**Khawaja Fareed university of Engineering &information technology Rahim yar khan**

**Department: Computer Engineering**

****

**Data Communication & Computer Networks**

**Lab**

# Open Ended Lab for software-based subjects.

an open-ended lab scenario for exploring data communication and computer networks:

**Title: Exploring Network Design and Performance Optimization**

## Objective:

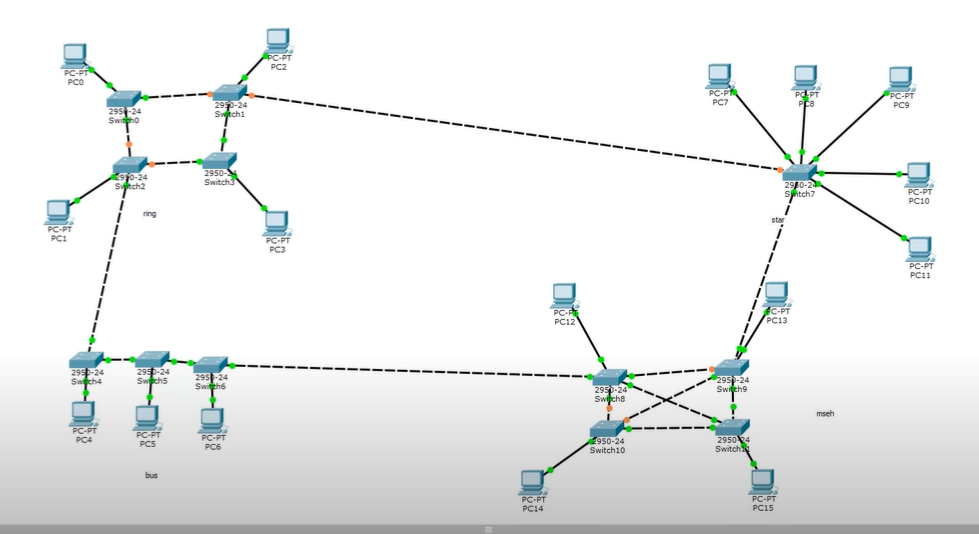
The objective of this open-ended lab is to provide students with hands-on experience in exploring various aspects of network design, protocols, and performance optimization in computer communication and networking.

## Tasks:

**Task no 1**

### Network Topology Design:

* + Design a network topology using simulation software or network design tools.
  + Include components such as routers, switches, hubs, and end devices (e.g., computers, servers, printers).



Consider factors such as network size, scalability, redundancy, and fault tolerance in your design.

* + Network Topology Overview:

Our network design encompasses multiple topologies within Cisco Packet Tracer, including ring, bus, mesh, and star topologies.

Ring Topology:

* Utilizing a ring topology, switches are interconnected in a circular fashion, with each switch linked to two others.
* PCs are directly connected to switches, enabling communication within the ring.

Bus Topology:

* Employing a bus topology, switches are linearly connected along a backbone cable.
* PCs connect to switches, facilitating communication along the shared network medium.

Mesh Topology:

* Incorporating a mesh topology, switches are interconnected with redundant links, providing multiple paths between switches.
* This topology enhances redundancy and fault tolerance within the network.

Star Topology:

* Adopting a star topology, all devices are connected to a central switch, acting as a hub for communication.
* PCs are directly connected to the central switch, streamlining network access.

Interconnection between Topologies:

* Establishing connections between switches from different topologies creates a hybrid network environment.
* For instance, switches from the ring, bus, and mesh topologies are interconnected, enabling communication across network segments.

Considerations:

* Throughout the design process, we prioritized factors such as network size, scalability, redundancy, and fault tolerance.
* Redundancy mechanisms like STP and redundant links were implemented to ensure network stability and resilience against failures.
* Security measures including access control lists and port security were considered to safeguard the network against unauthorized access and cyber threats.

### Protocol Exploration:

* + Investigate different network protocols and their roles in data communication.

# **Transmission Control Protocol/Internet Protocol (TCP/IP):**

# TCP/IP serves as the backbone of internet communication, ensuring reliable data transfer between devices. TCP guarantees data delivery by establishing connections and sequencing data packets, while IP handles addressing and routing to direct packets across networks.

# **Hypertext Transfer Protocol (HTTP):**

# HTTP governs the exchange of web content, allowing web browsers to request and receive web pages from servers. It defines the rules for client-server interaction, enabling seamless browsing experiences.

