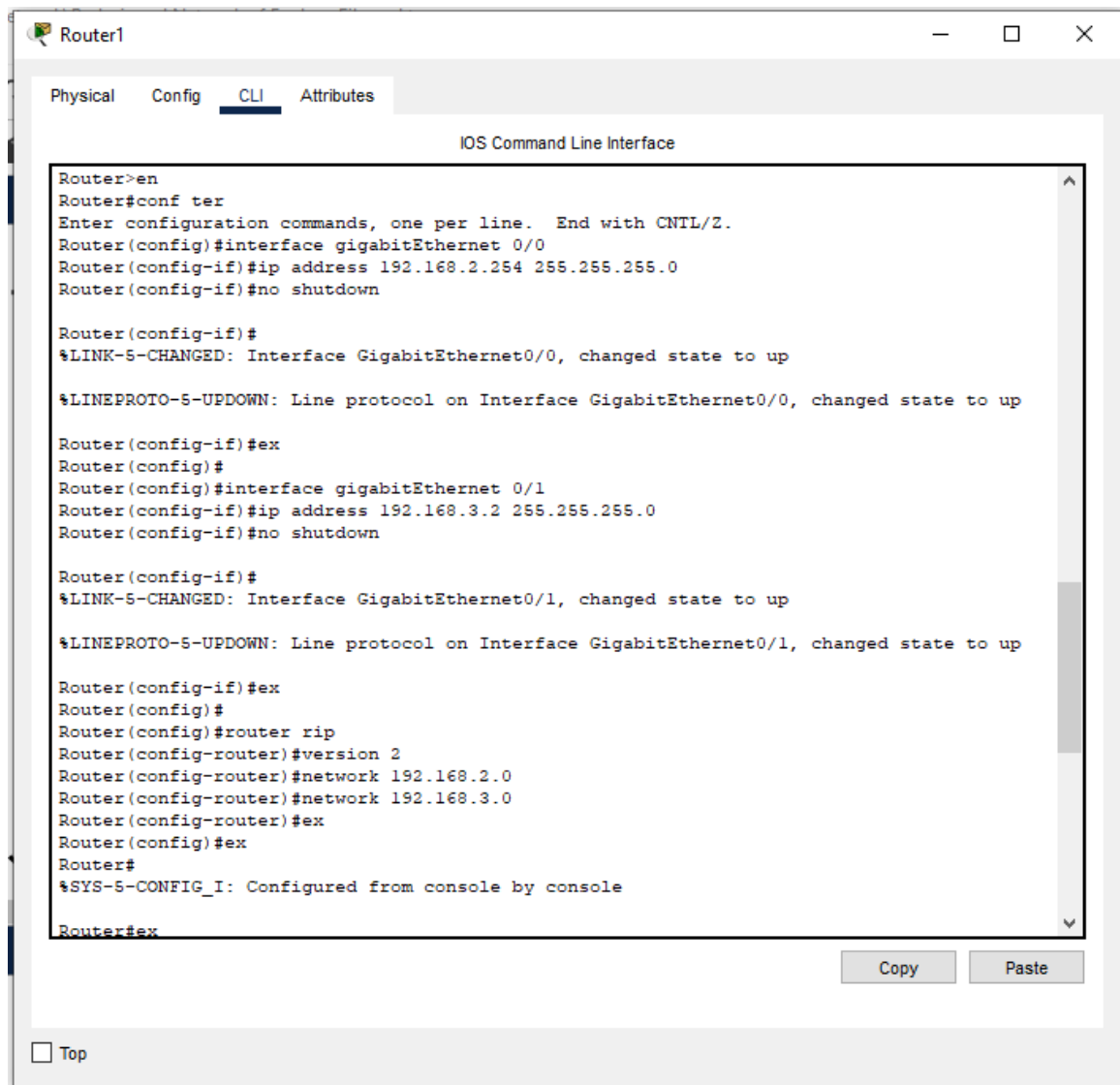


Figure 63 Router Configuration (Building B)



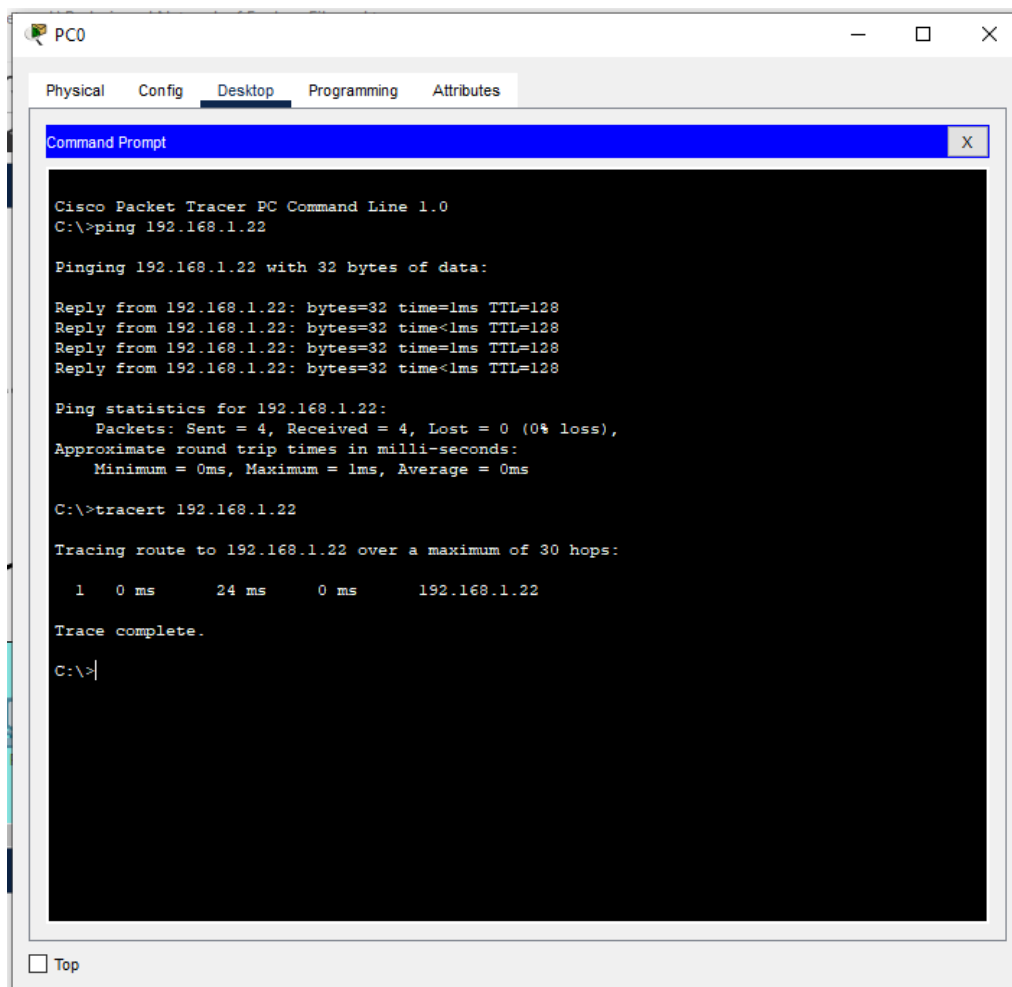
3.2 Conduct verification & Analyse test results against expected outcomes

3.2.1 Ping

The ping command is a widely used utility for quick reachability verification, sending five ICMP packets to a destination and returning five if reachability exists. It can be extended and customized with various options, including source interface, count, datagram size, timeout, pattern, and Type of Service.

Building A

Sales Department



```
PC0
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.22

Pinging 192.168.1.22 with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time=1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128
Reply from 192.168.1.22: bytes=32 time=1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 192.168.1.22

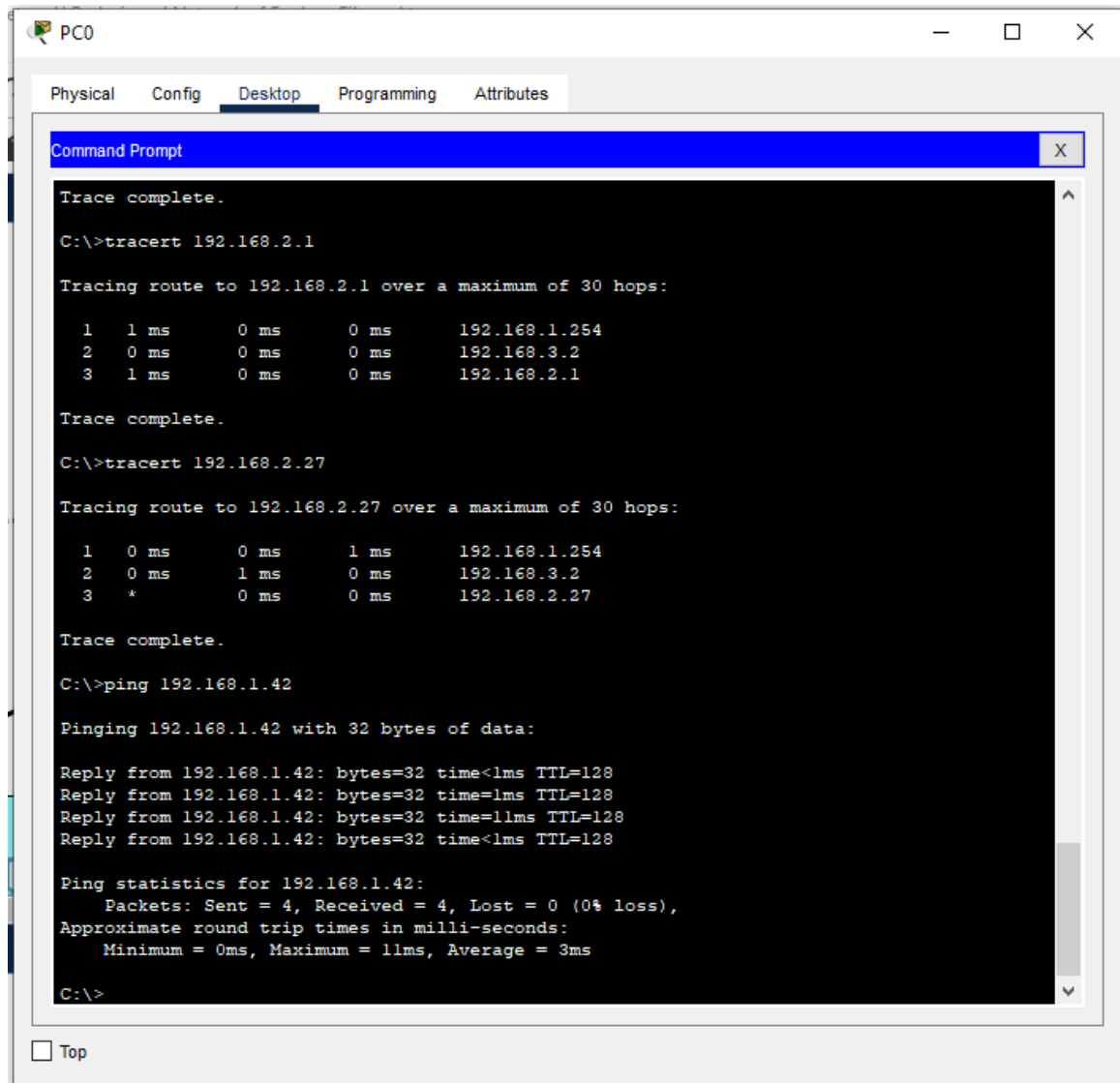
Tracing route to 192.168.1.22 over a maximum of 30 hops:

  1  0 ms      24 ms      0 ms      192.168.1.22

Trace complete.

C:\>
```

Figure 65 Test case pinging from Sales Department to General Office & Manager's



The screenshot shows a PC0 window with a Command Prompt open. The Command Prompt displays the results of three network tests: two traceroute commands and one ping command. The first traceroute is to 192.168.2.1, the second to 192.168.2.27, and the ping is to 192.168.1.42. The results show successful connections with no packet loss and low latency.

```

Trace complete.
C:\>tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    192.168.1.254
  2  0 ms    0 ms    0 ms    192.168.3.2
  3  1 ms    0 ms    0 ms    192.168.2.1

Trace complete.
C:\>tracert 192.168.2.27

Tracing route to 192.168.2.27 over a maximum of 30 hops:

  1  0 ms    0 ms    1 ms    192.168.1.254
  2  0 ms    1 ms    0 ms    192.168.3.2
  3  *        0 ms    0 ms    192.168.2.27

Trace complete.
C:\>ping 192.168.1.42

Pinging 192.168.1.42 with 32 bytes of data:

Reply from 192.168.1.42: bytes=32 time<1ms TTL=128
Reply from 192.168.1.42: bytes=32 time=1ms TTL=128
Reply from 192.168.1.42: bytes=32 time=11ms TTL=128
Reply from 192.168.1.42: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
  
```

Figure 66 Test case pinging from Sales Department to Administration Department

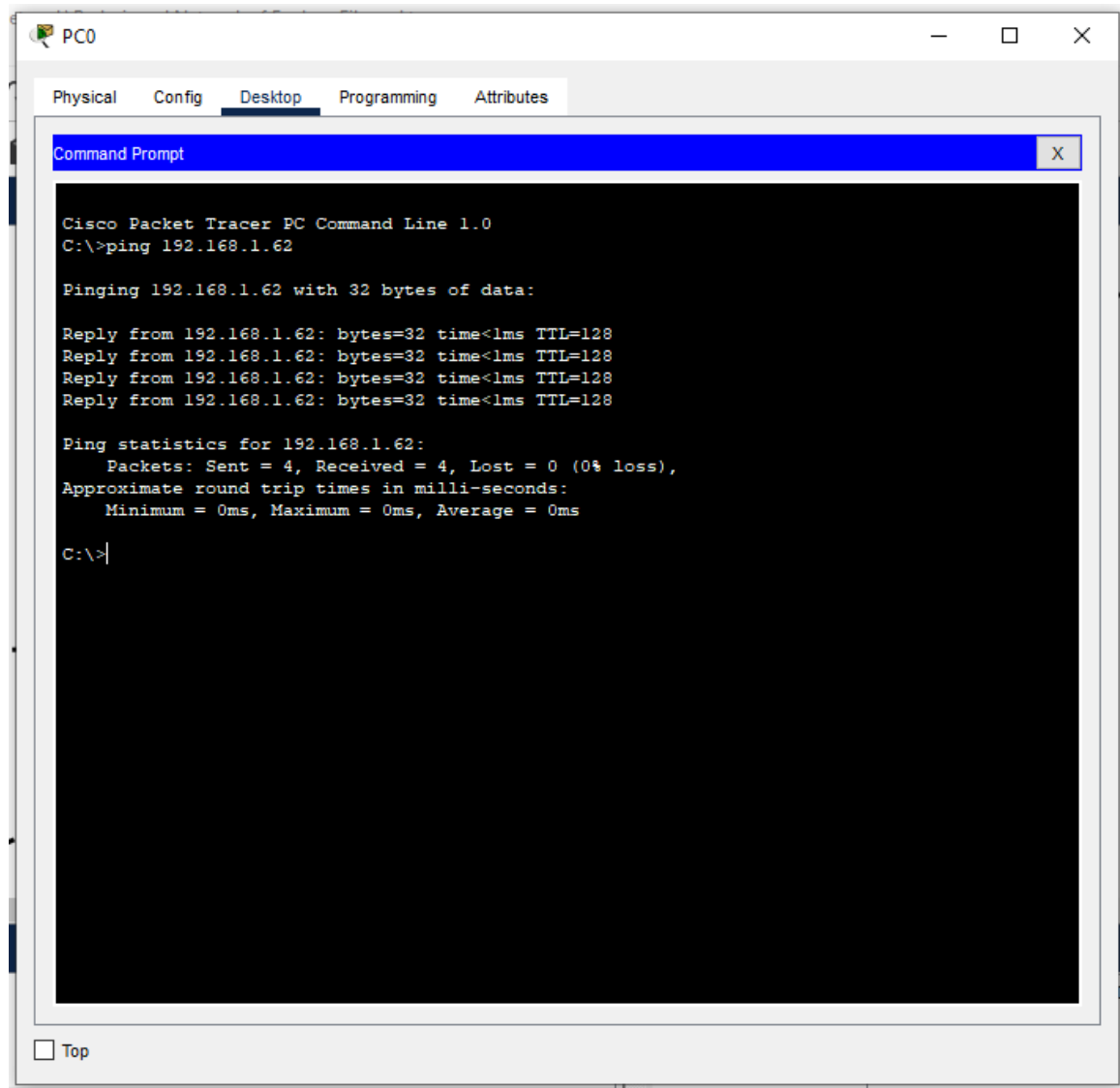
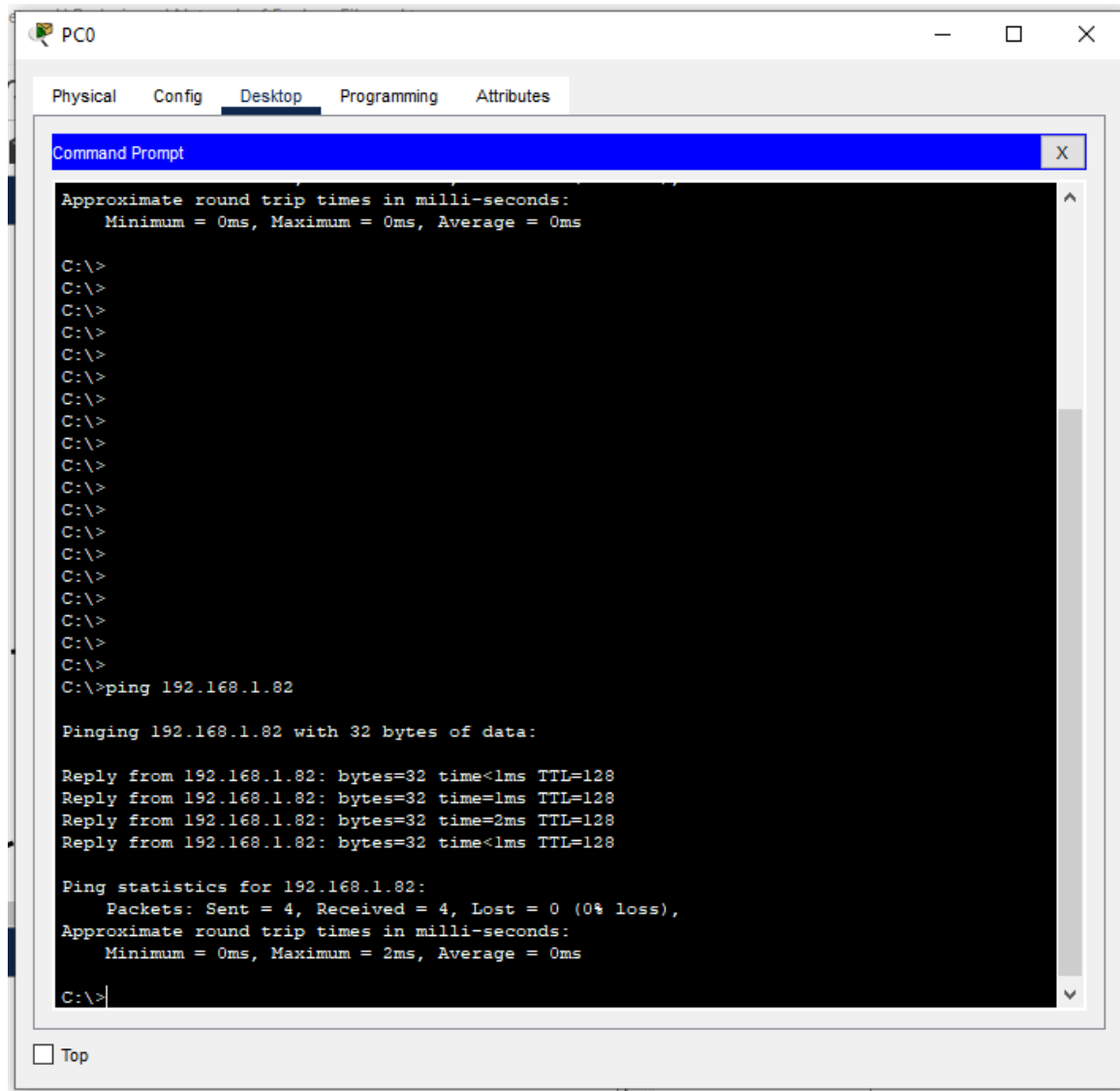


Figure 67 Test case pinging from Sales Department to Accounts Department



```

PC0
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.82

Pinging 192.168.1.82 with 32 bytes of data:

Reply from 192.168.1.82: bytes=32 time<1ms TTL=128
Reply from 192.168.1.82: bytes=32 time=1ms TTL=128
Reply from 192.168.1.82: bytes=32 time=2ms TTL=128
Reply from 192.168.1.82: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
  
```

Figure 68 Test case pinging from Sales Department to Customer & Reception Area

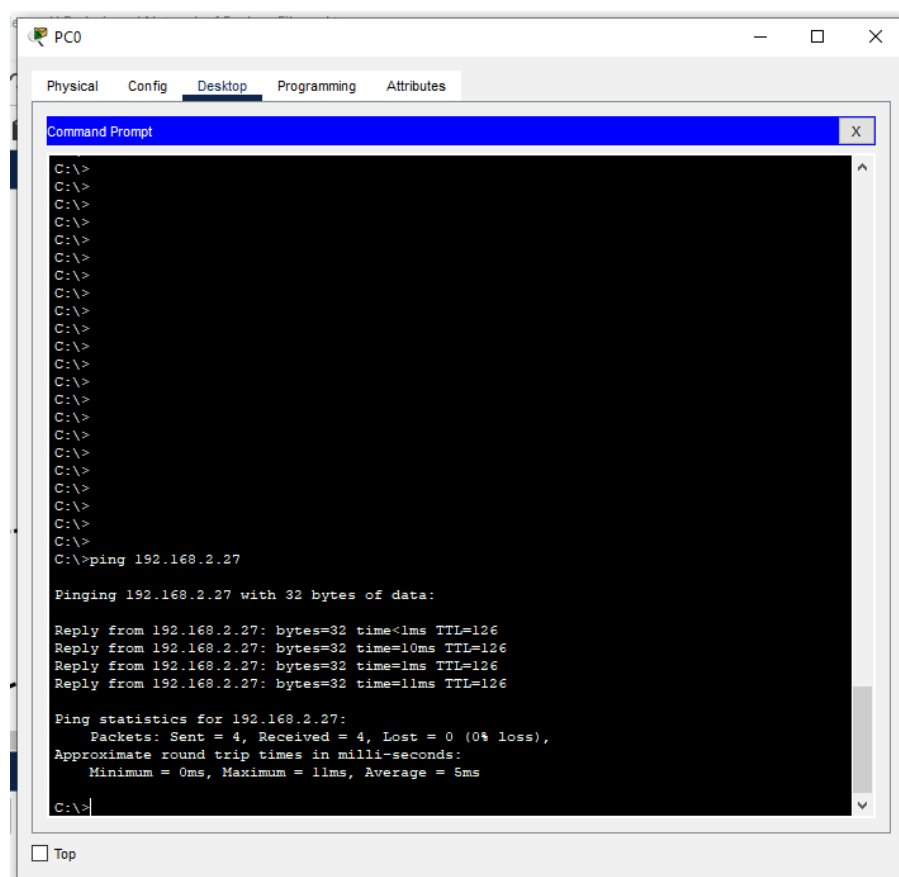
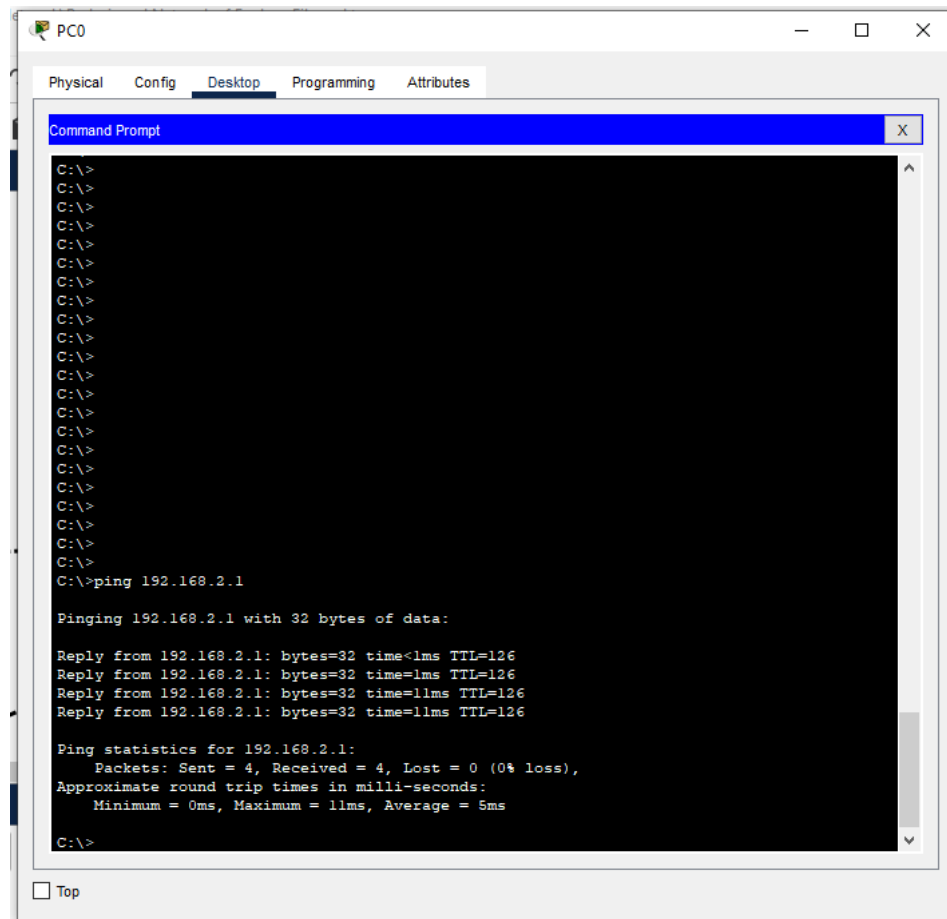


Figure 70 Test case pinging from Sales Department to Office

General Office & Manager's Department

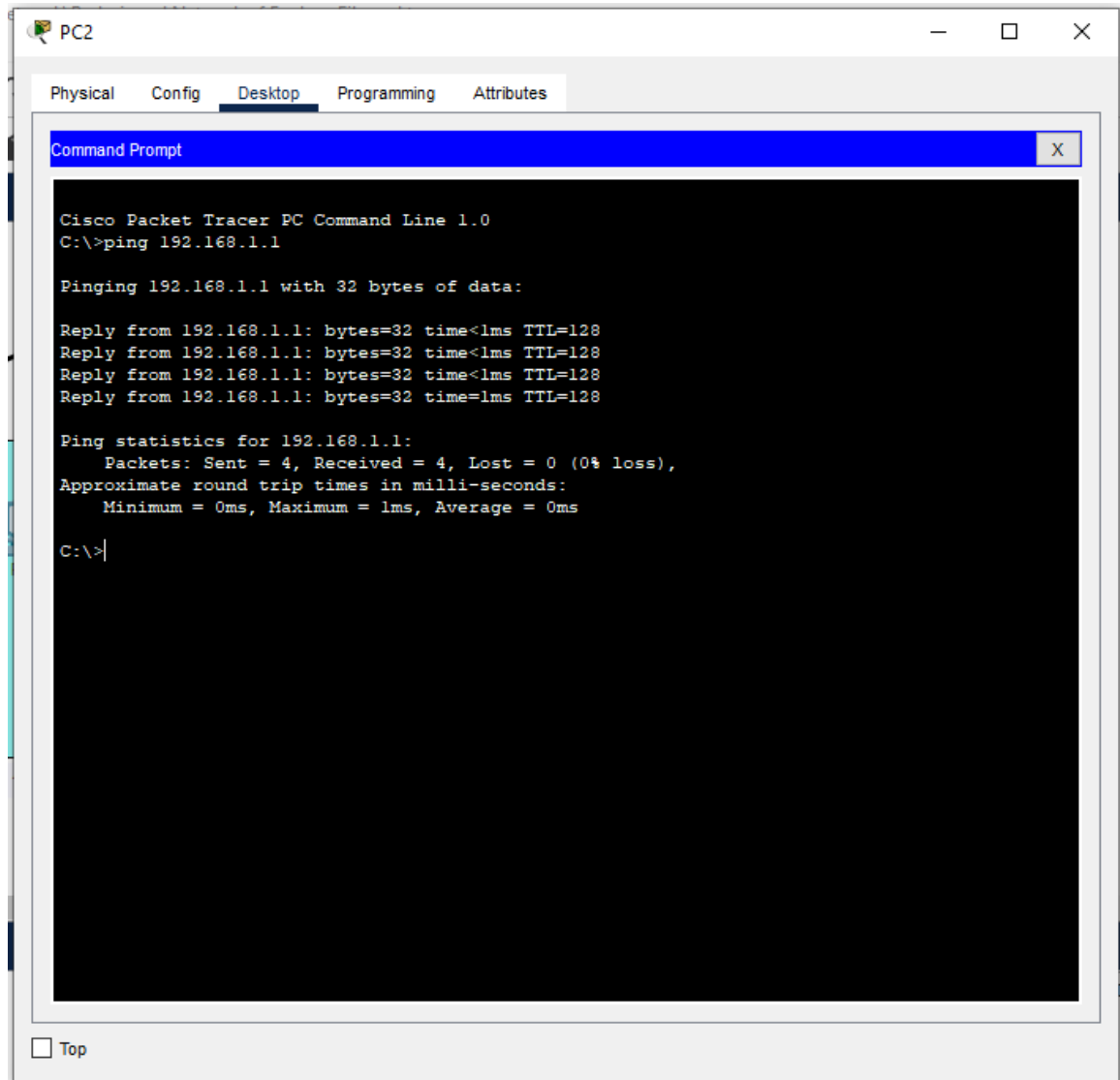
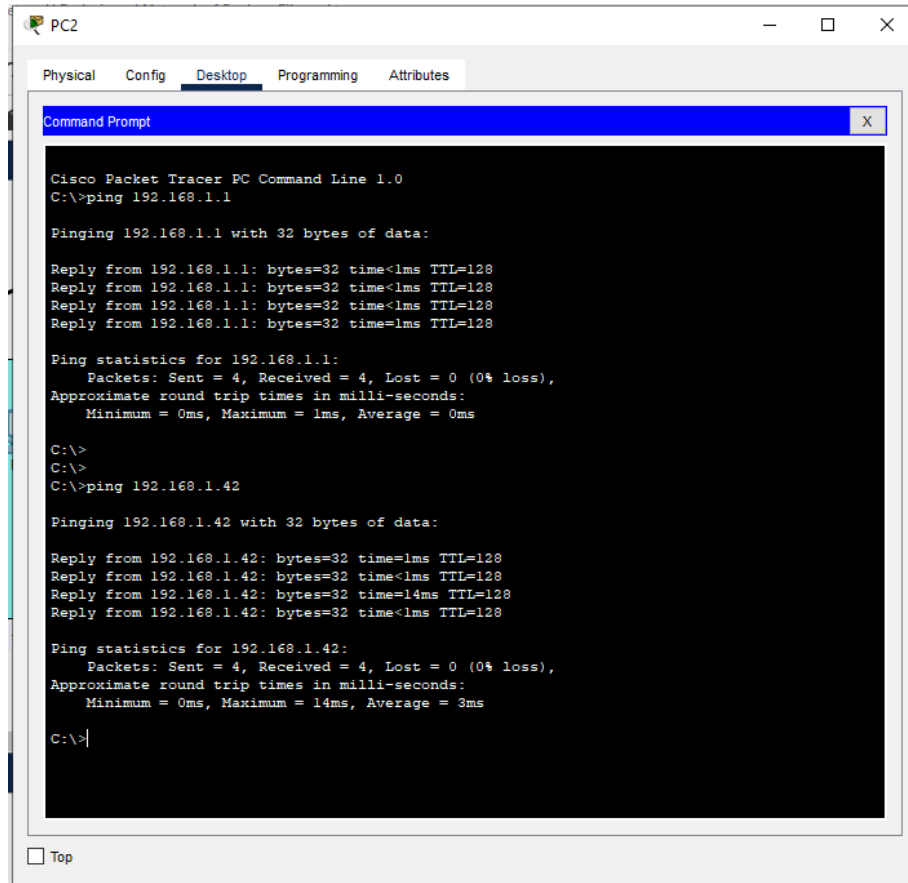


Figure 71 Test case pinging from General Office & Manager's to Sales Department



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
C:\>ping 192.168.1.42

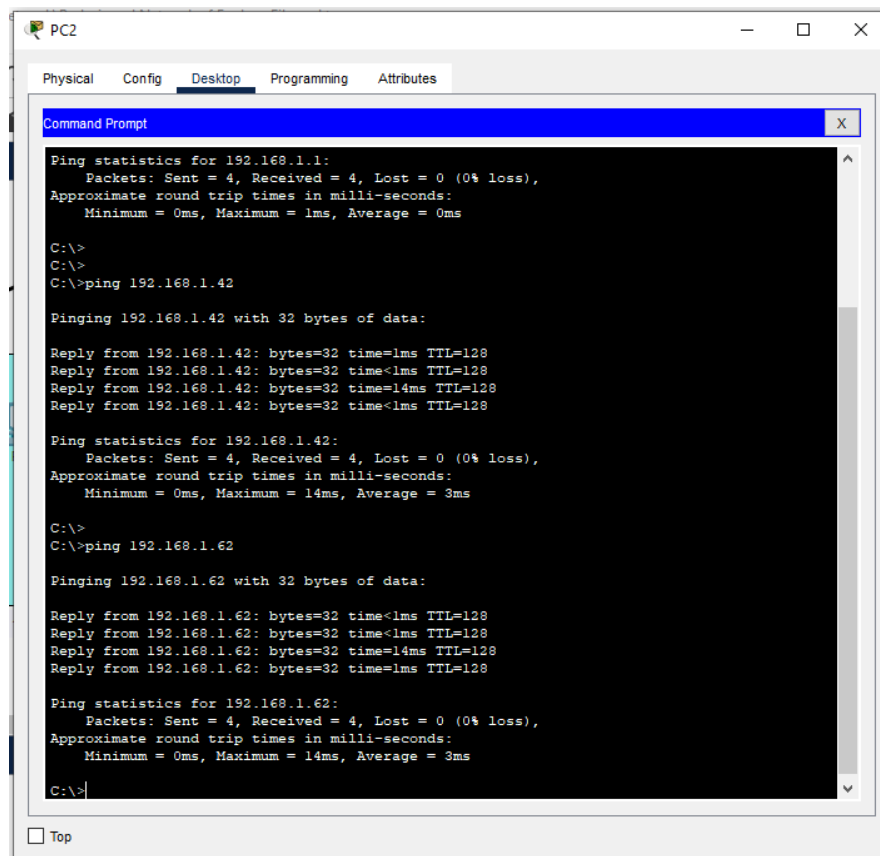
Pinging 192.168.1.42 with 32 bytes of data:

Reply from 192.168.1.42: bytes=32 time<1ms TTL=128
Reply from 192.168.1.42: bytes=32 time<1ms TTL=128
Reply from 192.168.1.42: bytes=32 time=14ms TTL=128
Reply from 192.168.1.42: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>
  
```

Figure 72 Test case pinging from General Office & Manager's to Administration Department



```

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
C:\>ping 192.168.1.42

Pinging 192.168.1.42 with 32 bytes of data:

Reply from 192.168.1.42: bytes=32 time<1ms TTL=128
Reply from 192.168.1.42: bytes=32 time<1ms TTL=128
Reply from 192.168.1.42: bytes=32 time=14ms TTL=128
Reply from 192.168.1.42: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>
C:\>ping 192.168.1.62

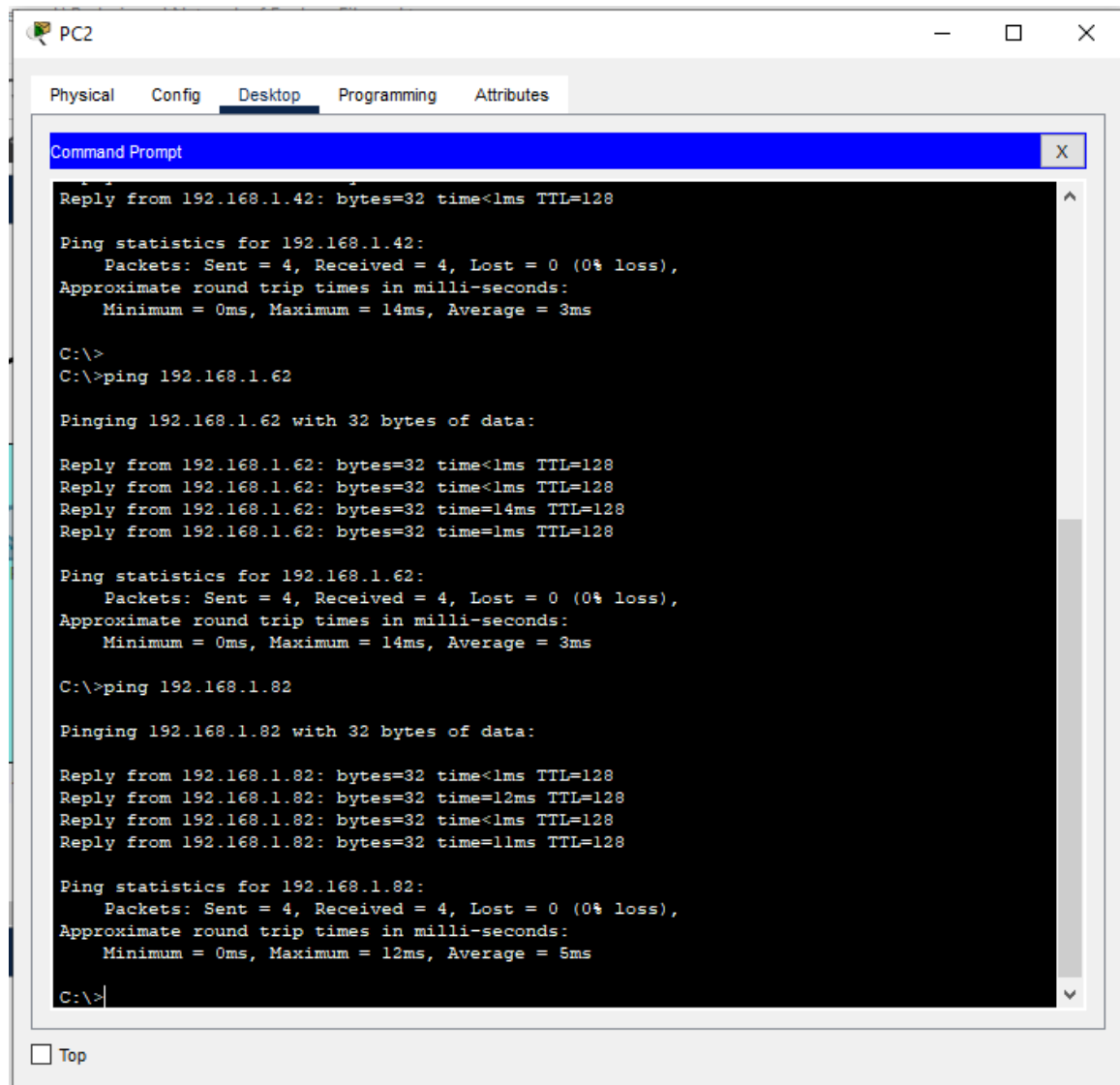
Pinging 192.168.1.62 with 32 bytes of data:

Reply from 192.168.1.62: bytes=32 time<1ms TTL=128
Reply from 192.168.1.62: bytes=32 time<1ms TTL=128
Reply from 192.168.1.62: bytes=32 time=14ms TTL=128
Reply from 192.168.1.62: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>
  
```

Figure 73 Test case pinging from General Office & Manager's to Accounts Department



```

PC2
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Reply from 192.168.1.42: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>
C:\>ping 192.168.1.62

Pinging 192.168.1.62 with 32 bytes of data:

Reply from 192.168.1.62: bytes=32 time<1ms TTL=128
Reply from 192.168.1.62: bytes=32 time<1ms TTL=128
Reply from 192.168.1.62: bytes=32 time=14ms TTL=128
Reply from 192.168.1.62: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>ping 192.168.1.82

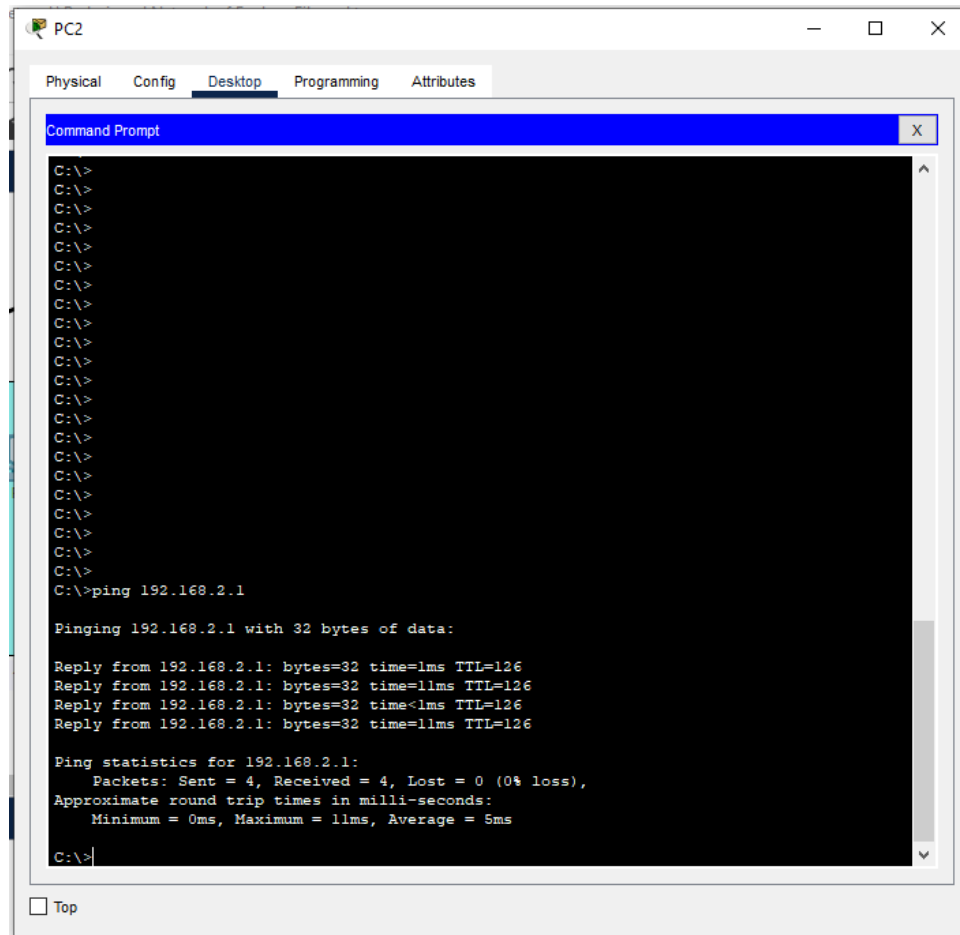
Pinging 192.168.1.82 with 32 bytes of data:

Reply from 192.168.1.82: bytes=32 time<1ms TTL=128
Reply from 192.168.1.82: bytes=32 time=12ms TTL=128
Reply from 192.168.1.82: bytes=32 time<1ms TTL=128
Reply from 192.168.1.82: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>
  
```

Figure 74 Test case pinging from General Office & Manager's to Customer & Reception Area



```

PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.1

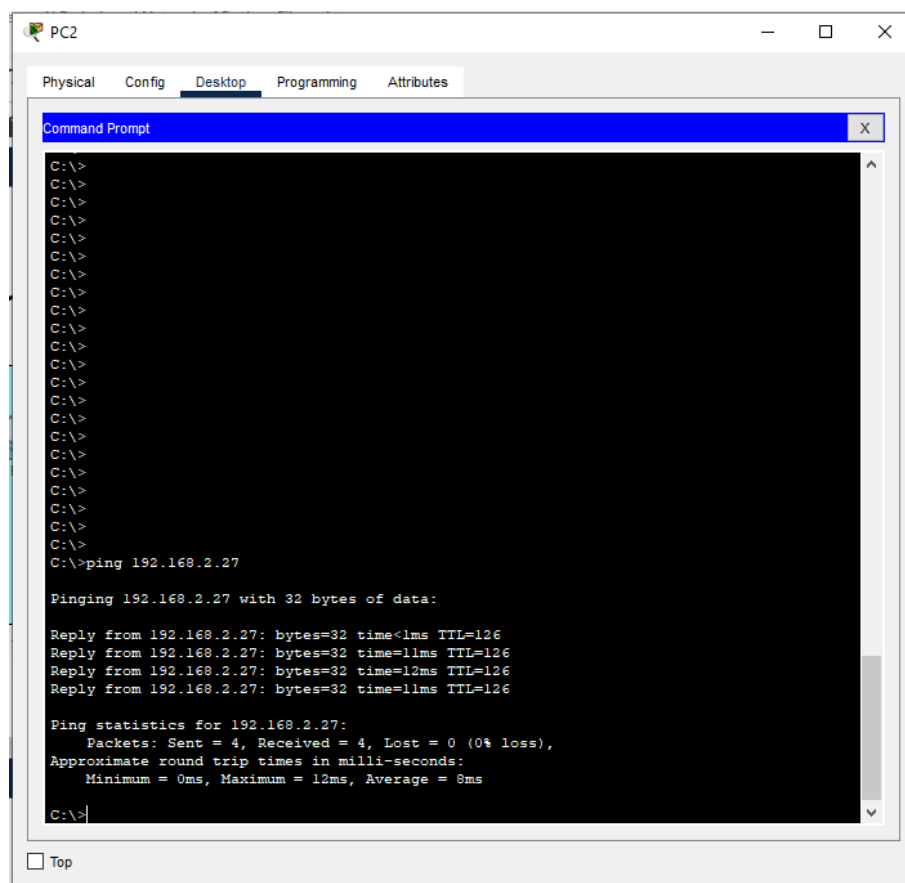
Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=11ms TTL=126
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>
  
```

Figure 75 Test case pinging from General Office & Manager's to Media Development & Storage



```

PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.27

Pinging 192.168.2.27 with 32 bytes of data:

Reply from 192.168.2.27: bytes=32 time<1ms TTL=126
Reply from 192.168.2.27: bytes=32 time=11ms TTL=126
Reply from 192.168.2.27: bytes=32 time=12ms TTL=126
Reply from 192.168.2.27: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 8ms