# **Domain Name System (DNS):**

# DNS acts as the internet's phonebook, translating human-readable domain names into machine-readable IP addresses. It enables users to access websites using familiar domain names, handling the behind-the-scenes address resolution process.

# **File Transfer Protocol (FTP):**

# FTP facilitates the transfer of files between clients and servers, serving as a reliable means of file sharing and management. It provides commands for uploading, downloading, and organizing files on remote servers.

# **Simple Mail Transfer Protocol (SMTP):**

# SMTP manages the transmission of email messages across servers, ensuring efficient delivery from sender to recipient. It handles tasks such as message routing, addressing, and delivery notification.

# **Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP):**

# POP3 and IMAP are email retrieval protocols used by clients to access messages stored on servers. POP3 downloads emails to a local device, while IMAP allows for remote access and synchronization across multiple devices.

# **Secure Shell (SSH) and Telnet:**

# SSH and Telnet facilitate remote access to network devices for configuration and management. While Telnet offers basic command-line access, SSH provides enhanced security through encryption, safeguarding sensitive data during transmission

# **Task 2 part 2**

* + **Compare and contrast protocols at different layers of the OSI model (e.g., TCP/IP, HTTP, DNS, FTP).**

Physical Layer (Layer 1):

* Ethernet (IEEE 802.3): Operates at the physical layer, defining specifications for hardware connections, signaling, and transmission of raw data bits over a physical medium like copper or fiber optic cables.
* Wi-Fi (IEEE 802.11): Also operates at the physical layer, but wirelessly. It defines specifications for wireless communication, including modulation techniques, channel access, and data transmission over radio frequencies.
* Fiber Distributed Data Interface (FDDI): Another physical layer protocol, primarily used in older fiber optic networks. It specifies token-passing mechanisms for transmitting data over fiber optic cables.

Data Link Layer (Layer 2):

* Ethernet (IEEE 802.3): Defines the data link layer frame format, MAC addressing, and Ethernet switching for LAN communication.
* Point-to-Point Protocol (PPP): A data link layer protocol used for establishing a direct connection between two network devices over serial links, commonly used in dial-up and DSL connections.
* IEEE 802.1Q (VLAN tagging): A protocol used for implementing virtual LANs (VLANs) at the data link layer, allowing network segmentation and isolation.

Network Layer (Layer 3):

* Internet Protocol (IP): Operates at the network layer, providing logical addressing, routing, and packet forwarding across interconnected networks.
* Internet Control Message Protocol (ICMP): A network layer protocol used for error reporting, diagnostics, and network management tasks such as ping and traceroute.
* Open Shortest Path First (OSPF): A routing protocol operating at the network layer, used for dynamic routing within autonomous systems, utilizing link-state routing algorithms.

Transport Layer (Layer 4):

* Transmission Control Protocol (TCP): Operates at the transport layer, providing reliable, connection-oriented data delivery, flow control, and error recovery mechanisms.
* User Datagram Protocol (UDP): Also operates at the transport layer, providing lightweight, connectionless data delivery without error correction or flow control, suitable for real-time applications.
* Stream Control Transmission Protocol (SCTP): A transport layer protocol offering features of both TCP and UDP, providing reliable, message-oriented data delivery with support for multi-homing and multistreaming.

Session Layer (Layer 5):

* NetBIOS (Network Basic Input/Output System): Historically used at the session layer, providing communication services between applications over a LAN. It has been largely replaced by other protocols in modern networks.
* Remote Procedure Call (RPC): A session layer protocol used for inter-process communication between networked systems, allowing remote execution of procedures and functions.
* Session Initiation Protocol (SIP): An application layer protocol used for initiating, modifying, and terminating multimedia sessions over IP networks, commonly used in VoIP and video conferencing applications.