C:\>
  
```

Figure 76 Test case pinging from General Office & Manager's to Office

Administration Department

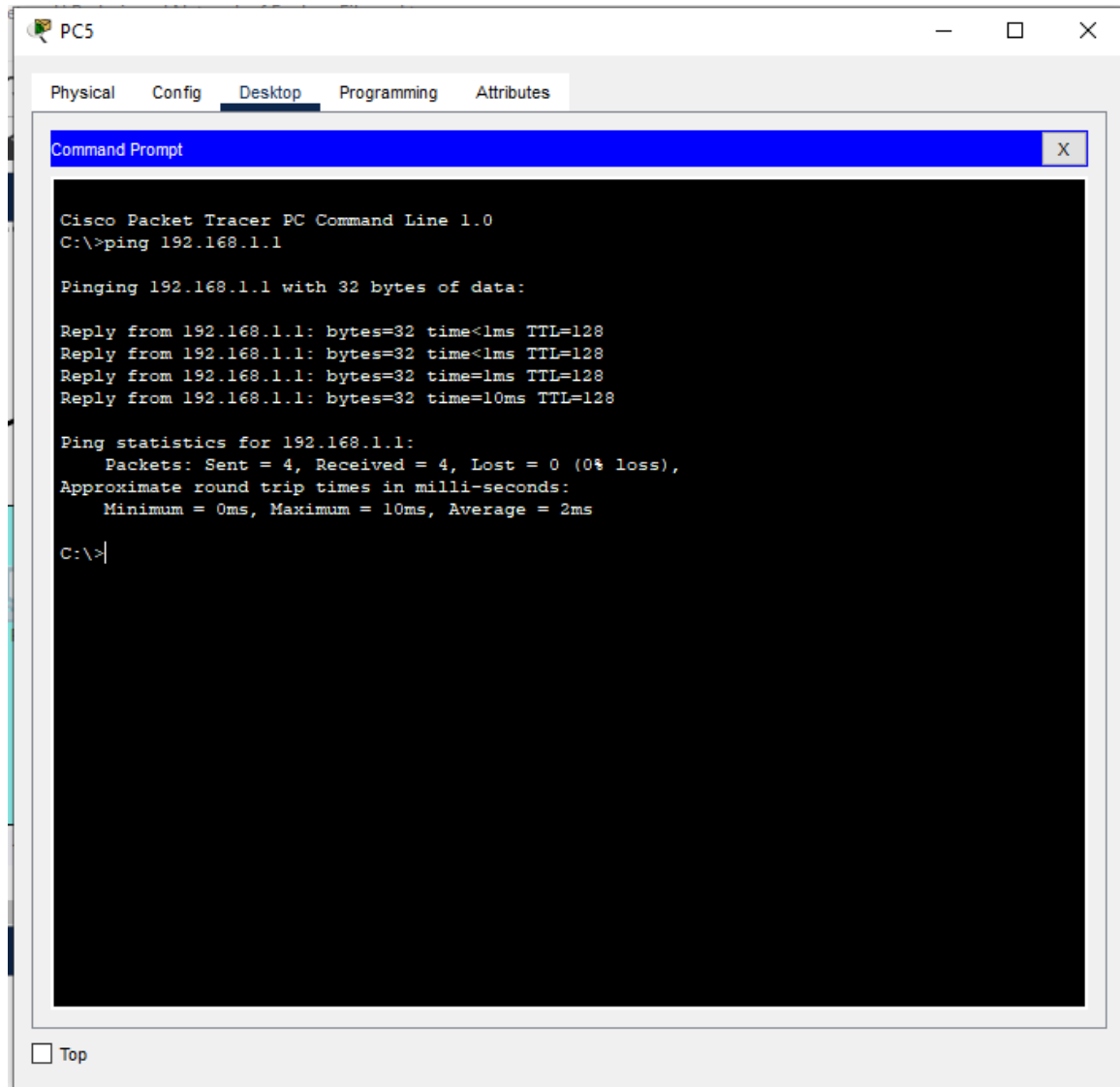


Figure 77 Test case pinging from Administration to Sales Department

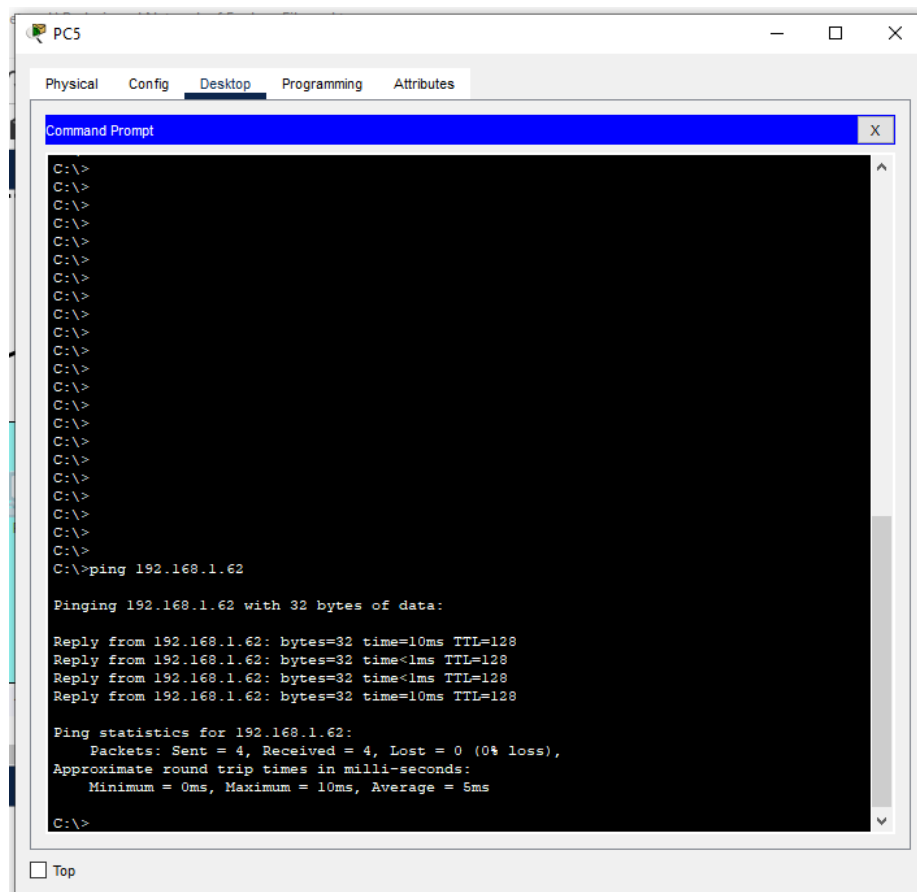
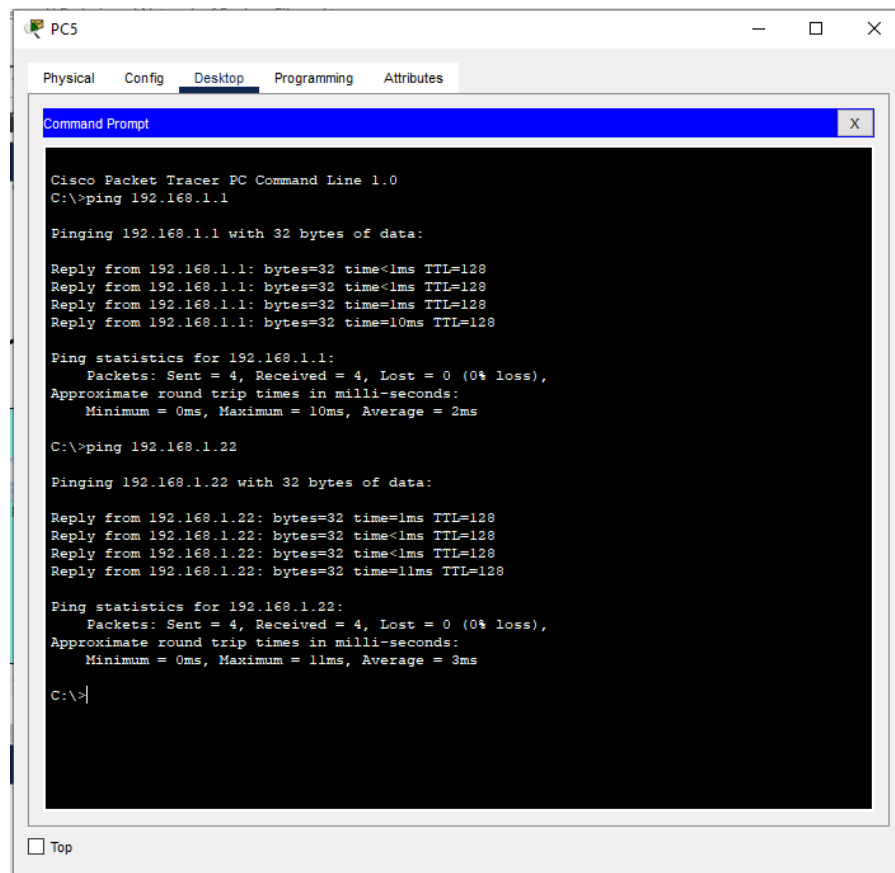


Figure 79 Test case pinging from Administration to General Accounts Department

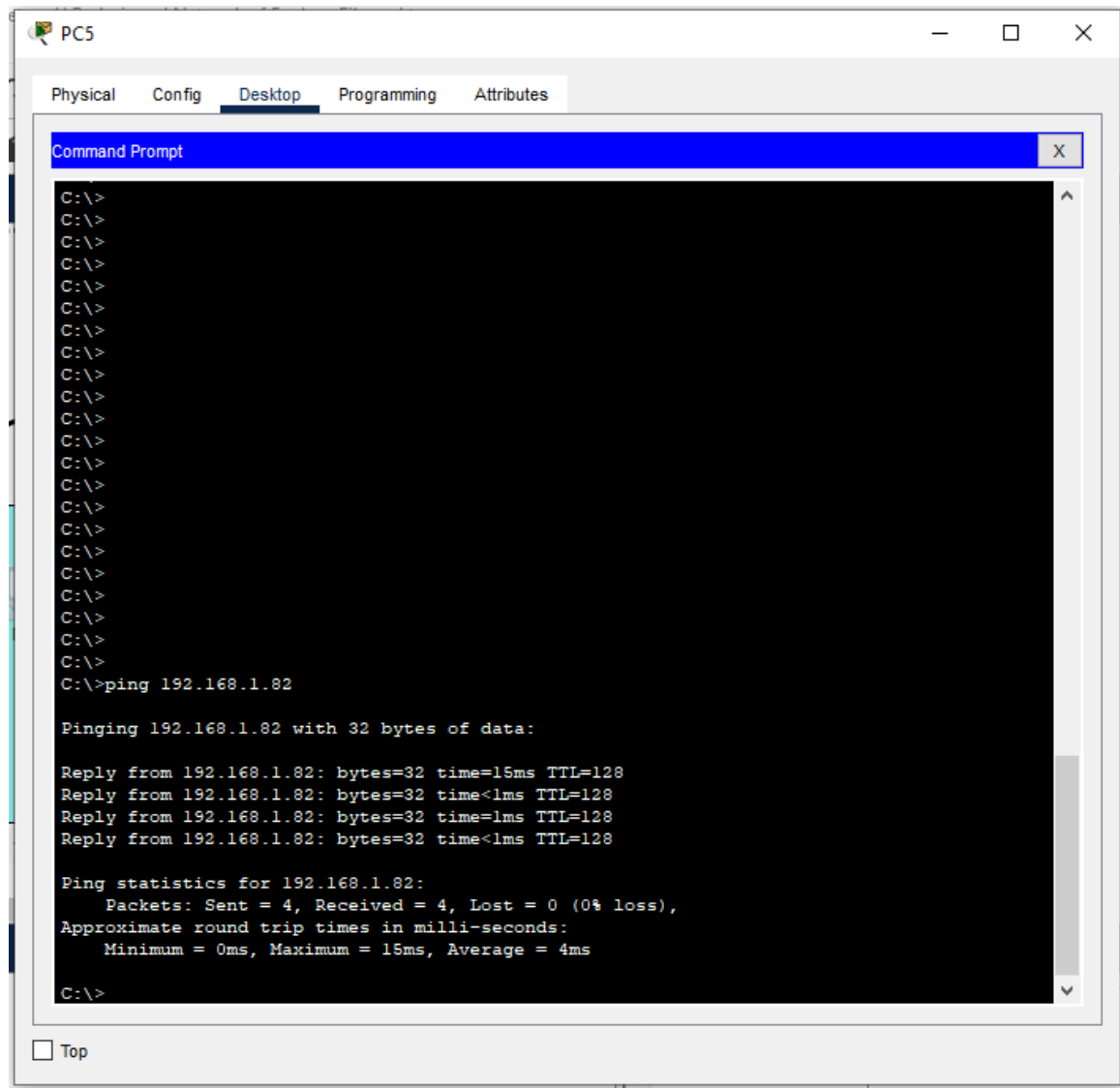
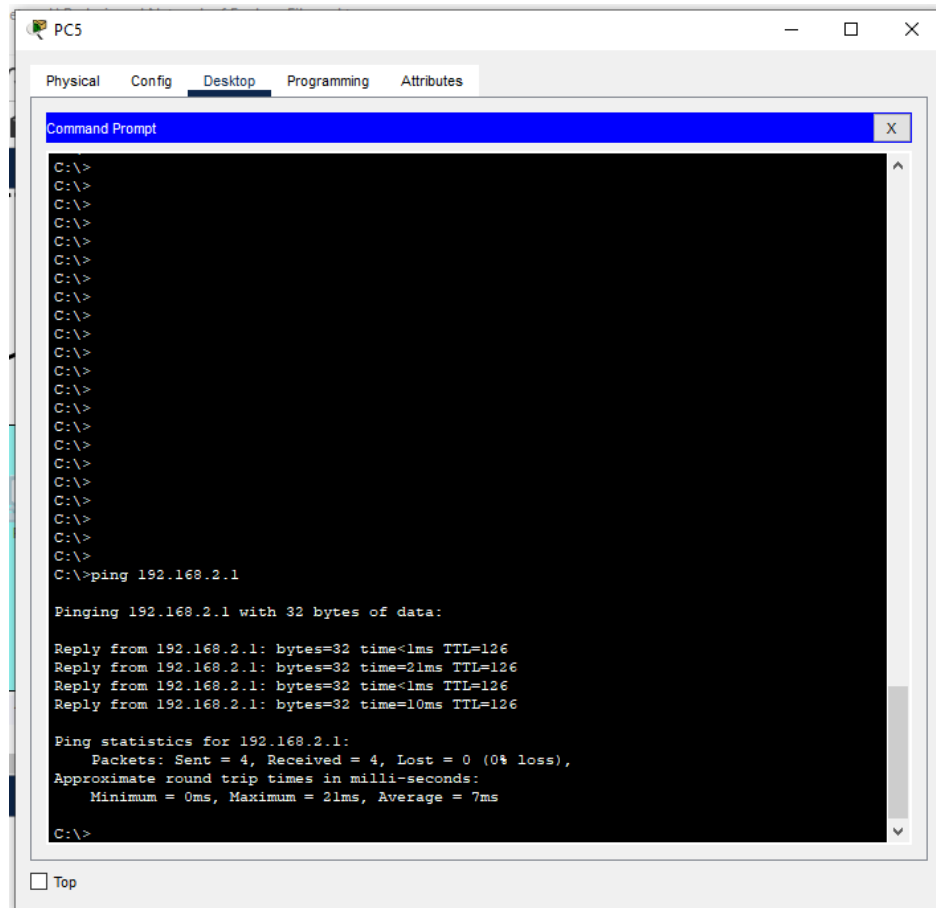


Figure 80 Test case pinging from Administration to General Customer & Reception Area



```

PC5
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.1

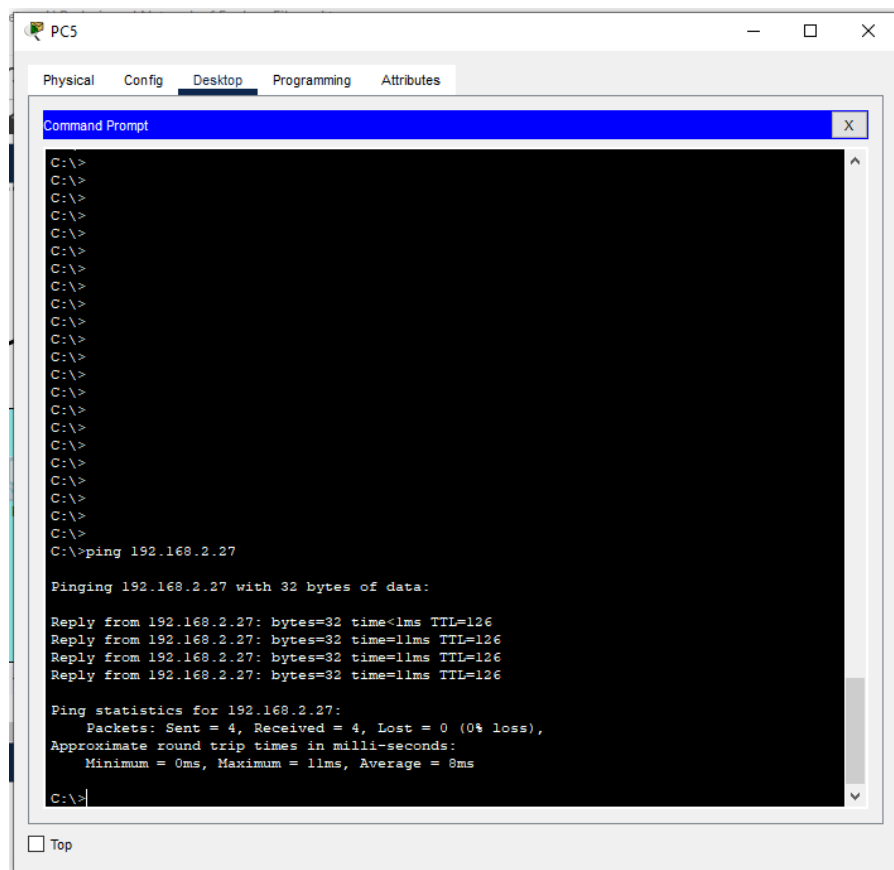
Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=21ms TTL=126
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 21ms, Average = 7ms

C:\>
  
```

Figure 81Test case pinging from Administration to Media Development & Storage



```

PC5
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.27

Pinging 192.168.2.27 with 32 bytes of data:

Reply from 192.168.2.27: bytes=32 time<1ms TTL=126
Reply from 192.168.2.27: bytes=32 time=11ms TTL=126
Reply from 192.168.2.27: bytes=32 time=11ms TTL=126
Reply from 192.168.2.27: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>
  
```


Figure 82 Test case pinging from Administration to Office

Accounts Department

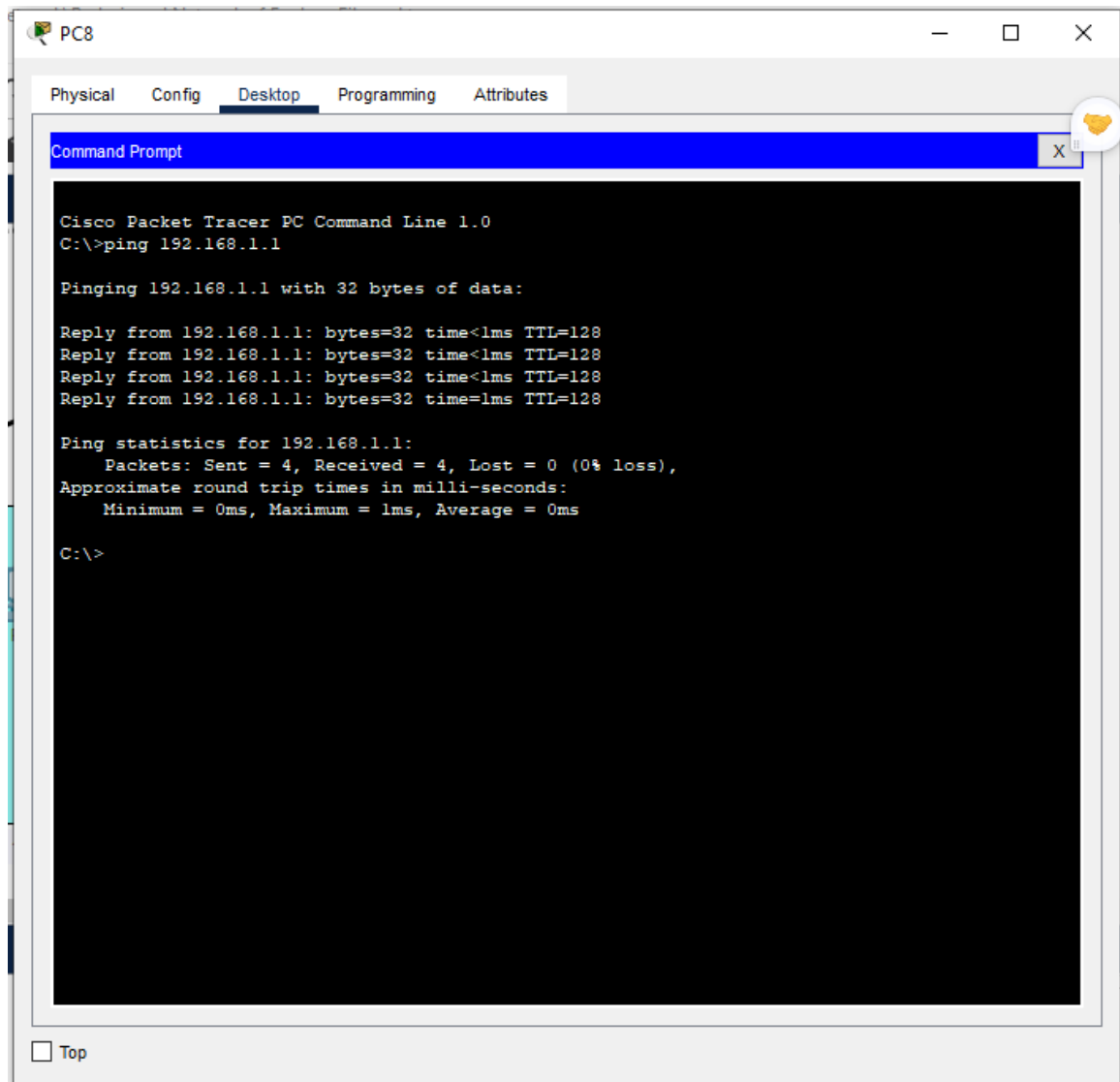
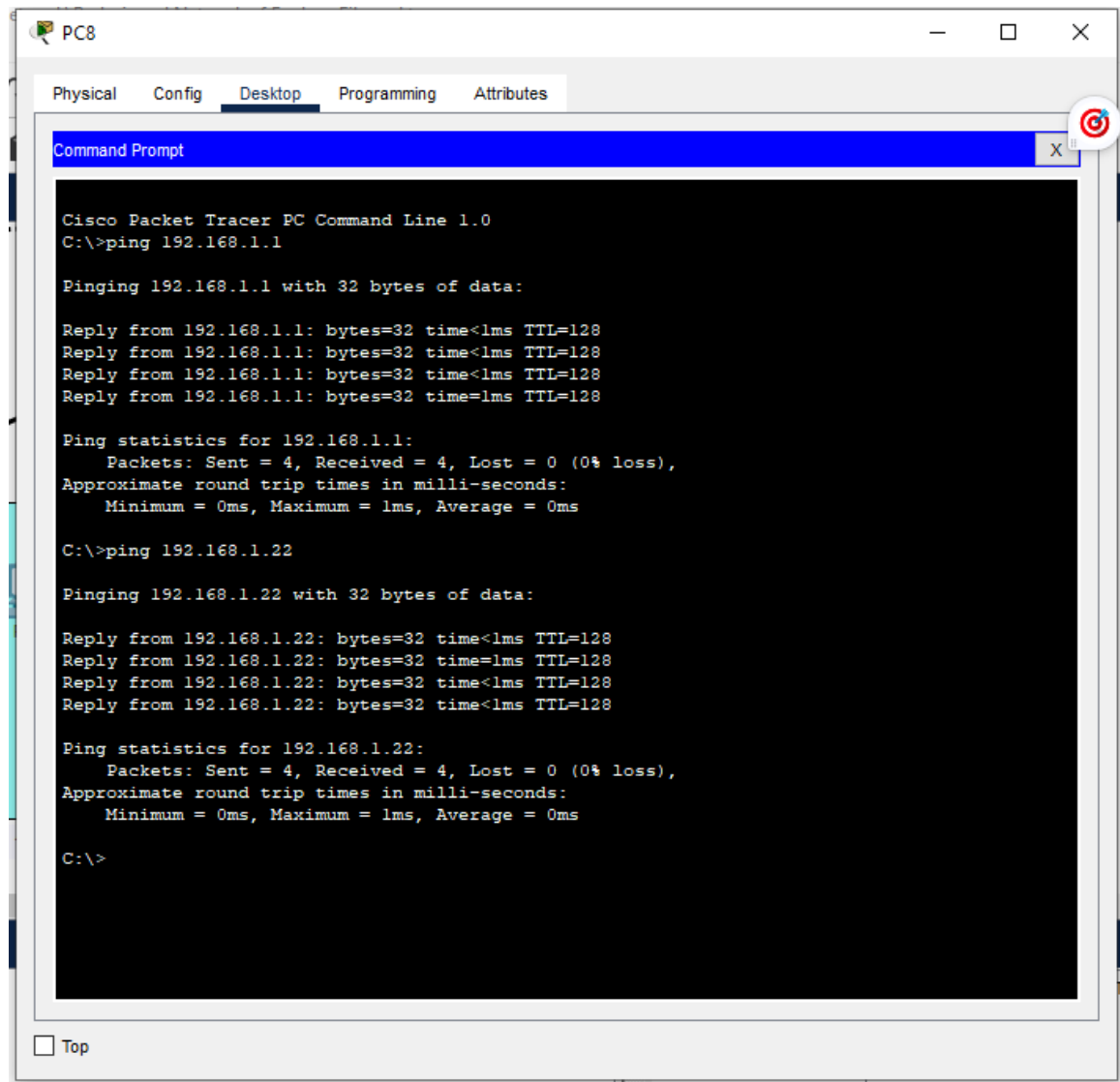


Figure 83 Test case pinging from Accounts to Sales Department



```

PC8
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.22

Pinging 192.168.1.22 with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time<1ms TTL=128
Reply from 192.168.1.22: bytes=32 time=1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Figure 84 Test case pinging from Accounts to General Office & Manager's





Customer & Reception Area

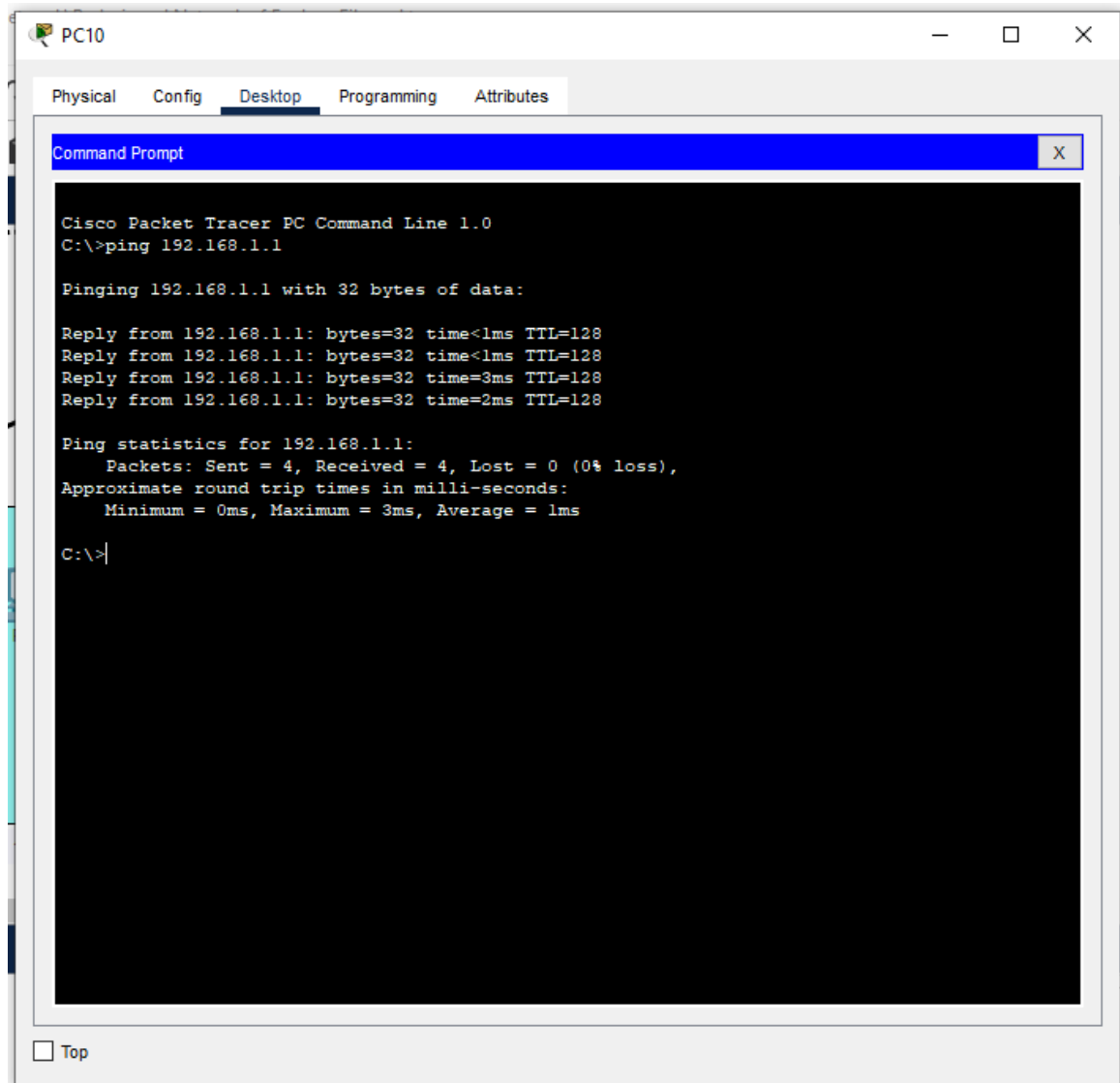


Figure 89 Test case pinging from Customer & Reception Area to Sales Department

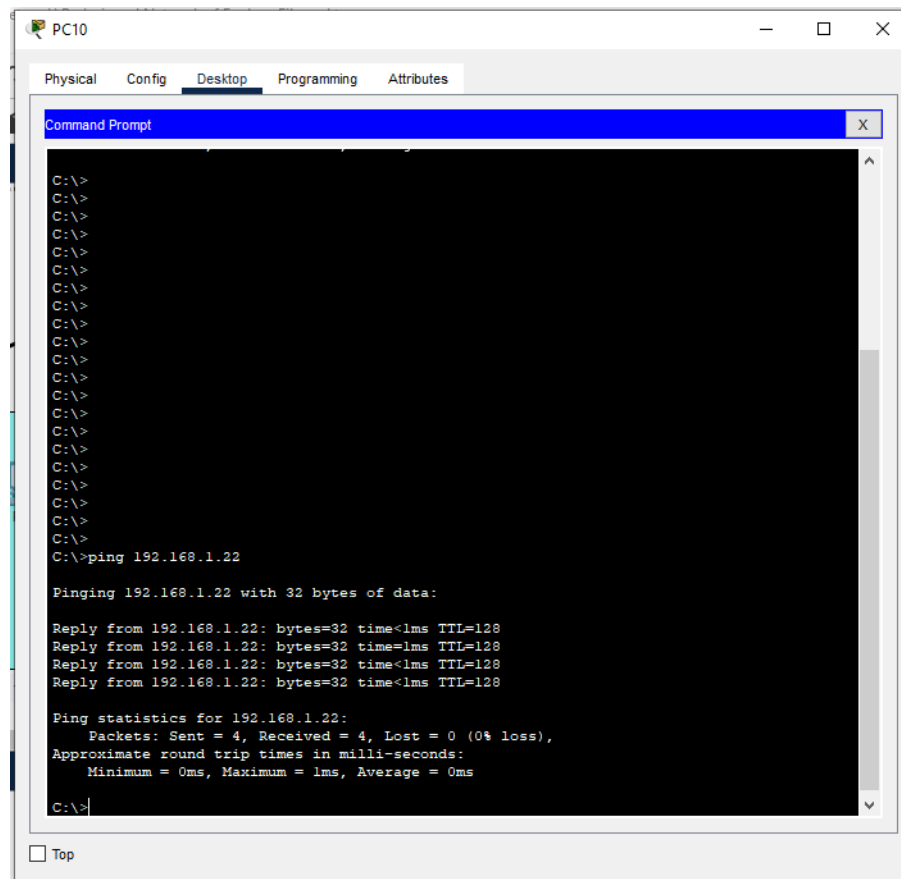


Figure 90 Test case pinging from Customer & Reception Area to General Office & Manager's

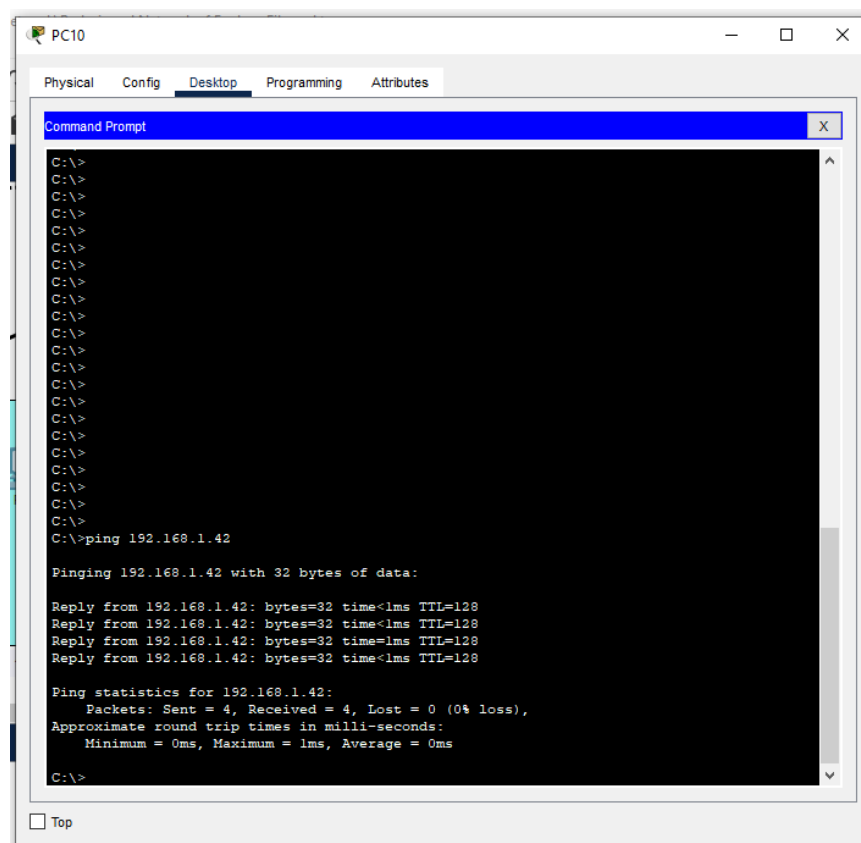


Figure 91 Test case pinging from Customer & Reception Area to Administration



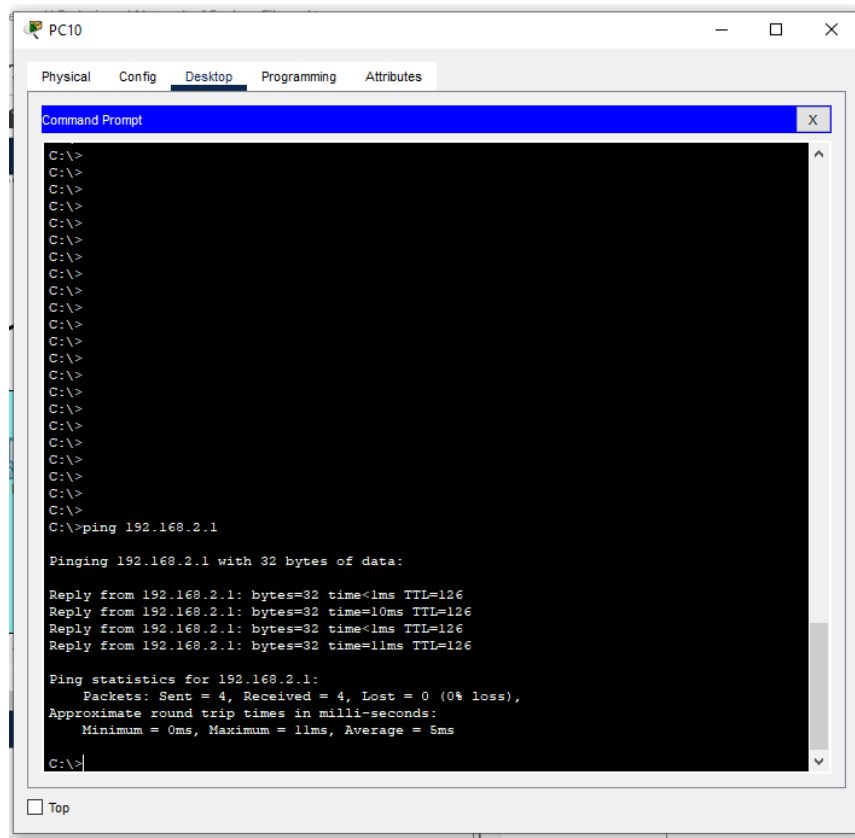


Figure 93 Test case pinging from Customer & Reception Area to Media Development & Storage

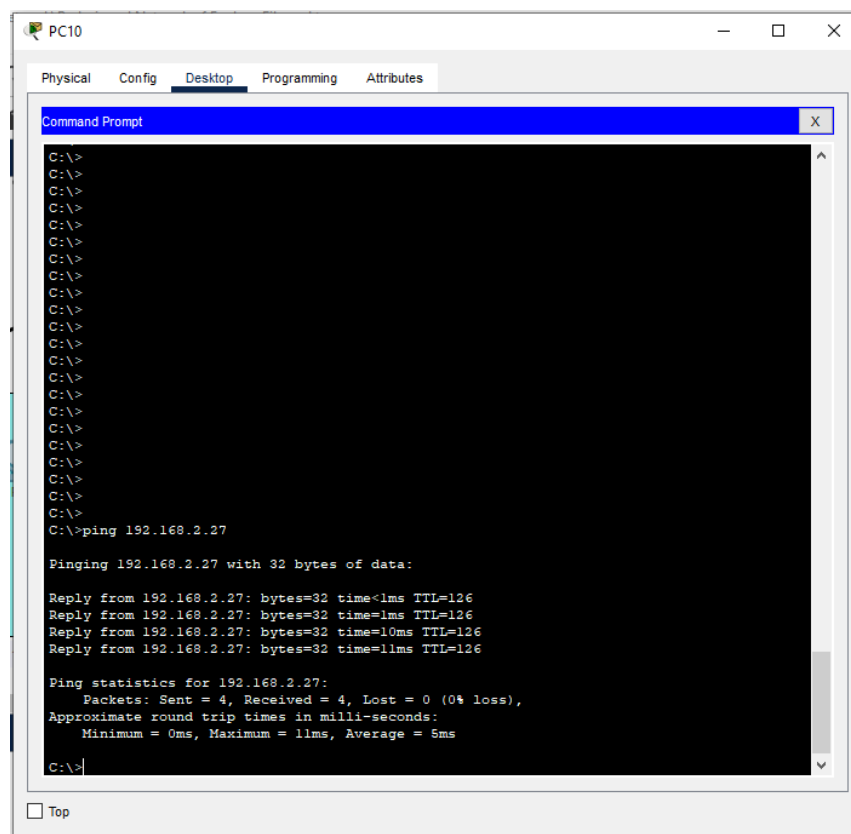
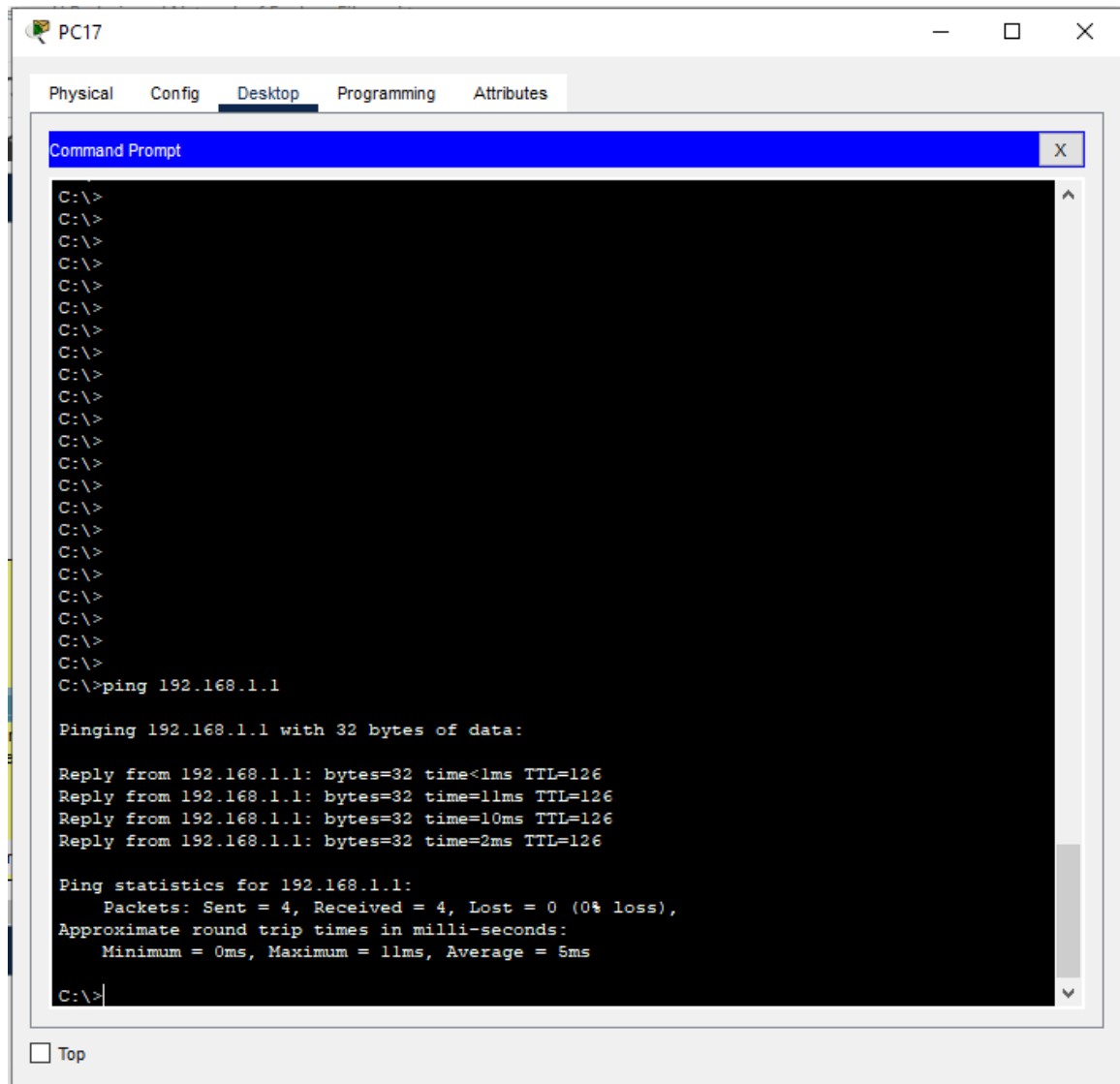


Figure 94 Test case pinging from Customer & Reception Area to Office

Media Development & Storage



```
PC17
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time=10ms TTL=126
Reply from 192.168.1.1: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms
C:\>
```

Figure 95 Test case pinging from Media Development & Storage to Sales Department

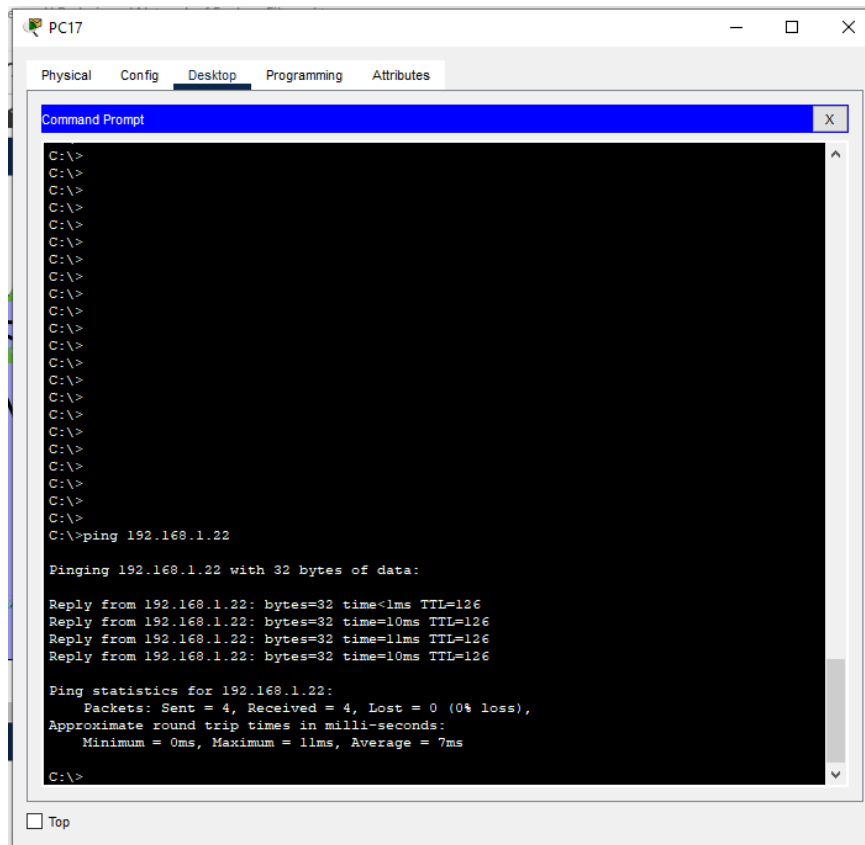


Figure 96 Test case pinging from Media Development & Storage to General Office & Manager's