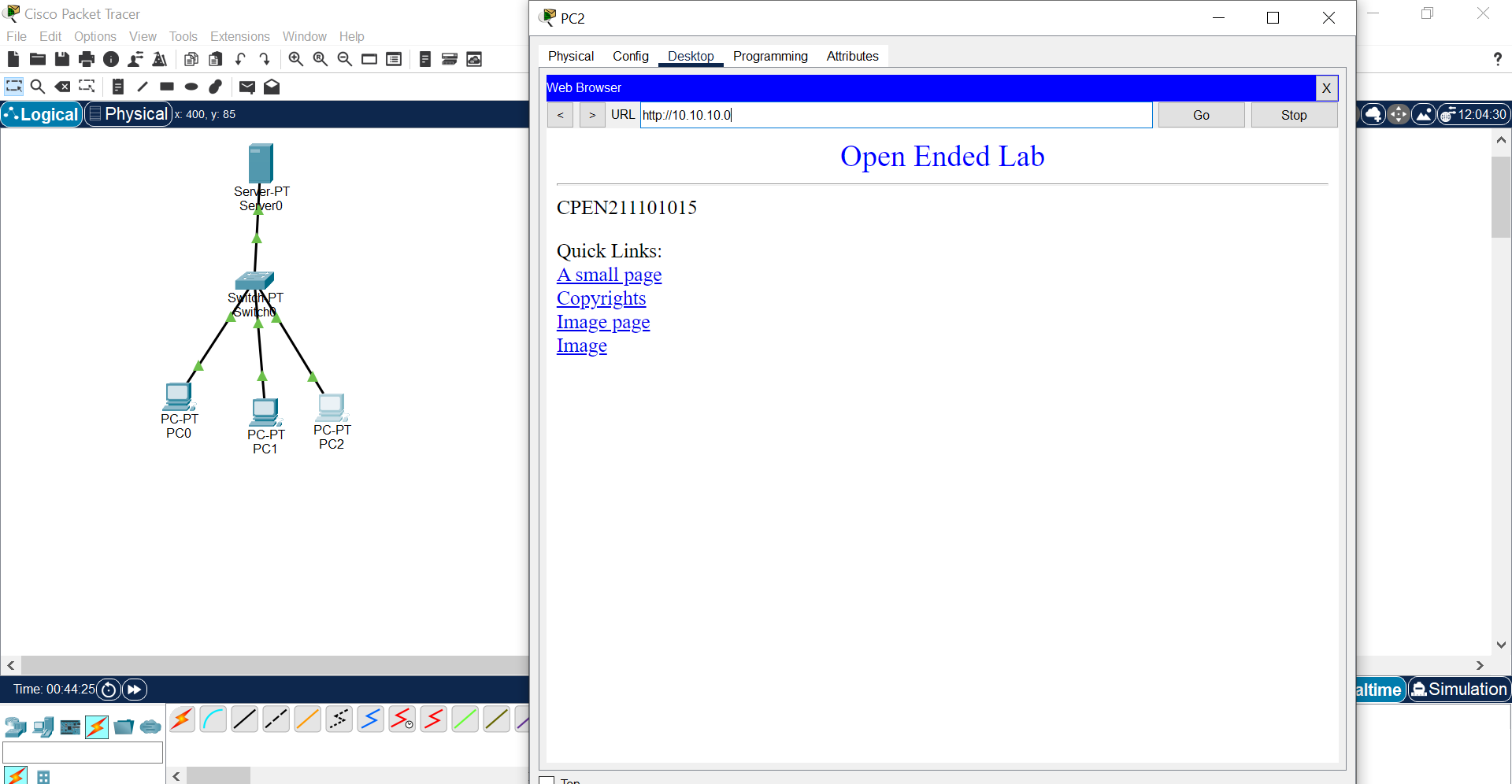
Presentation Layer (Layer 6):

* Secure Sockets Layer (SSL) / Transport Layer Security (TLS): Provides encryption, authentication, and data integrity services for secure communication between networked applications, typically operating above the transport layer.
* Multipurpose Internet Mail Extensions (MIME): Defines formats for encoding multimedia content and email attachments, facilitating interoperability between email clients and servers.
* Graphics Interchange Format (GIF): A file format used for displaying images and animations on web pages, with data compression and color palette features defined at the presentation layer.