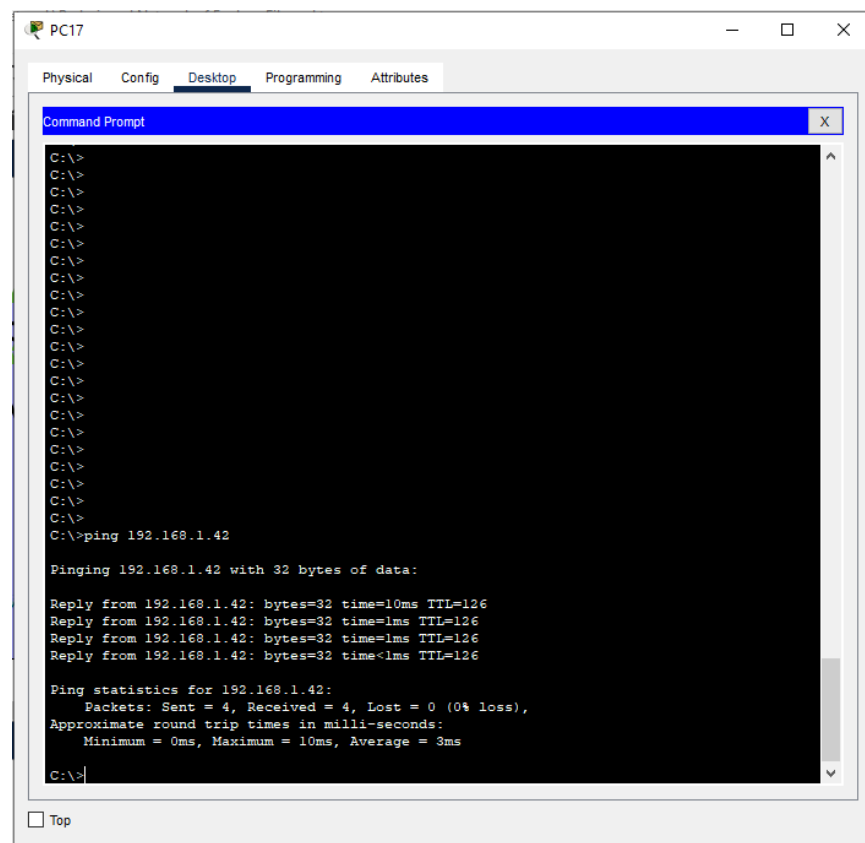


Figure 97 Test case pinging from Media Development & Storage to Administration

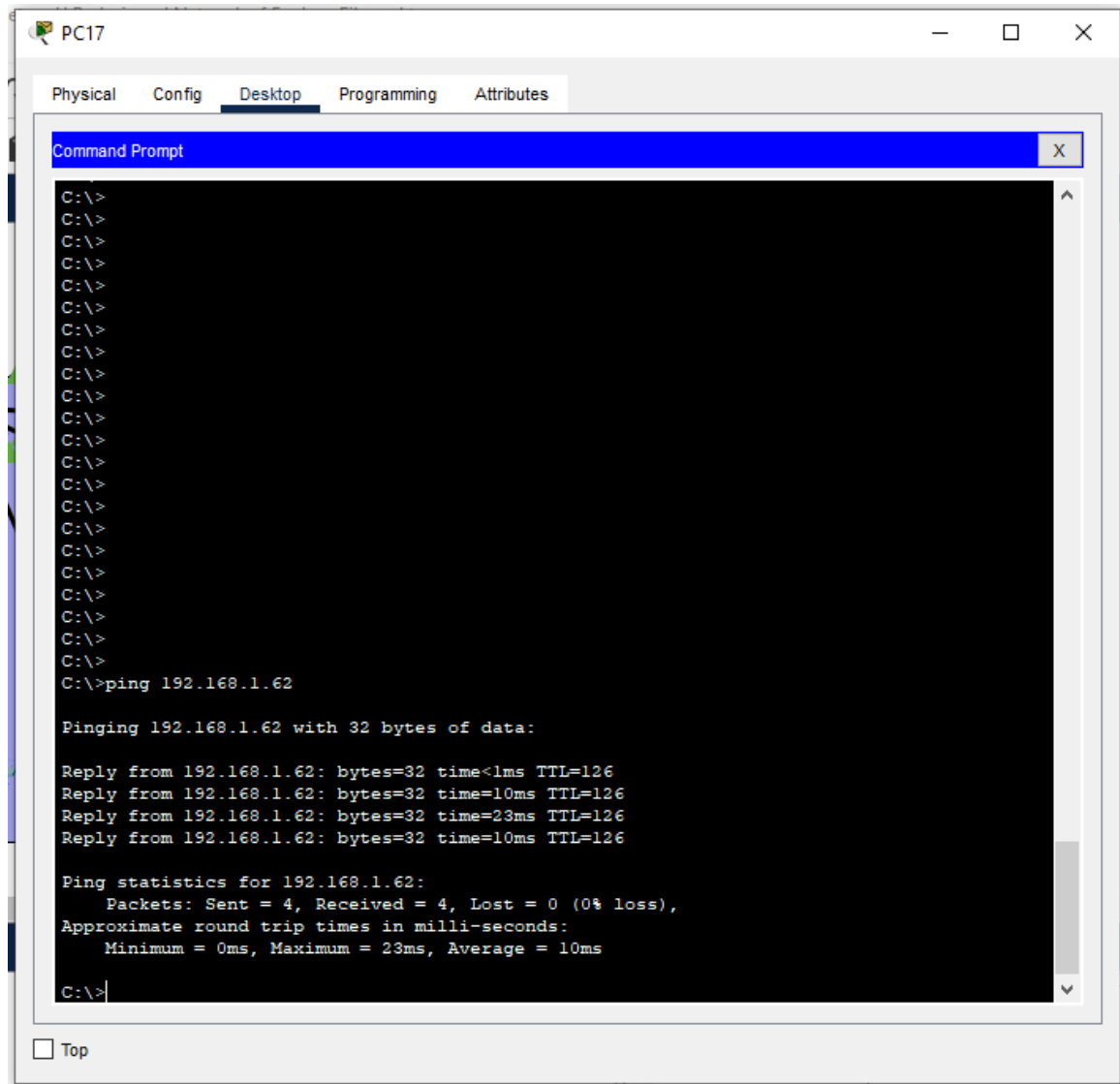


Figure 98 Test case pinging from Media Development & Storage to Accounts

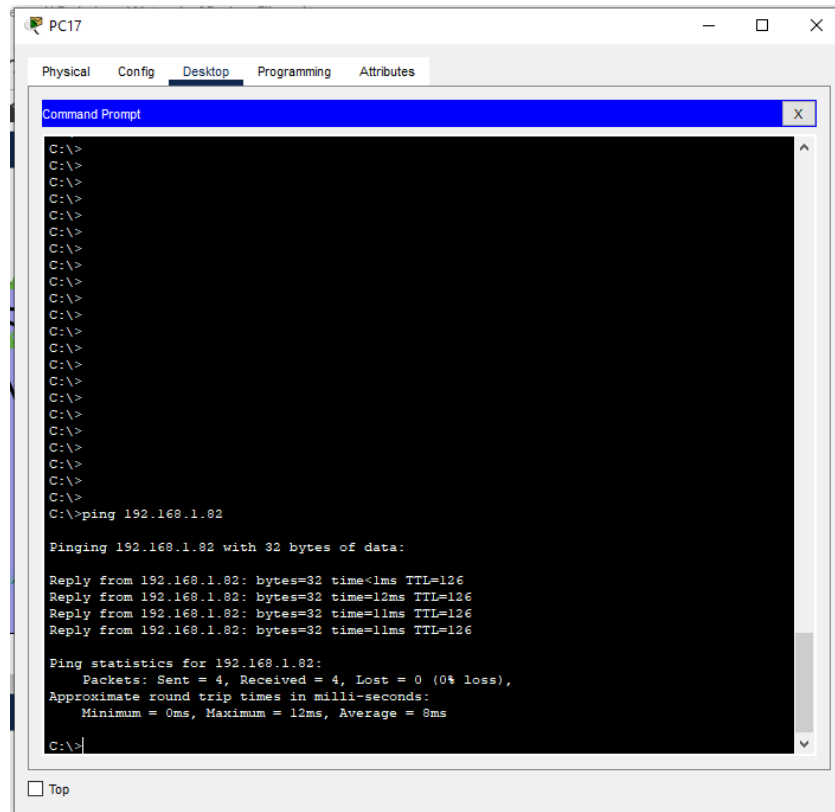


Figure 99 Test case pinging from Media Development & Storage to Customer & Reception Area

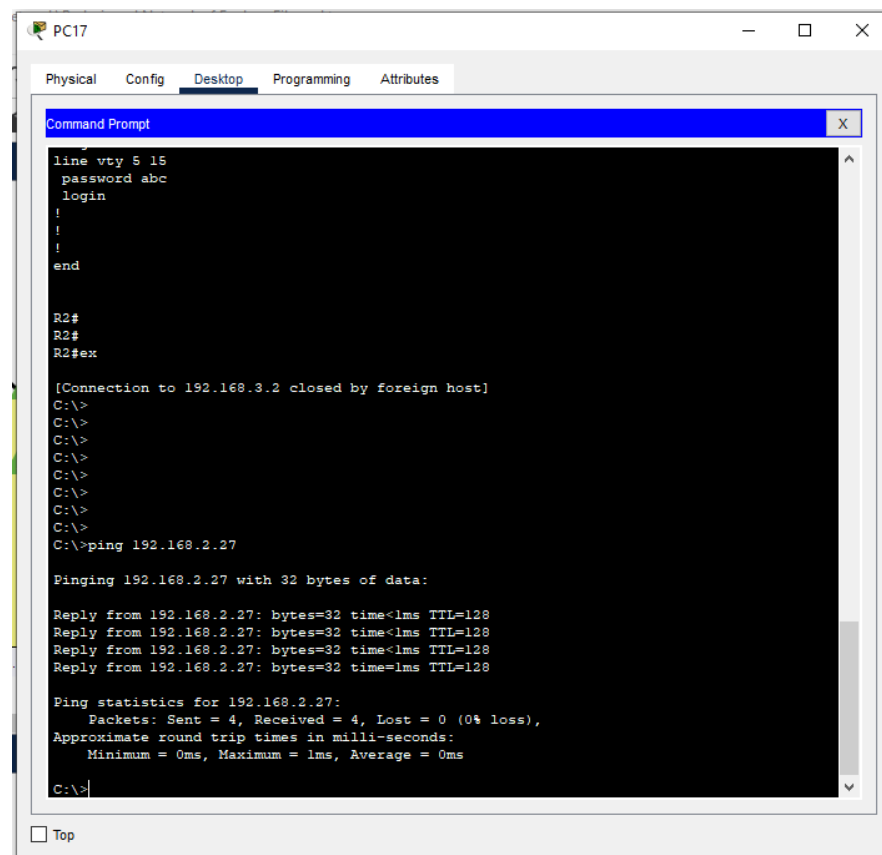
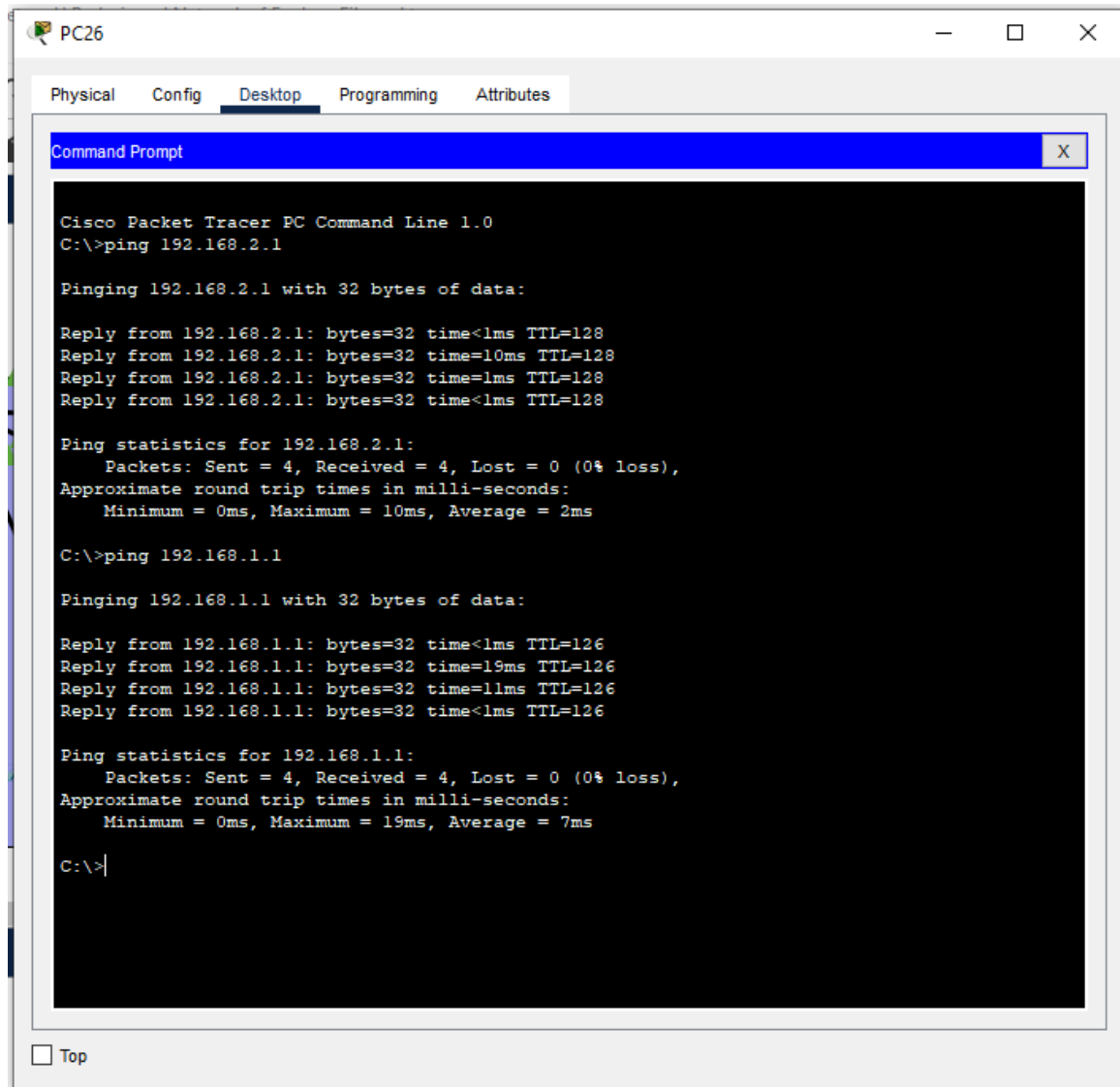


Figure 100 Test case pinging from Media Development & Storage to Office

Office



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=10ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=19ms TTL=126
Reply from 192.168.1.1: bytes=32 time=11ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 7ms

C:\>|
  
```

Figure 101 Test case pinging from Office to Sales Department

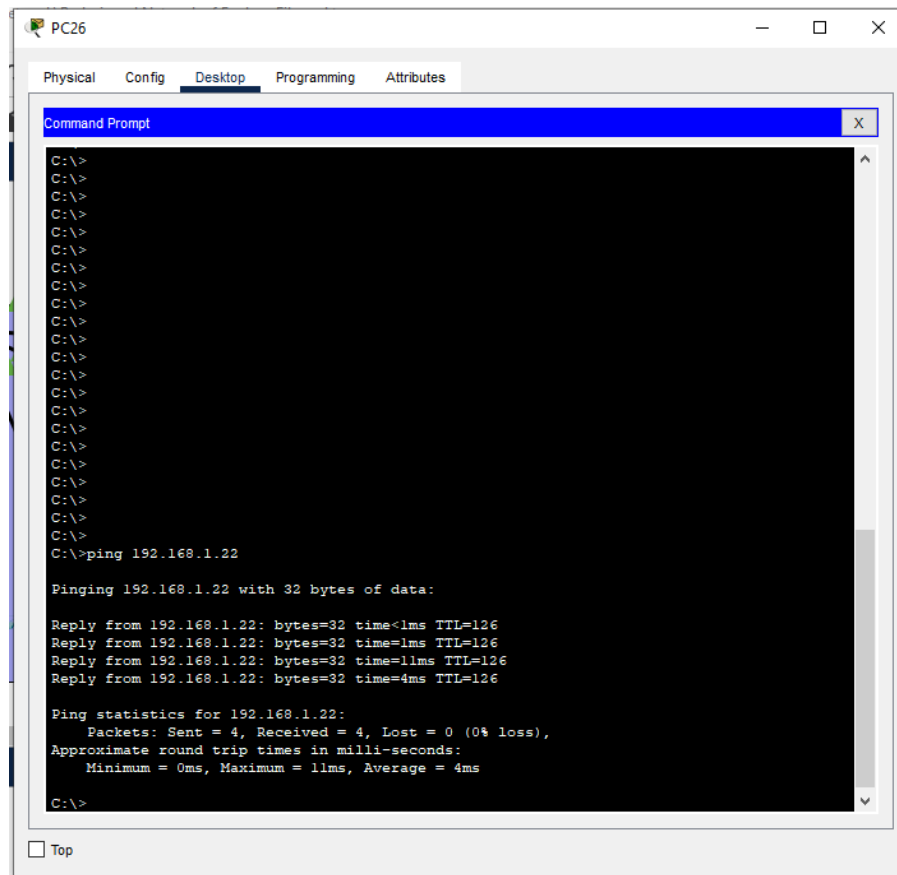
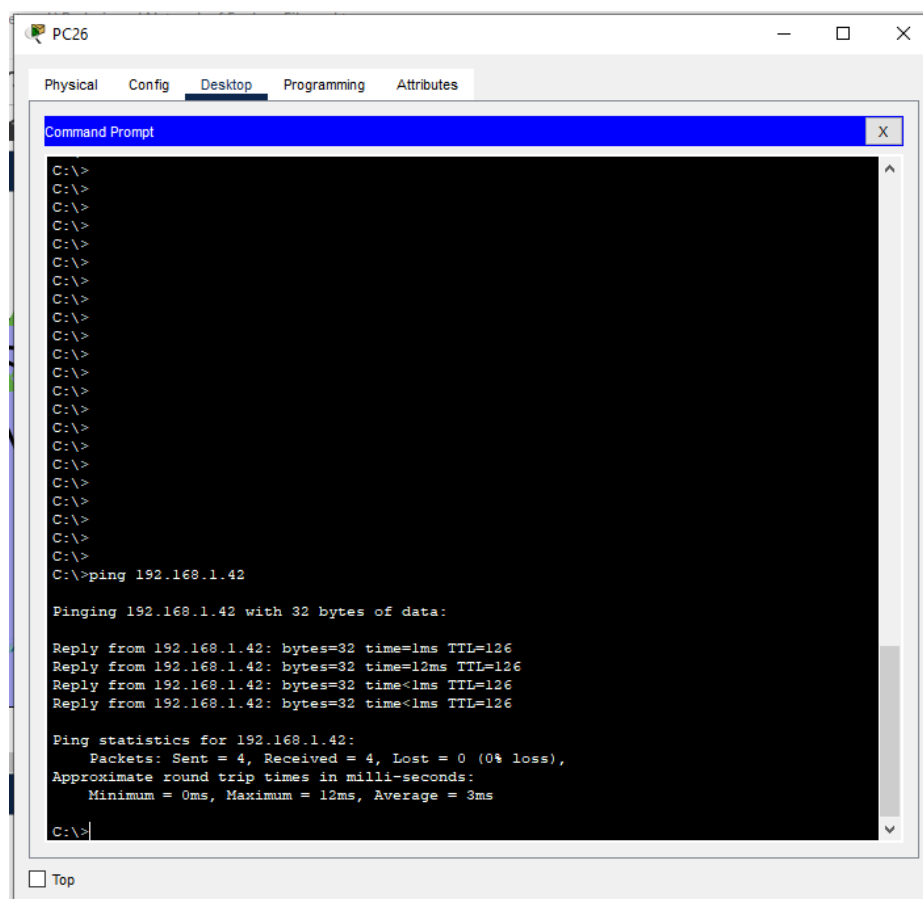
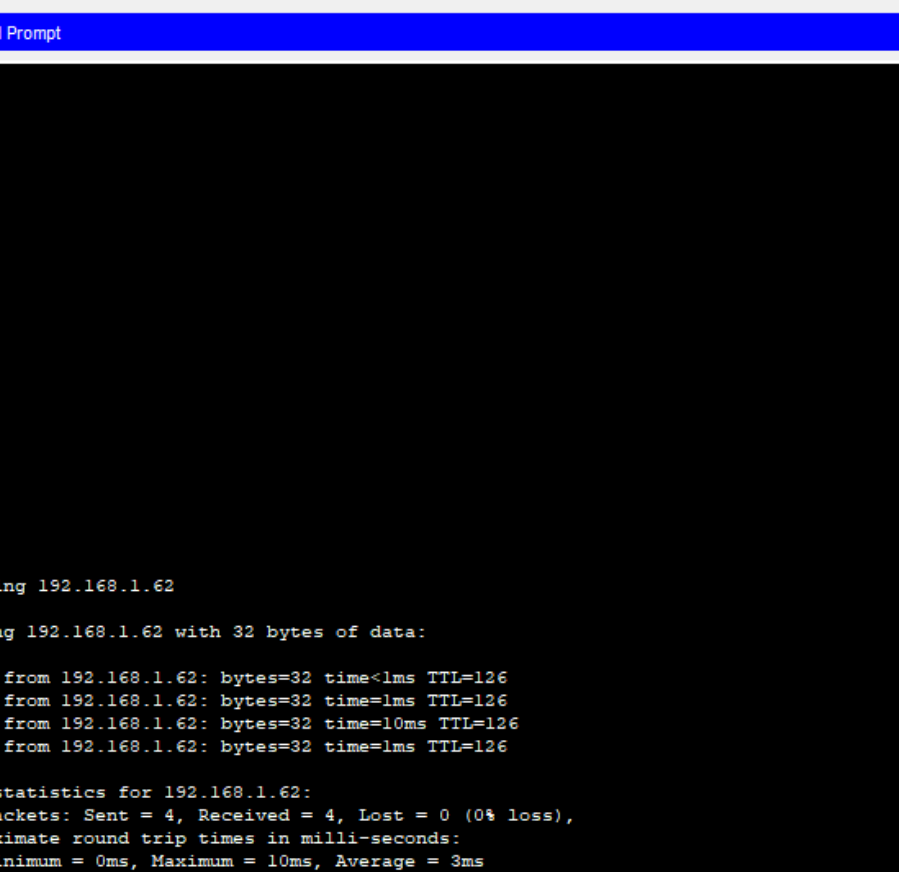


Figure 102 Test case pinging from Office to General Office & Manager's





The screenshot shows a window titled "PC2" with a standard Windows interface. Inside the window, there are four tabs: "Physical", "Config", "Desktop", and "Attributes". The "Desktop" tab is currently selected. Below the tabs, a "Command Prompt" window is open, displaying the following text:

```
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>ping 192.168.1.62  
  
Pinging 192.168.1.62 with 32 bytes of data:  
  
Reply from 192.168.1.62: bytes=32 time<1ms TTL=126  
Reply from 192.168.1.62: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.62: bytes=32 time=10ms TTL=126  
Reply from 192.168.1.62: bytes=32 time=1ms TTL=126  
  
Ping statistics for 192.168.1.62:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 10ms, Average = 3ms  
  
C:\>
```

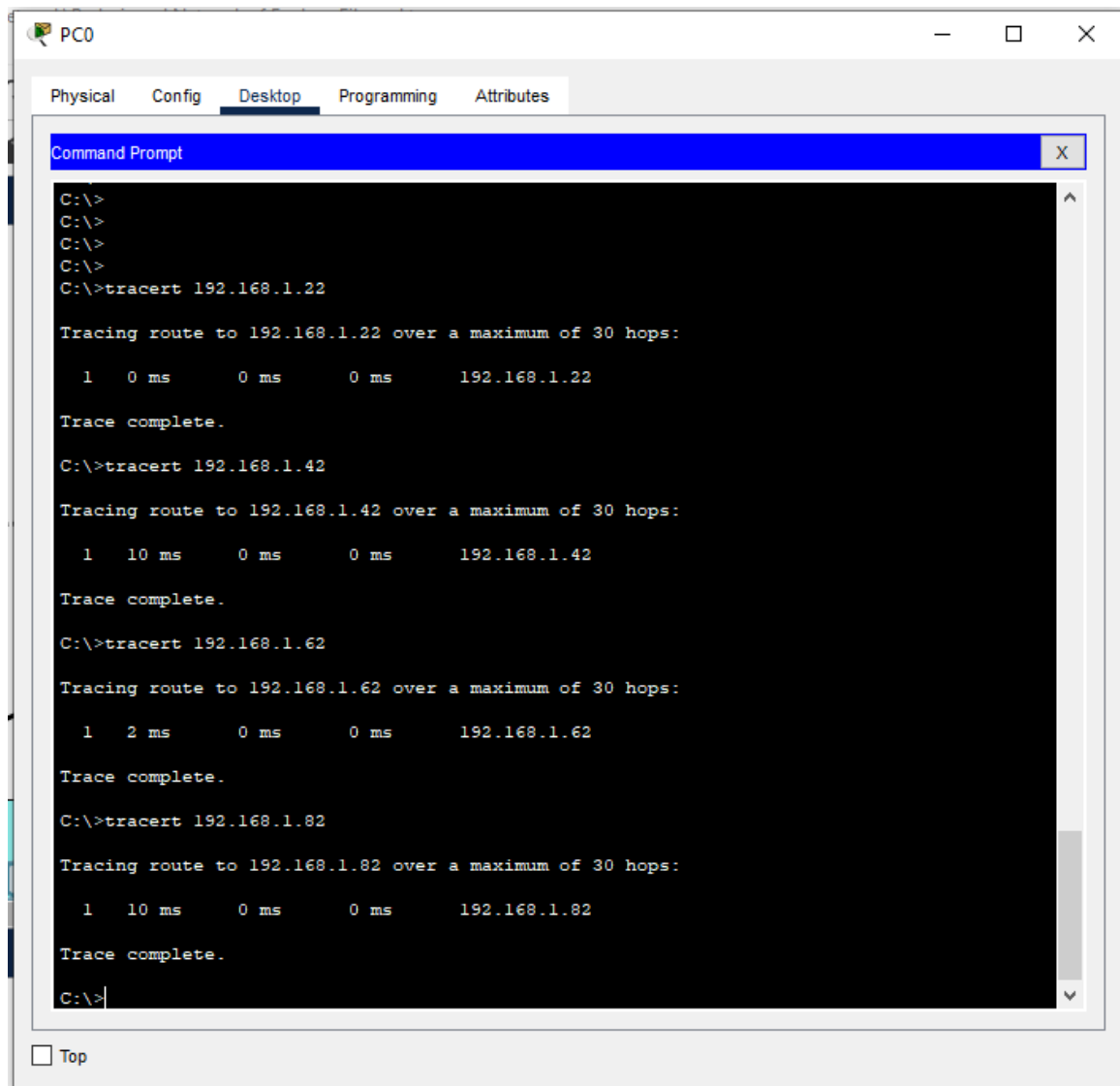
At the bottom left of the window, there is a checkbox labeled "Top".

L. SACHINTHA PRABODHI LIYANAGE – NETWORKING – ASSIGNMENT NO 01



3.2.2 Traceroute

The traceroute command verifies network operation by sending packets to determine the path from source to destination using the Time to Live (TTL) functionality in the IP header. The TTL field allows a source to set the number of hops a packet can travel before being dropped. If TTL expires, a device returns an unreachable message, and the traceroute utility continues sending packets until the source address matches the destination device.



```

C:\>
C:\>
C:\>
C:\>
C:\>tracert 192.168.1.22

Tracing route to 192.168.1.22 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.22

Trace complete.

C:\>tracert 192.168.1.42

Tracing route to 192.168.1.42 over a maximum of 30 hops:

  1  10 ms   0 ms    0 ms    192.168.1.42

Trace complete.

C:\>tracert 192.168.1.62

Tracing route to 192.168.1.62 over a maximum of 30 hops:

  1   2 ms   0 ms    0 ms    192.168.1.62

Trace complete.

C:\>tracert 192.168.1.82

Tracing route to 192.168.1.82 over a maximum of 30 hops:

  1  10 ms   0 ms    0 ms    192.168.1.82

Trace complete.

C:\>
  
```

Figure 107 Displays traceroute (Building A)

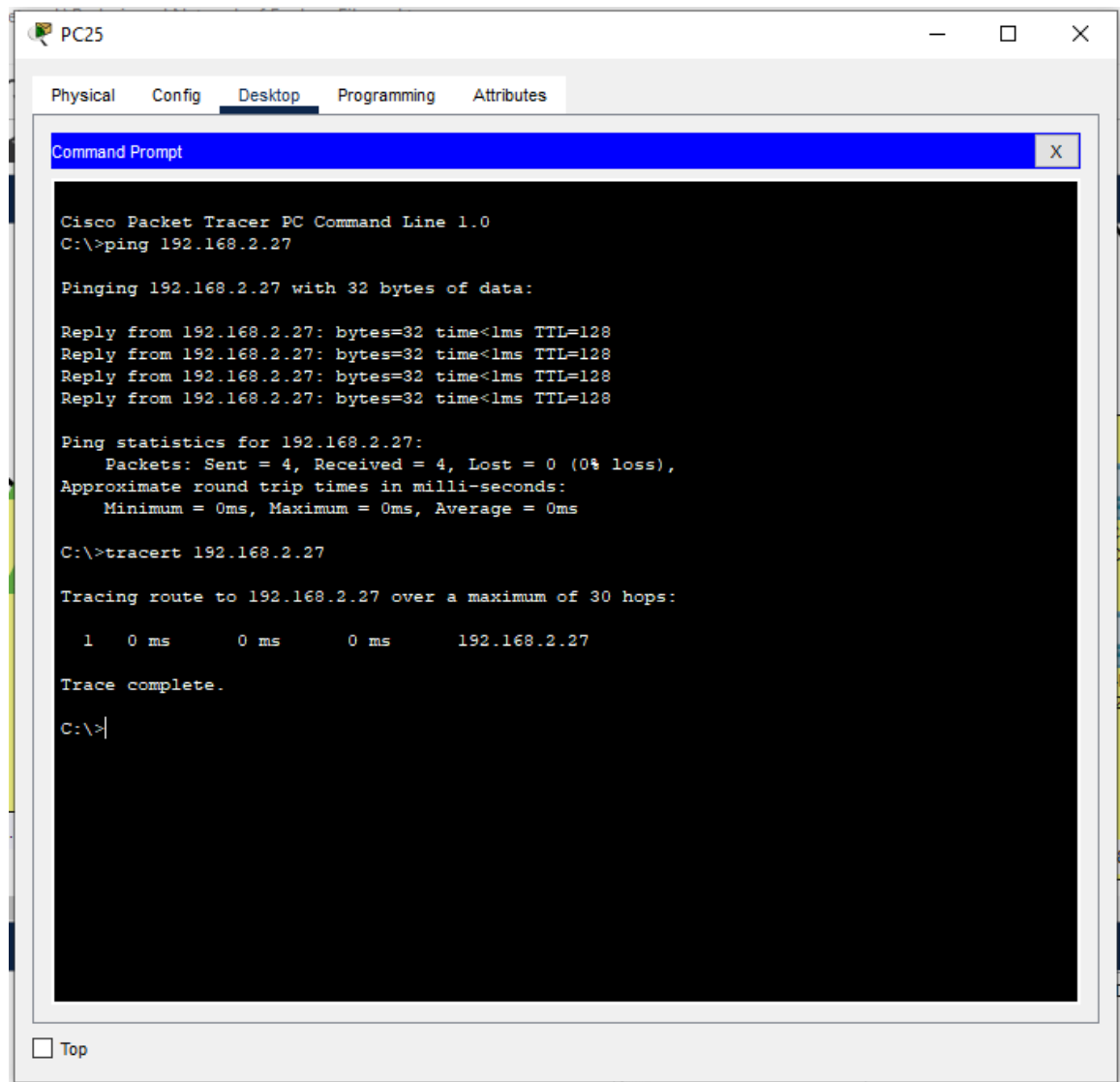


Figure 108 Displays traceroute (Building B)

3.2.3 Telnet

Telnet is a bidirectional, intelligent content-arranged correspondence protocol using virtual terminal associations, storing client information in an 8-bit byte format.

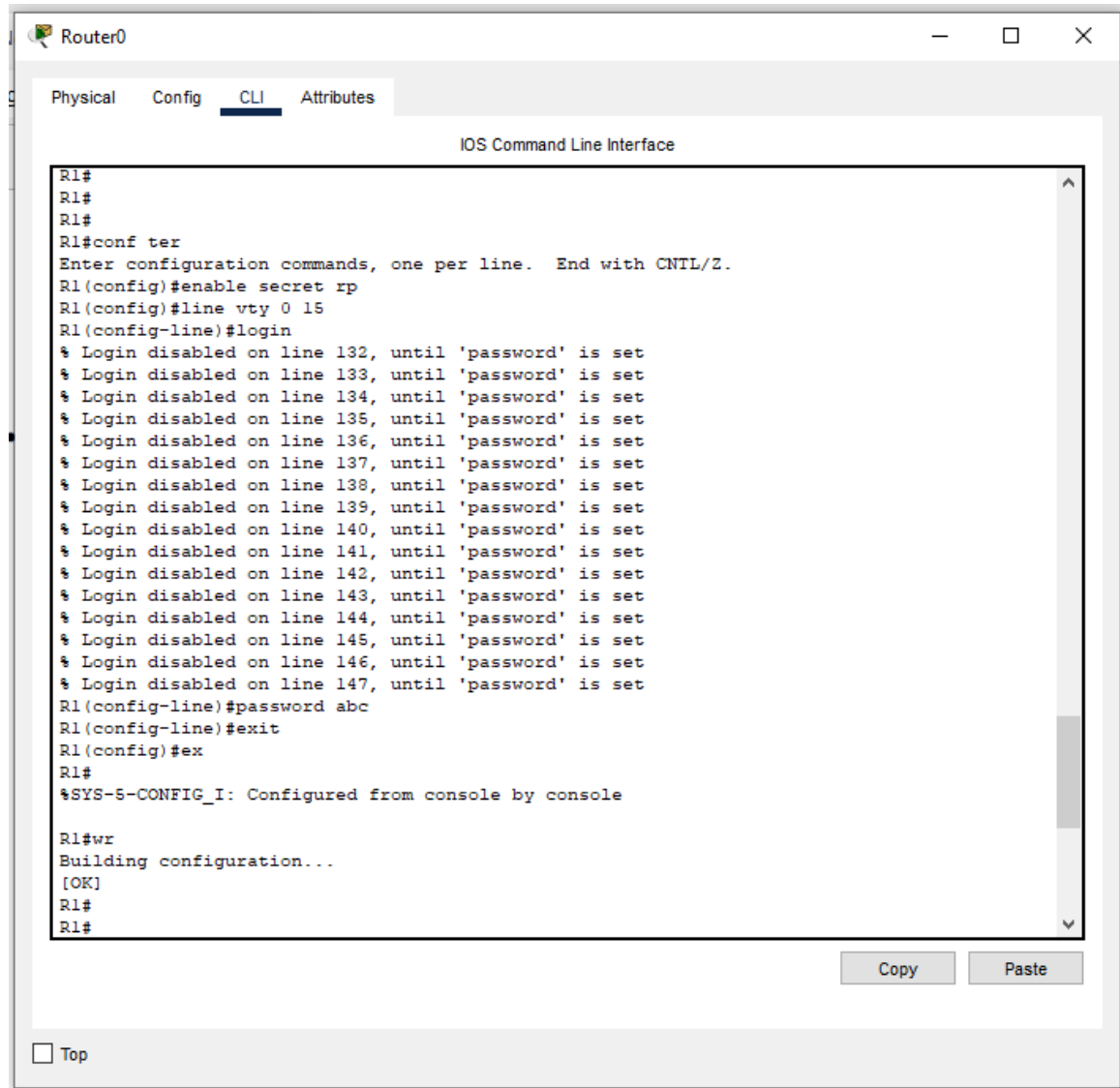


Figure 109 Telnet (Building A)

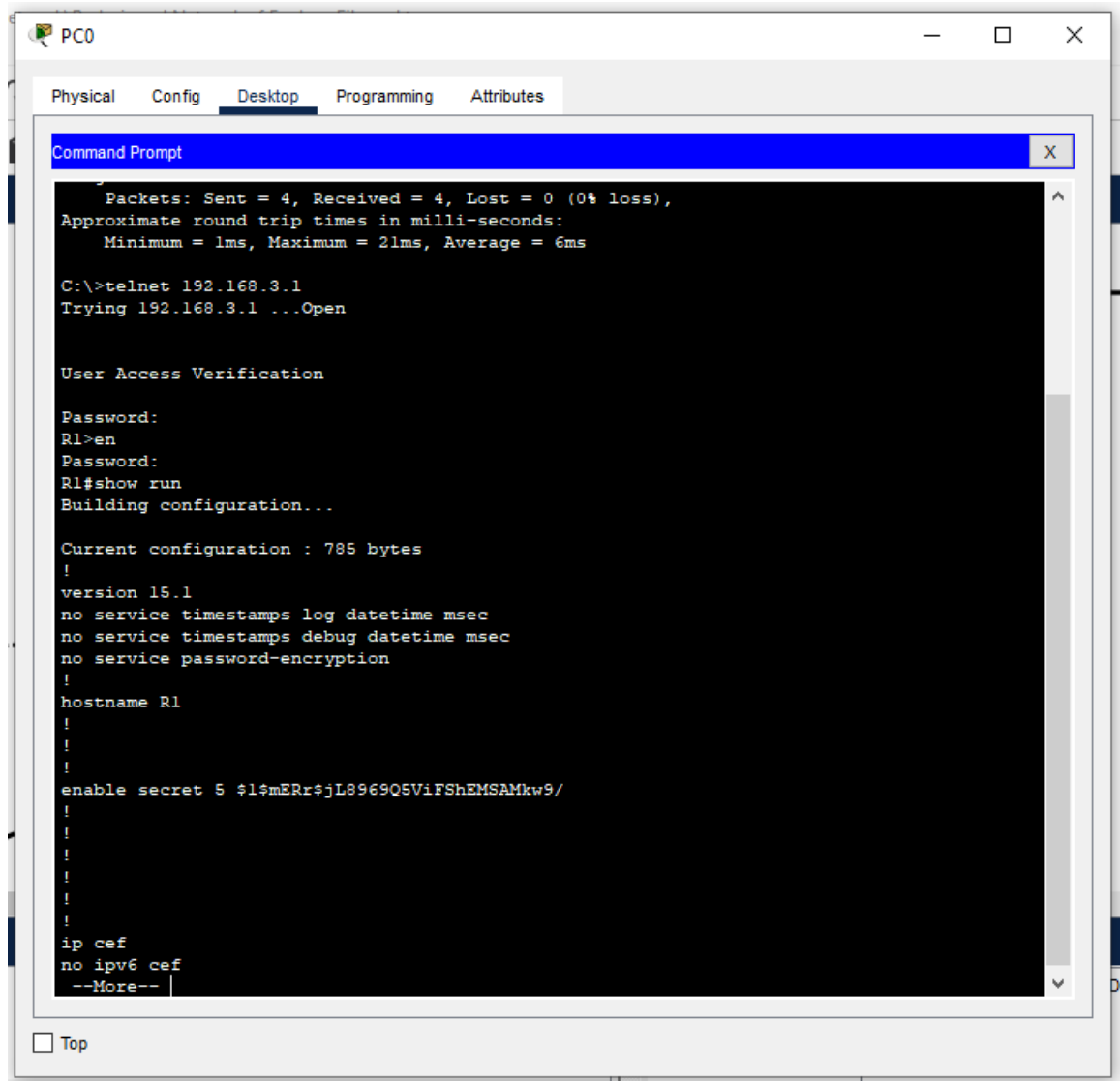
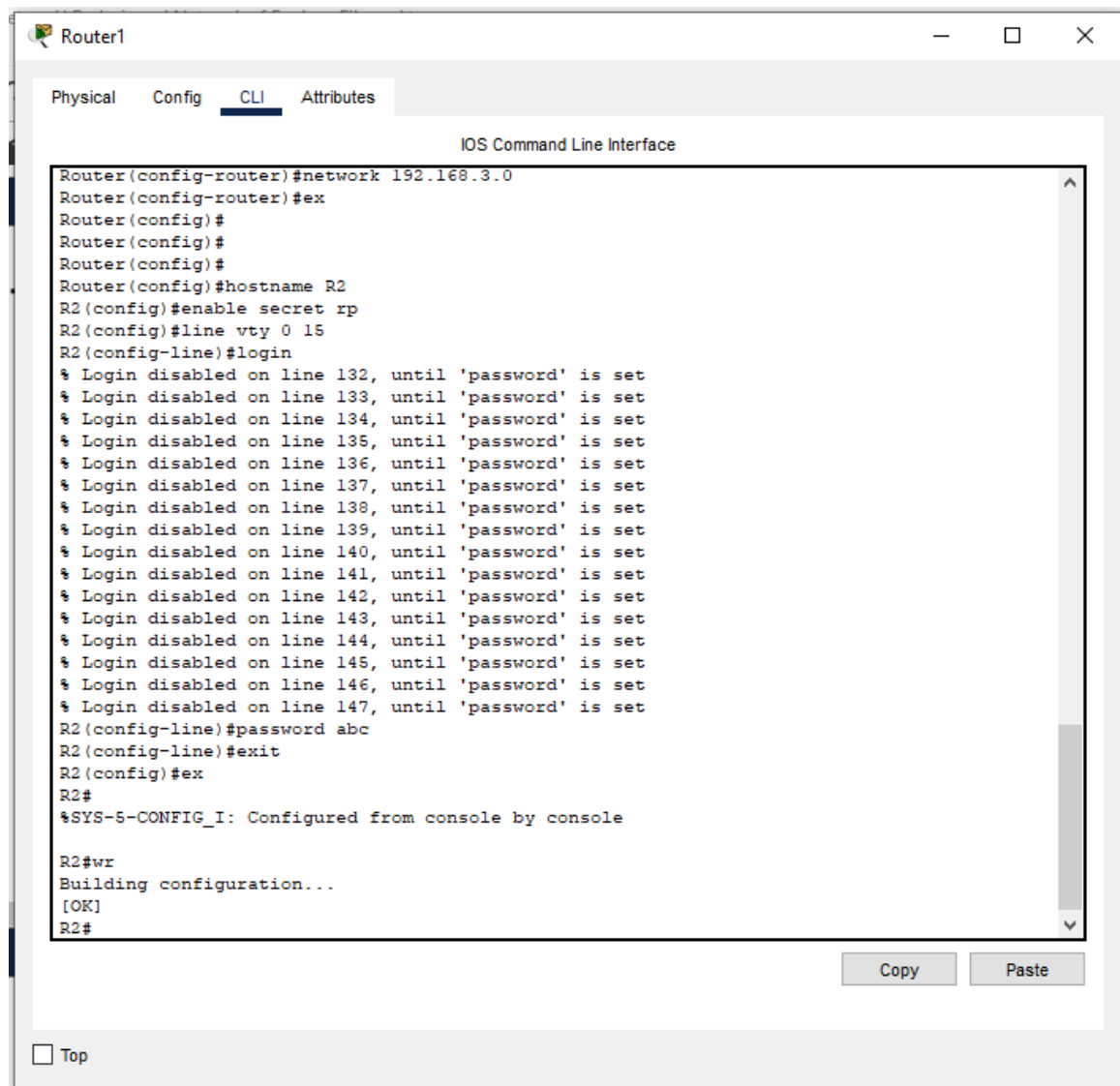


Figure 110 Result of telnet (Building A)



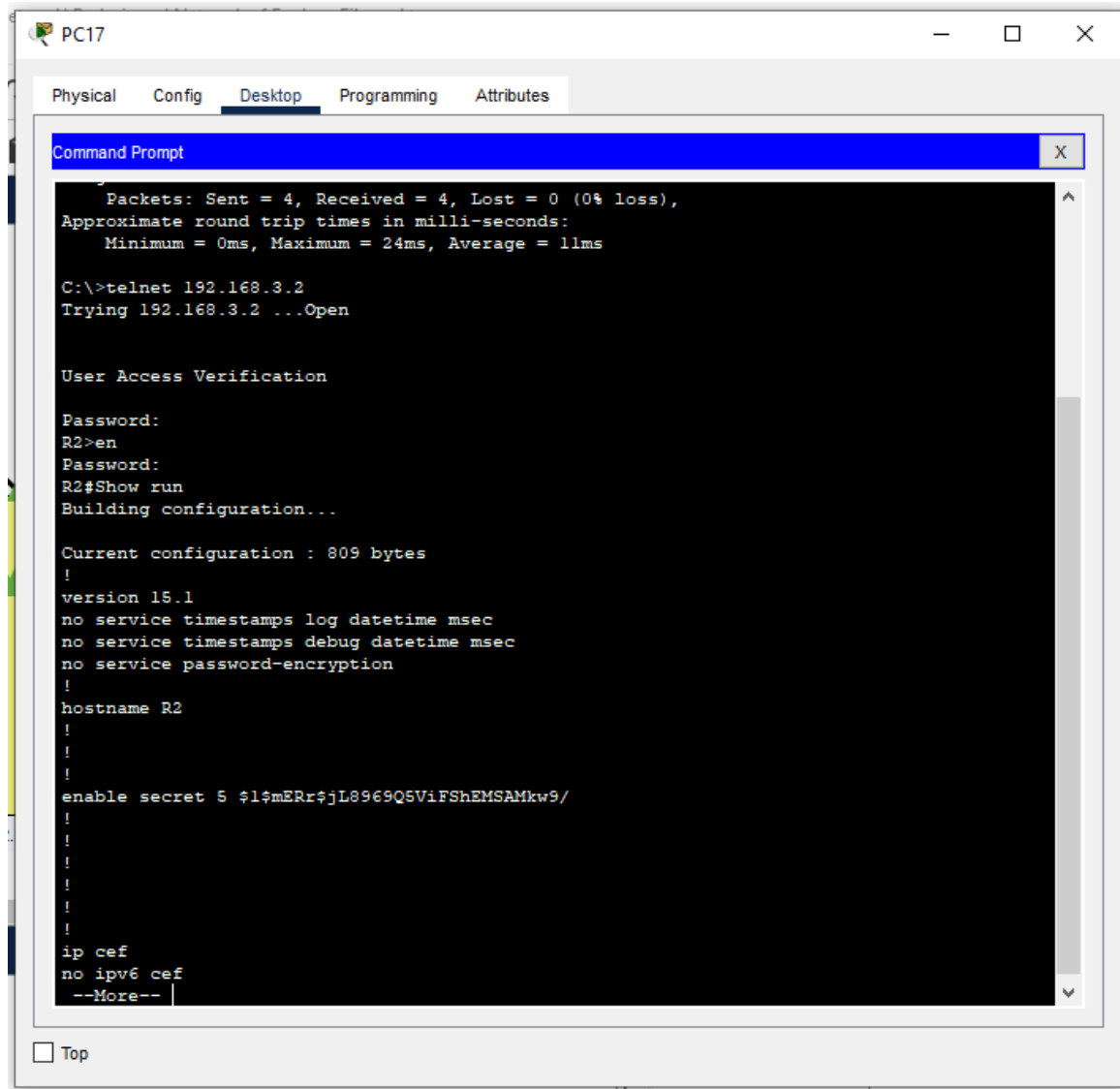
```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-router)#network 192.168.3.0
Router(config-router)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#hostname R2
R2(config)#enable secret rp
R2(config)#line vty 0 15
R2(config-line)#login
% Login disabled on line 132, until 'password' is set
% Login disabled on line 133, until 'password' is set
% Login disabled on line 134, until 'password' is set
% Login disabled on line 135, until 'password' is set
% Login disabled on line 136, until 'password' is set
% Login disabled on line 137, until 'password' is set
% Login disabled on line 138, until 'password' is set
% Login disabled on line 139, until 'password' is set
% Login disabled on line 140, until 'password' is set
% Login disabled on line 141, until 'password' is set
% Login disabled on line 142, until 'password' is set
% Login disabled on line 143, until 'password' is set
% Login disabled on line 144, until 'password' is set
% Login disabled on line 145, until 'password' is set
% Login disabled on line 146, until 'password' is set
% Login disabled on line 147, until 'password' is set
R2(config-line)#password abc
R2(config-line)#exit
R2(config)#ex
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr
Building configuration...
[OK]
R2#
Copy Paste
Top

```

Figure 111 Telnet (Building B)



```

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 24ms, Average = 11ms

C:\>telnet 192.168.3.2
Trying 192.168.3.2 ...Open

User Access Verification

Password:
R2>en
Password:
R2#Show run
Building configuration...