Application Layer (Layer 7):

* Hypertext Transfer Protocol (HTTP): An application layer protocol for distributed, collaborative, and hypermedia information systems, commonly used for accessing web resources and websites.
* File Transfer Protocol (FTP): Another application layer protocol used for transferring files between clients and servers over a network, supporting various file operations such as upload, download, and deletion.
* Simple Mail Transfer Protocol (SMTP): A protocol for email transmission, operating at the application layer to route and deliver electronic mail messages between mail servers.
  + **Implement and test a subset of protocols to understand their functionality and usage in network communication.**
  + **Using http in cisco packet tracer**
  + HTTP (Hypertext Transfer Protocol):

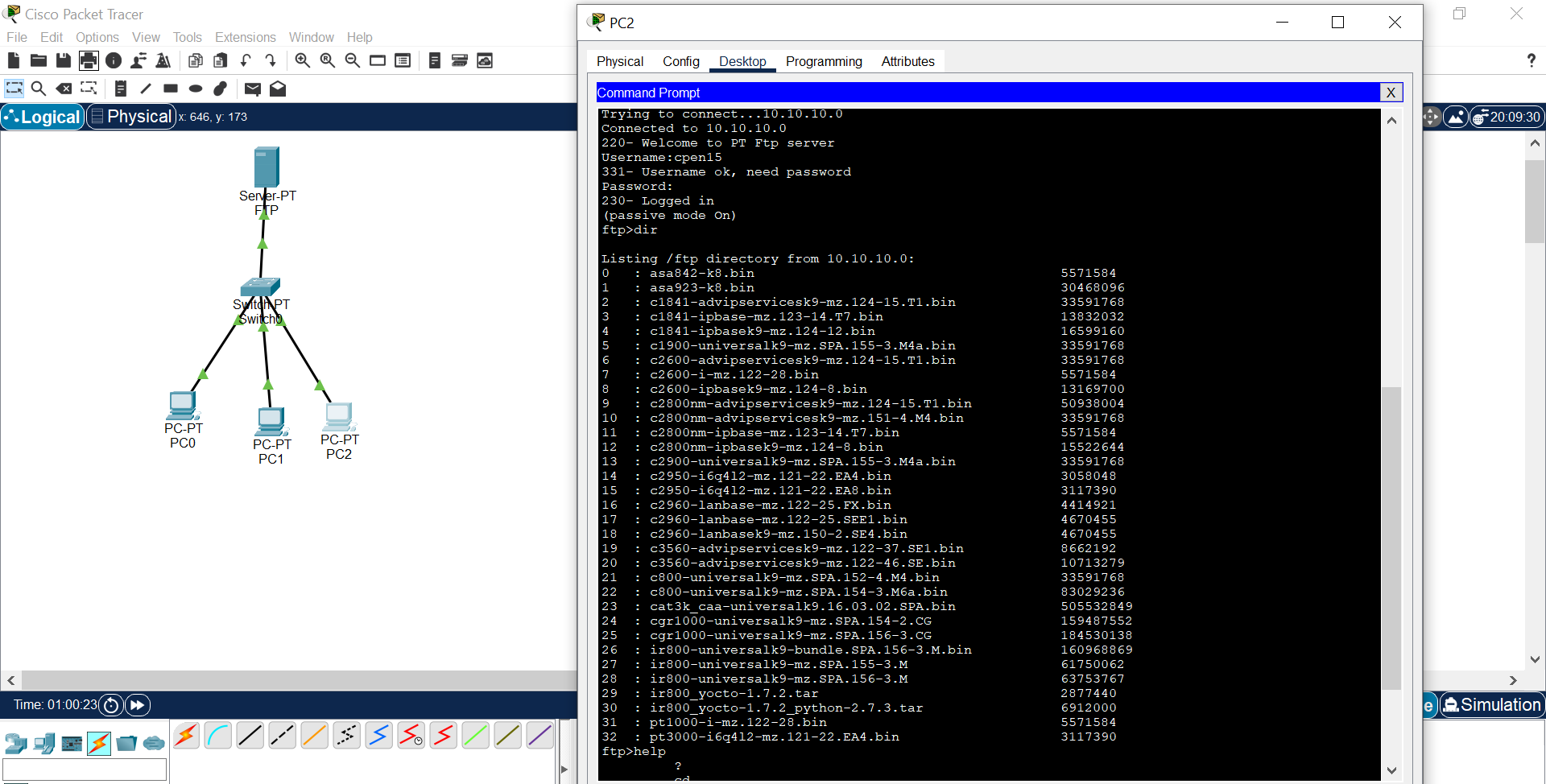
1. Definition: HTTP is an application layer protocol for transmitting web documents over the internet.
2. Role: It enables web browsers to request resources from servers and receive responses.
3. Communication Model: HTTP follows a client-server model.
4. Stateless Protocol: Each request is independent, requiring additional mechanisms for session state.
5. Protocol Versions: HTTP/1.1 (widely used), HTTP/2 (performance improvements).
6. Request-Response Cycle: Clients send requests, servers process and respond with resources.
7. Methods: GET, POST, PUT, DELETE, HEAD (indicating action).
8. Status Codes: Indicate request outcomes (e.g., 200 OK, 404 Not Found).