Current configuration : 809 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$jL8969Q5ViFShEMSAMkw9/
!
!
!
!
!
!
ip cef
no ipv6 cef
--More--
  
```

Figure 112 Result of telnet (Building B)

3.2.4 SSH

Secure shell (SSH) is a cryptographic protocol for secure communication, remote login, and order execution on unsecured systems like the Internet.

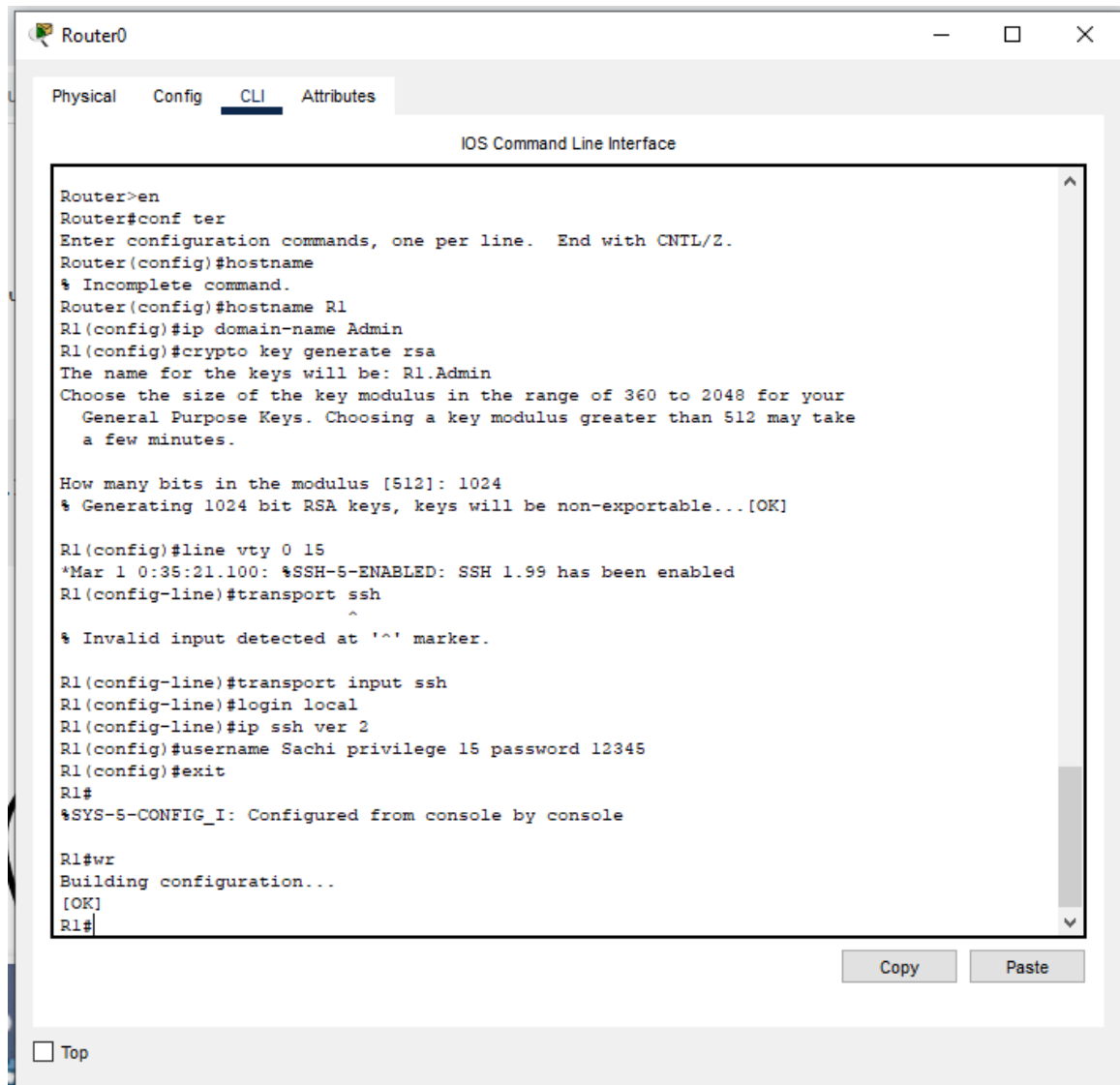


Figure 113 SSH (Building A)

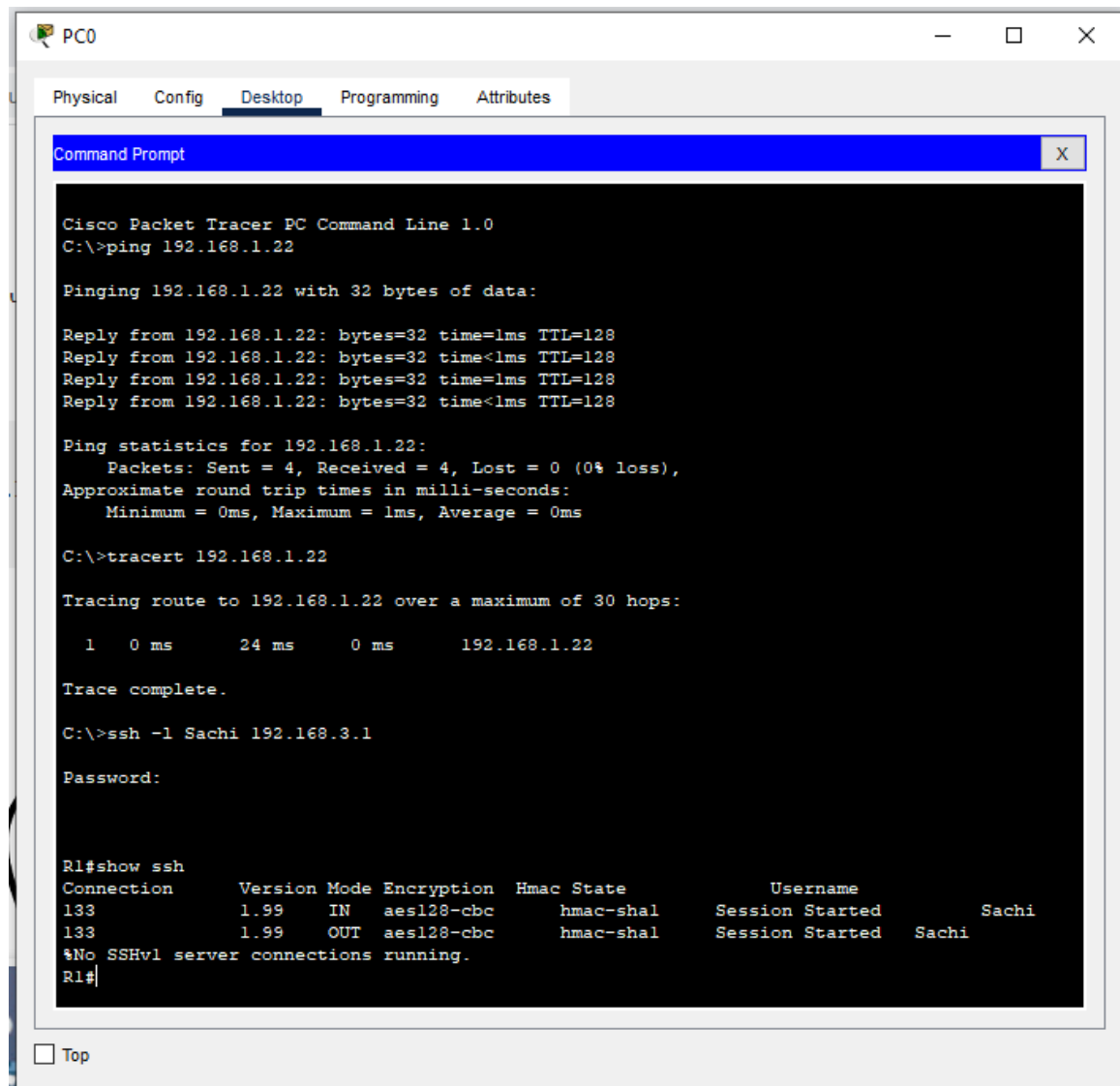


Figure 114 Result of SSH (Building A)

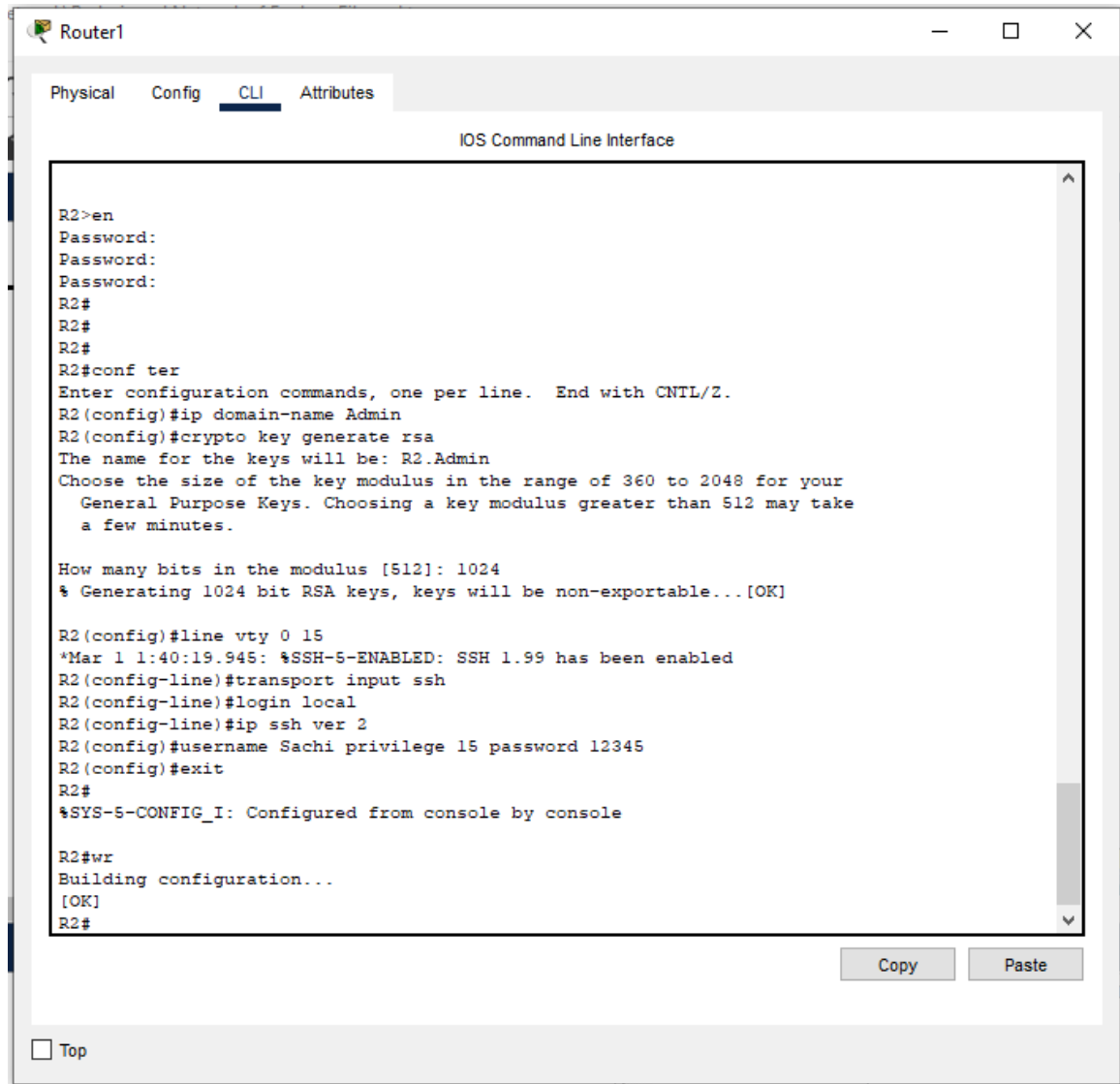
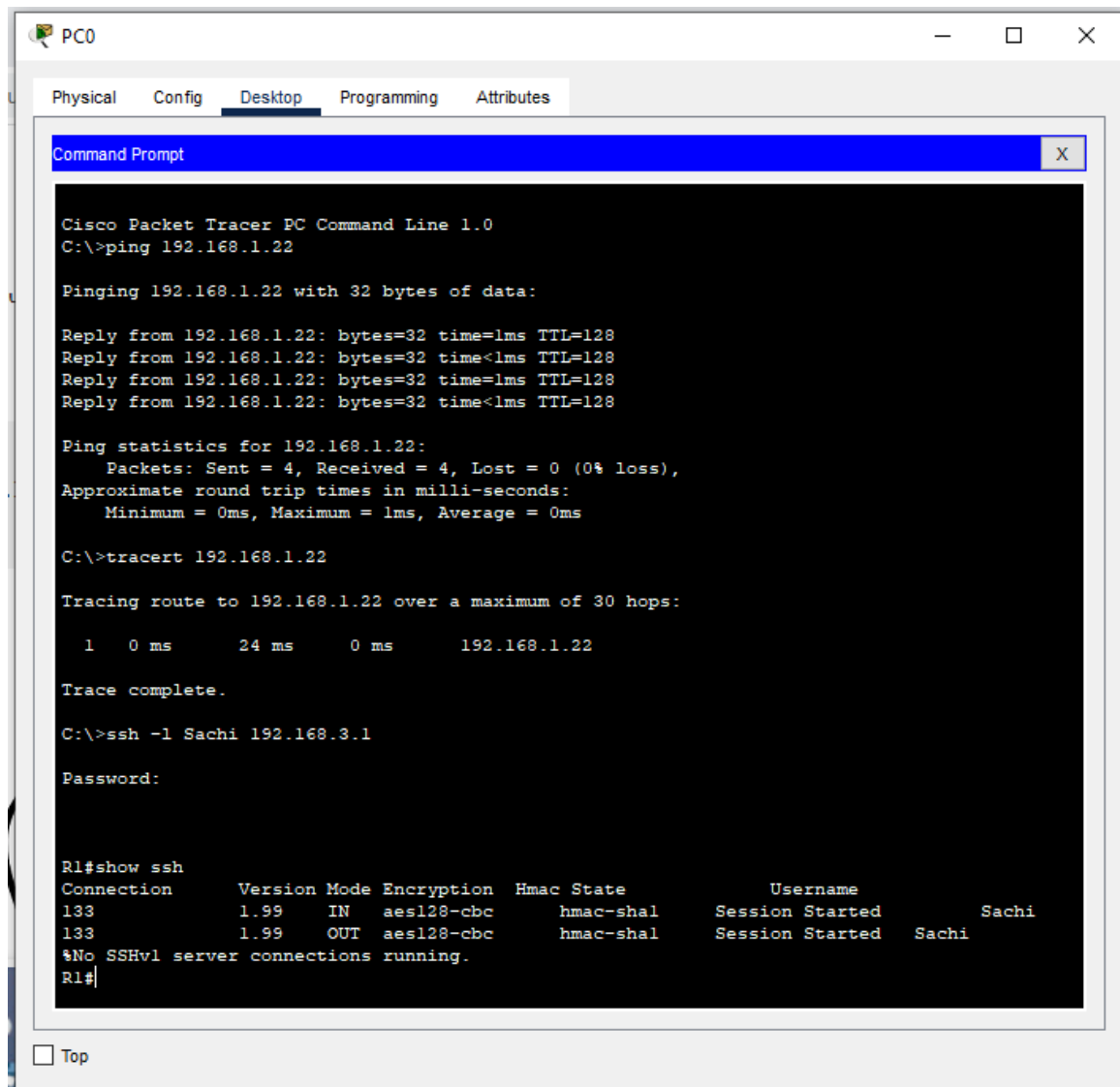


Figure 115 SSH (Building B)



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.22

Pinging 192.168.1.22 with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time=1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128
Reply from 192.168.1.22: bytes=32 time=1ms TTL=128
Reply from 192.168.1.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 192.168.1.22

Tracing route to 192.168.1.22 over a maximum of 30 hops:

  0  0 ms    24 ms    0 ms    192.168.1.22

Trace complete.

C:\>ssh -l Sachi 192.168.3.1

Password:

R1#show ssh
Connection      Version Mode Encryption  Hmac State      Username
133             1.99   IN   aes128-cbc    hmac-shal  Session Started Sachi
133             1.99   OUT  aes128-cbc    hmac-shal  Session Started Sachi
%No SSHv1 server connections running.
R1#
  
```

Figure 116 Result of SSH (Building B)

3.2.5 Ipconfig

The ipconfig command is a Windows utility that displays IP configuration settings for network interfaces, including IP address, subnet mask, default gateway, and DNS servers. To use it, open the Command Prompt, type ipconfig, and press Enter. It displays information for all active network interfaces, including Ethernet, Wi-Fi, and virtual adapters.

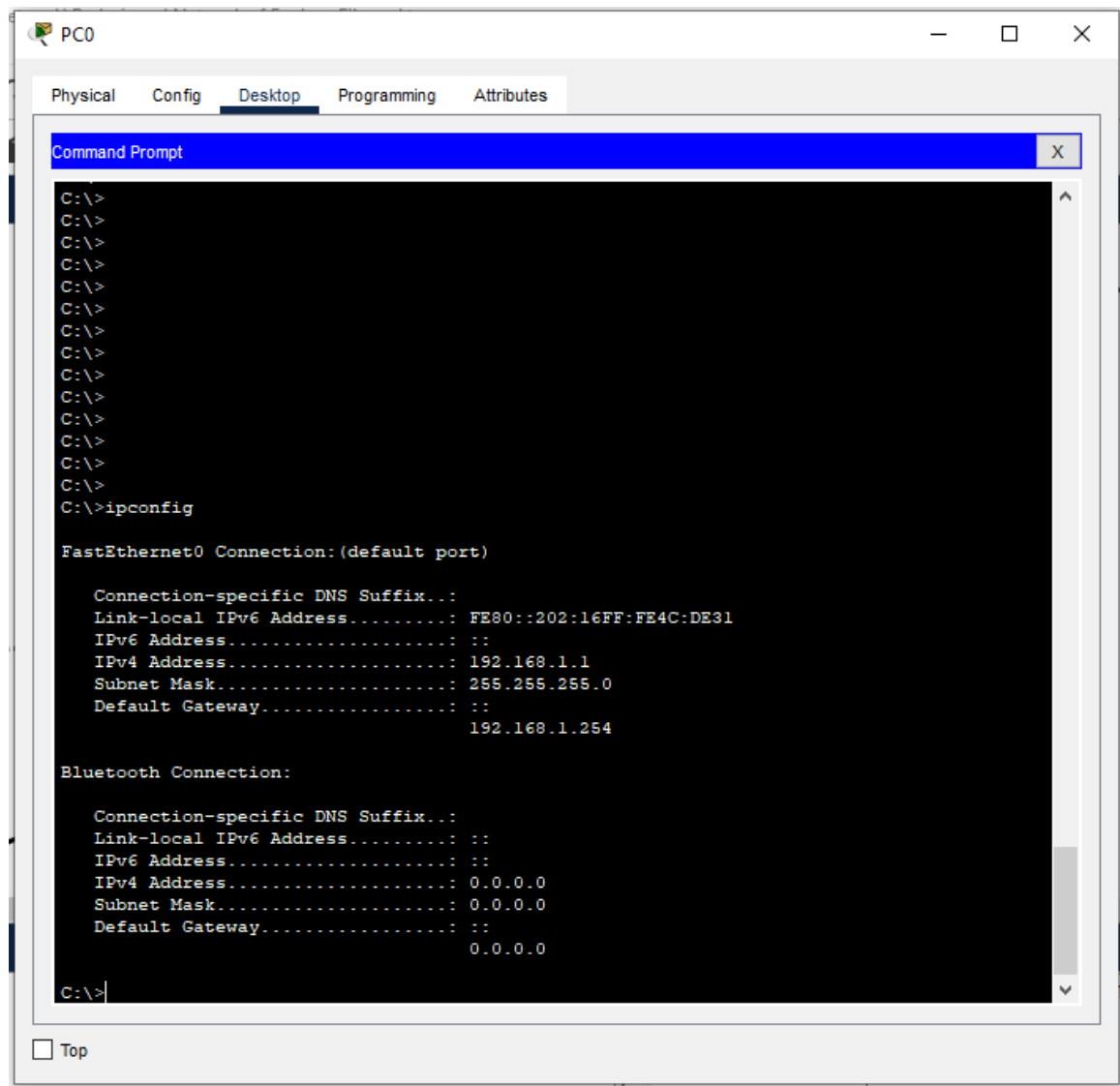


Figure 117 Displays ipconfig for Sales Department PC

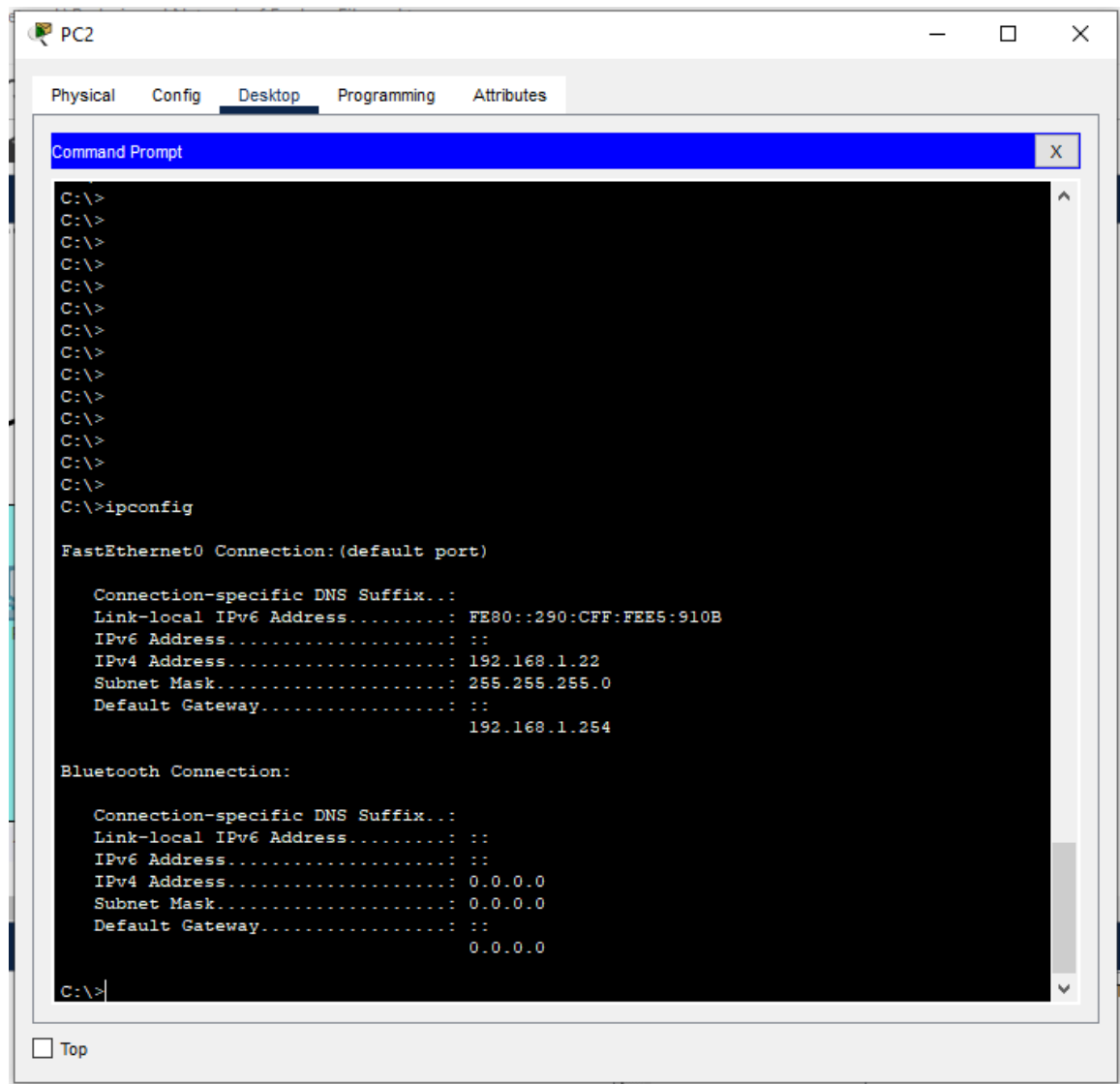


Figure 118 Displays ipconfig for General Office & Manager's Department PC

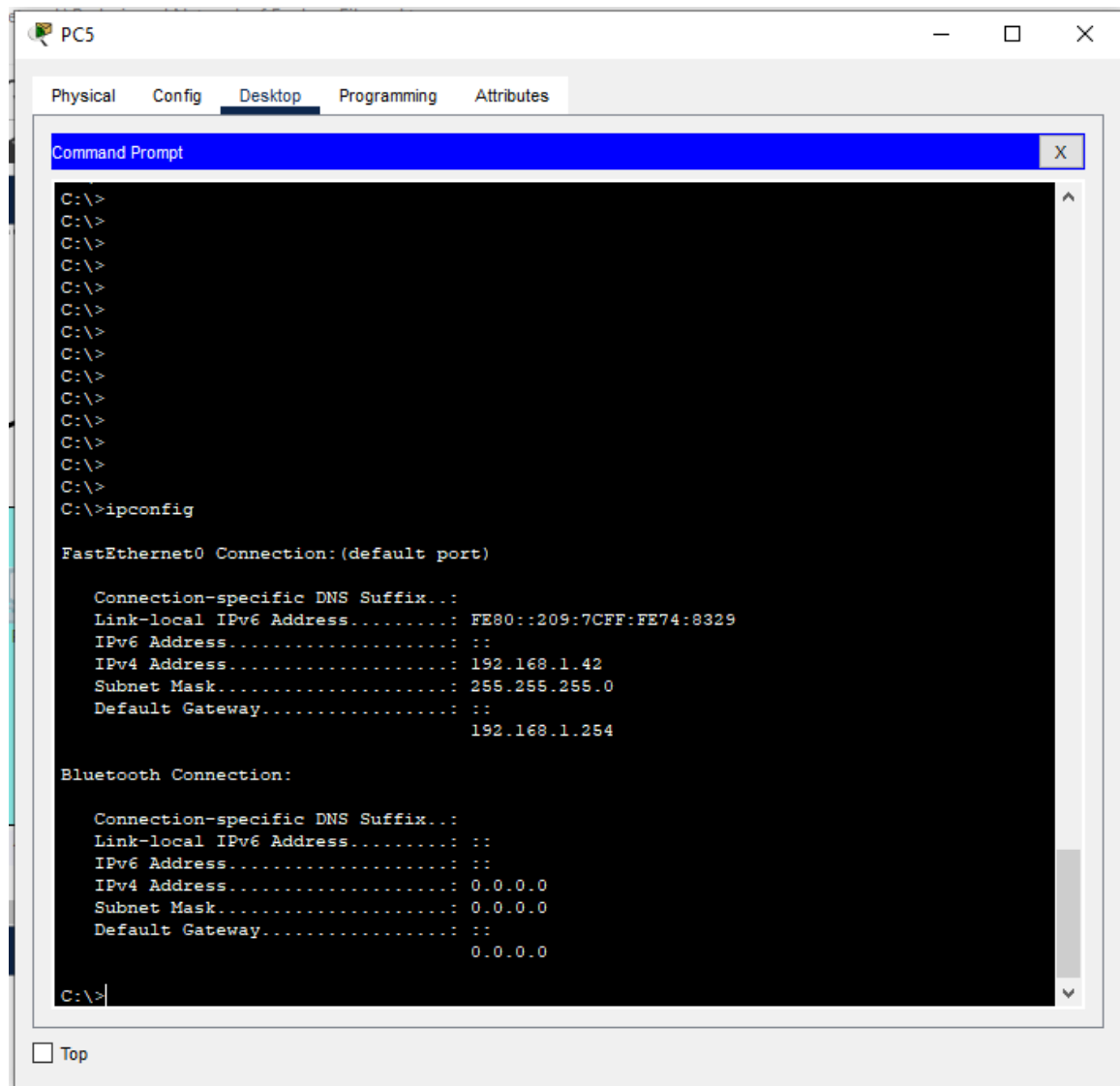


Figure 119 Displays ipconfig for Administration Department PC

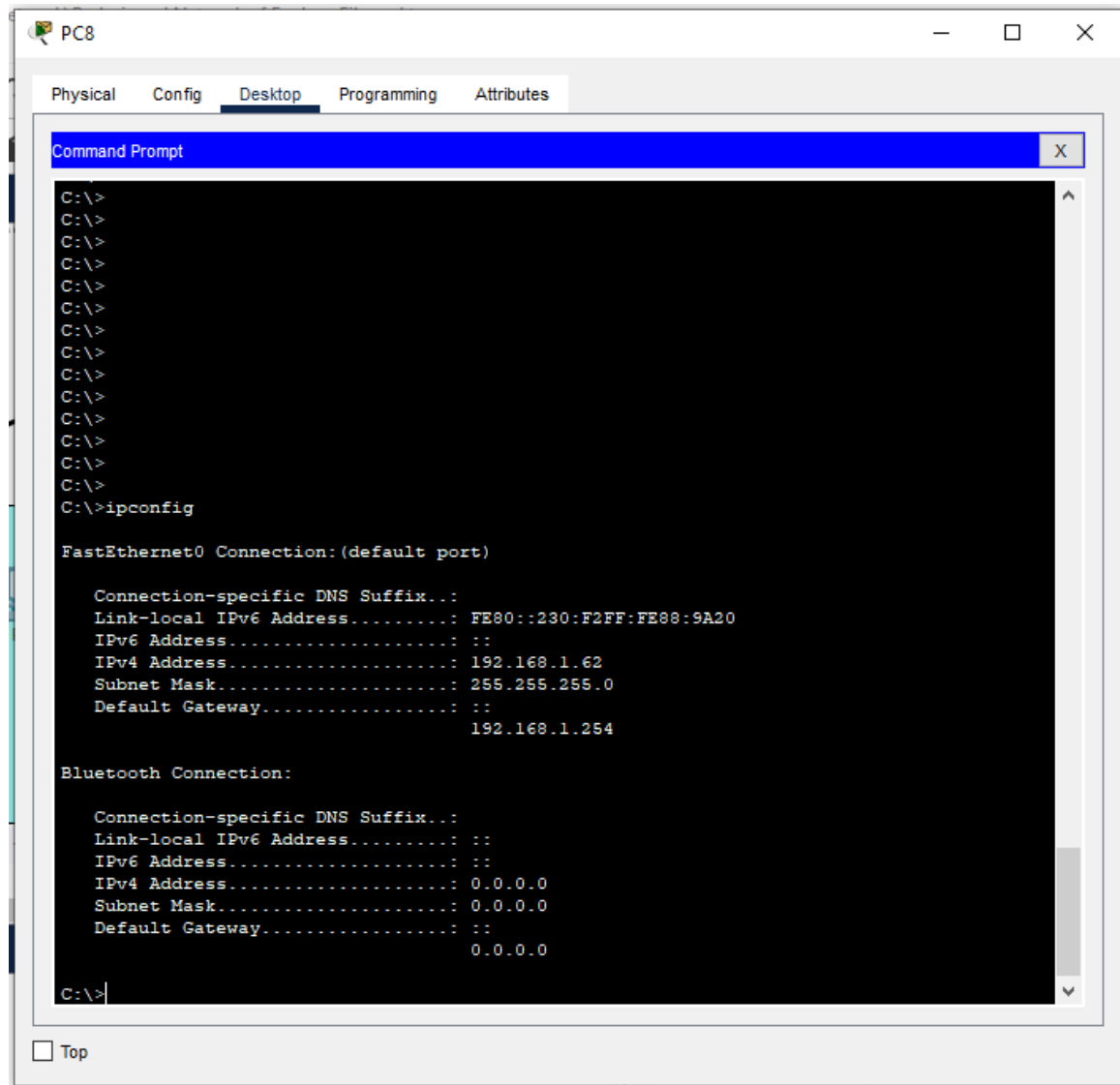


Figure 120 Displays ipconfig for Accounts Department PC

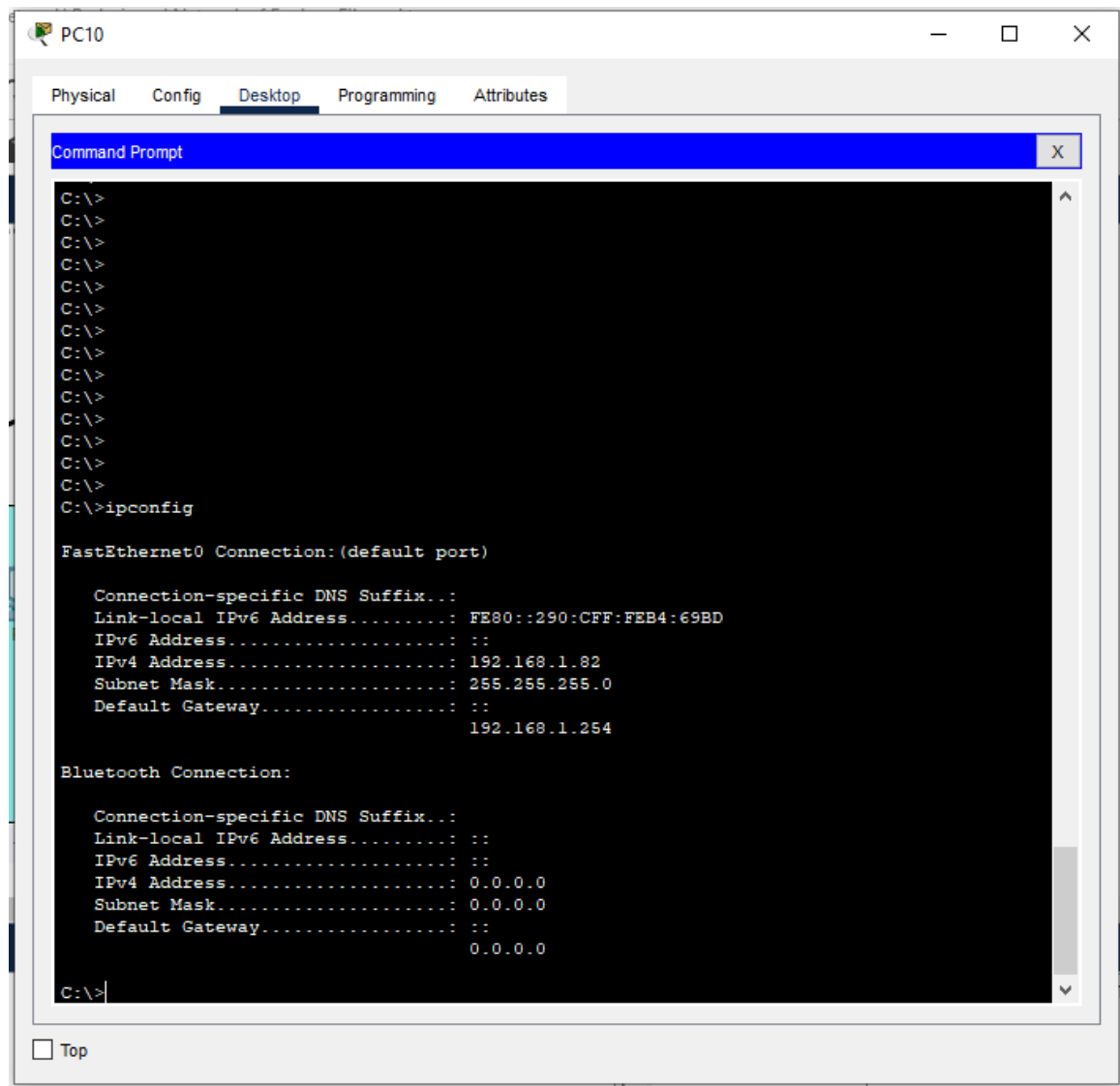


Figure 121 Displays ipconfig for Customer & Reception Area Department PC

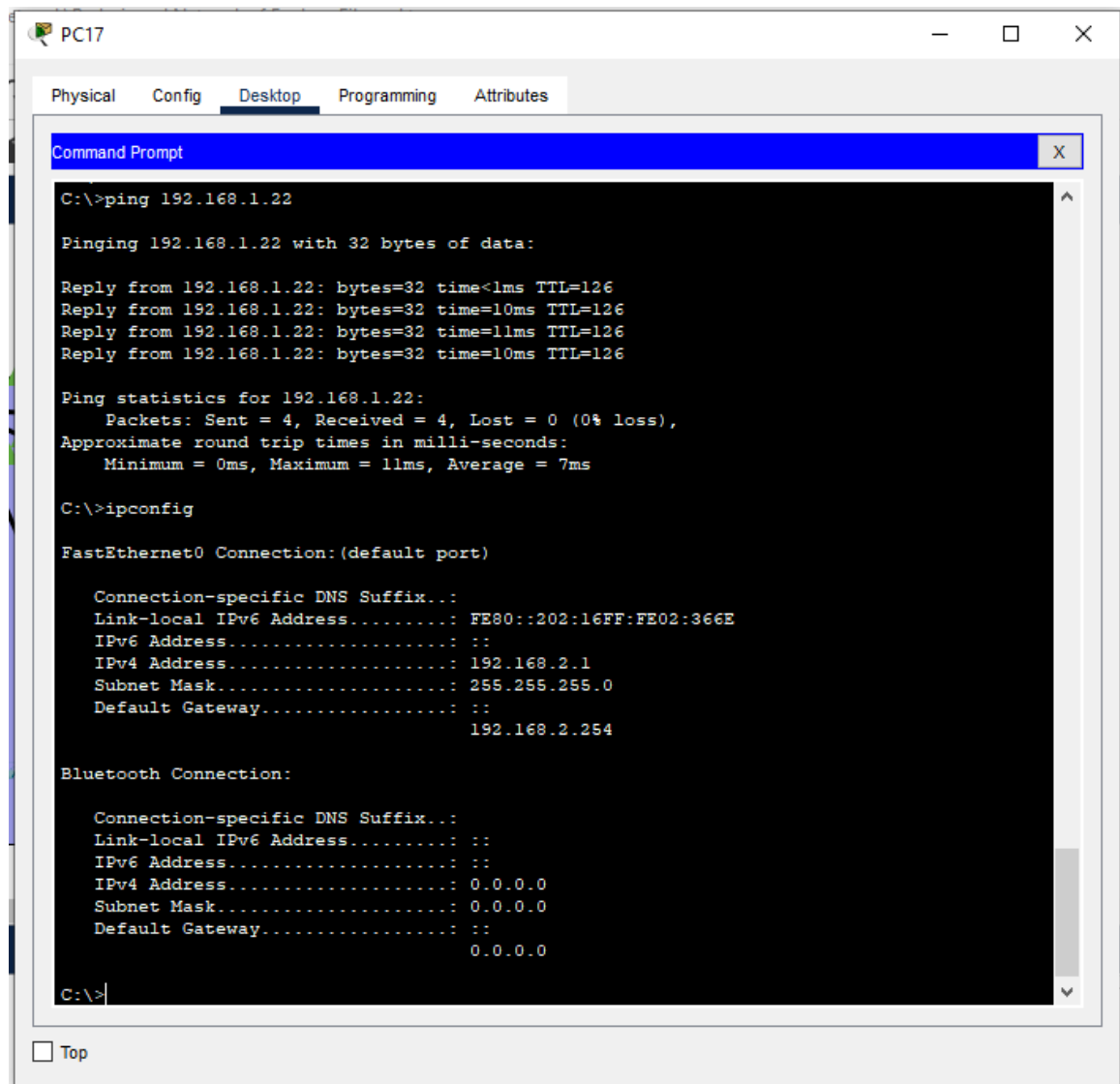


Figure 122 Displays ipconfig for Media Development & Storage Department PC

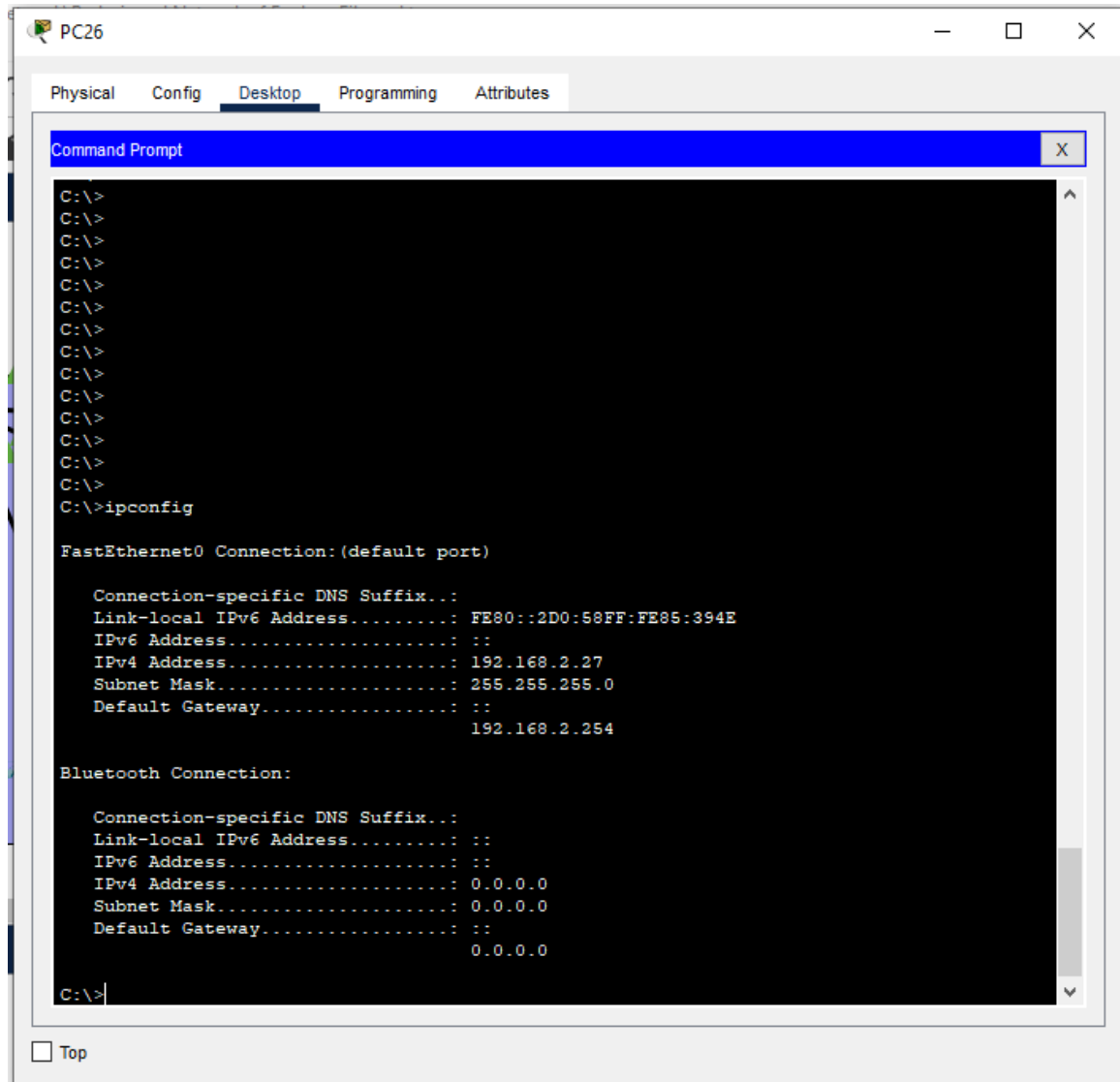


Figure 123 Displays ipconfig for Office Department PC

3.3 Explore system's capabilities for device growth and communication

The existing network infrastructure of Enclave Movie Company provides a foundation for device growth and communication, but it may require enhancements to meet modern-day standards. Here are some considerations regarding the system's capabilities for device growth and communication are as follows.

Scalability: The current network setup seems to be designed to accommodate the existing number of devices in each building. However, it is important to assess the scalability of the infrastructure to support future growth. As the company expands and more devices are added, the network should be able to handle increased traffic and provide sufficient resources for all connected devices.

LAN Connectivity: The LAN in Building A, connecting twelve desktop computers and two printers, allows for local communication and file sharing among the devices. This setup can be expanded by adding more switches or utilizing higher-capacity switches to accommodate additional devices in the future.

VLANs: Assigning VLANs to each department provides logical separation and network segmentation. This enhances security and facilitates efficient communication within each department. As the company grows and new departments are added, additional VLANs can be created to accommodate the new departments and ensure secure communication between them.

Switches and Routers: The current setup utilizes nine switches connected to two routers. This allows for the interconnection of devices within each building and facilitates communication between the buildings. Depending on the growth of the company and the number of devices to be added, it may be necessary to upgrade switches or add more switches to ensure sufficient network capacity and connectivity.

Wireless Access Point: The installation of a wireless access point enables wireless connectivity for devices, such as laptops and mobile devices. This allows flexibility and

mobility within Building B. As the number of wireless devices increases, additional access points may be required to ensure optimal coverage and performance.

Security: When enhancing the network infrastructure, security measures should be a priority. Implementing measures such as firewalls, intrusion detection systems, and encryption protocols can help protect the network from unauthorized access and ensure the security of sensitive data.

Network Monitoring and Management: As the network grows, it becomes important to have robust network monitoring and management tools in place. These tools can help administrators keep track of network performance, identify bottlenecks, troubleshoot issues, and optimize the network infrastructure to meet the communication needs of the organization.

Quality of Service (QoS): QoS can be implemented to prioritize traffic and ensure that communication devices, such as VoIP phones or video conferencing systems, receive sufficient bandwidth and low latency. This is important for maintaining the quality of real-time communication services.

Power over Ethernet (PoE): PoE switches can be utilized to power communication devices such as IP phones, wireless access points, or surveillance cameras, eliminating the need for separate power sources. This simplifies installation and allows for flexibility in device placement.

Network Access Control (NAC): NAC solutions can be implemented to ensure that only authorized devices and users are allowed to connect to the network. This helps in securing the network and preventing unauthorized access.

In summary, while the existing network infrastructure of Enclave Movie Company provides a foundation for device growth and communication, enhancements may be needed to meet modern-day standards. Scalability, VLANs, switches, routers, wireless access points, security measures, network monitoring, Quality of Service (QoS), Power over Ethernet (PoE), and Network Access Control (NAC) are all important considerations when planning to enhance and secure the network infrastructure.

Harvard Referencing

- <https://aws.amazon.com/what-is/computer-networking/>
- https://www.tutorialspoint.com/data_communication_computer_network/computer_network_models.htm
- <https://www.guru99.com/tcp-ip-model.html>
- <https://www.geeksforgeeks.org/similarities-between-tcp-ip-model-and-osi-model/>
- <https://www.sunbirdcim.com/glossary/ring-topology#:~:text=Ring%20topology%20is%20a%20type,known%20as%20a%20unidirectional%20ring>
- <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-hybrid-topology/>
- <https://www.javatpoint.com/computer-network-tutorial>
- <https://www.techtarget.com/searchvmware/definition/VMware-Workstation>