**File transfer Protocol:**

FTP (File Transfer Protocol):

1. Definition: FTP is an application layer protocol for transferring files between clients and servers over a network.
2. Role: It provides a mechanism for uploading, downloading, and managing files on remote servers.
3. Communication Model: FTP operates on a client-server model, where clients establish connections to servers for file transfer.
4. Connection Modes: FTP supports two connection modes:
   * Active Mode: Client opens a data connection to the server.
   * Passive Mode: Server opens a data connection to the client.
5. Commands: FTP uses commands such as RETR (retrieve), STOR (store), LIST (list directory contents), and DELE (delete) to perform file operations.
6. Authentication: Users are authenticated using usernames and passwords, with options for anonymous access (username: anonymous, password: email address).
7. Data Transfer: FTP transfers data in clear text, making it vulnerable to interception. FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) provide secure alternatives.
8. Ports: FTP uses port 21 for control connections and additional ports for data connections (20 for active mode, dynamic ports for passive mode).



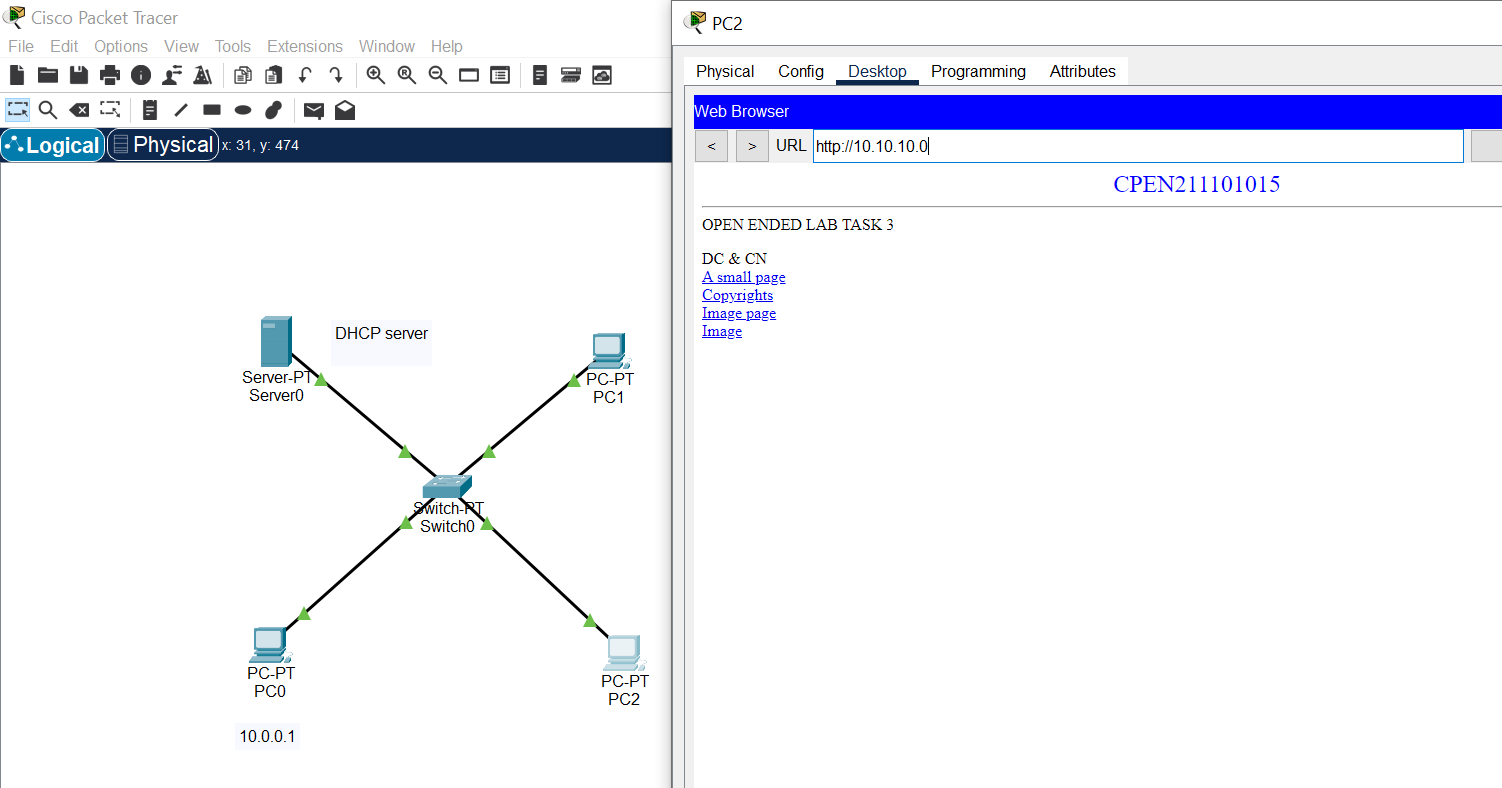
### 

### 

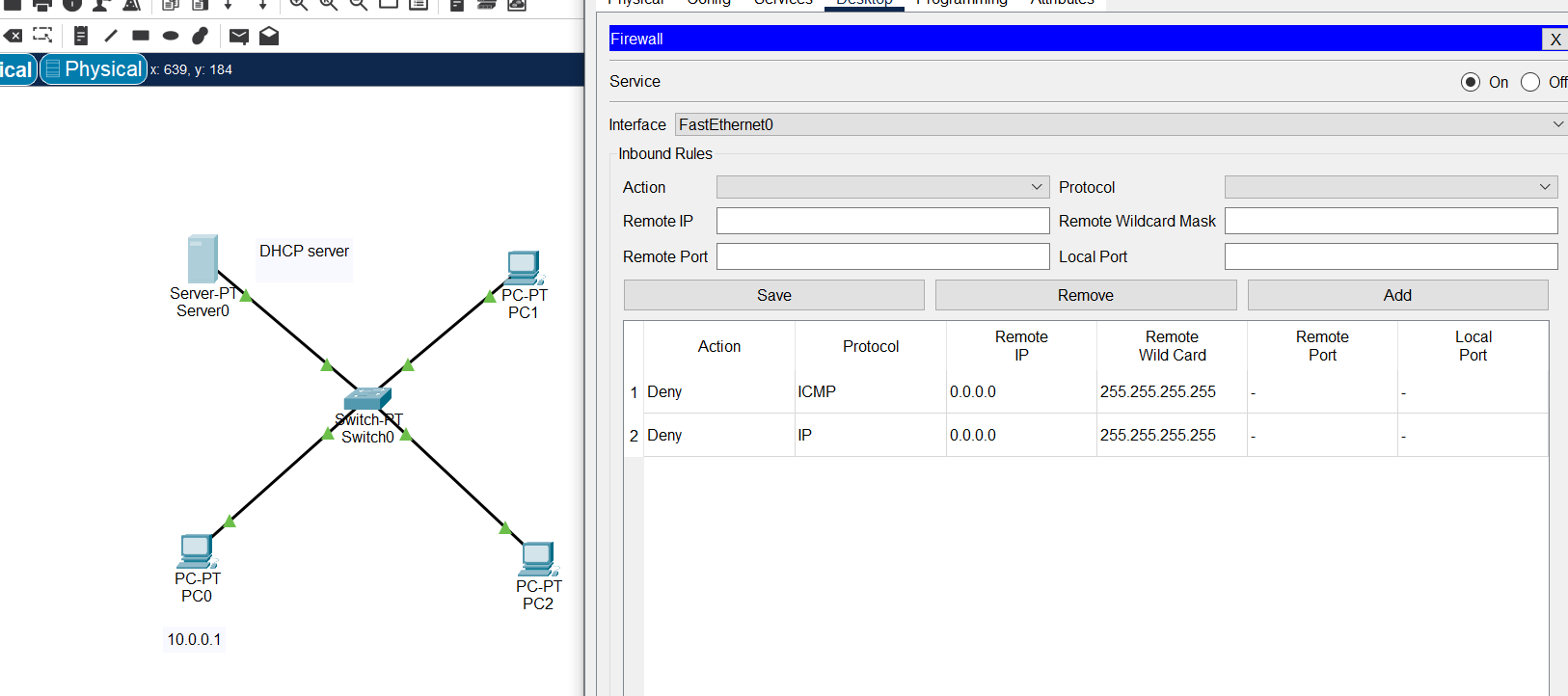
### Security and Reliability:

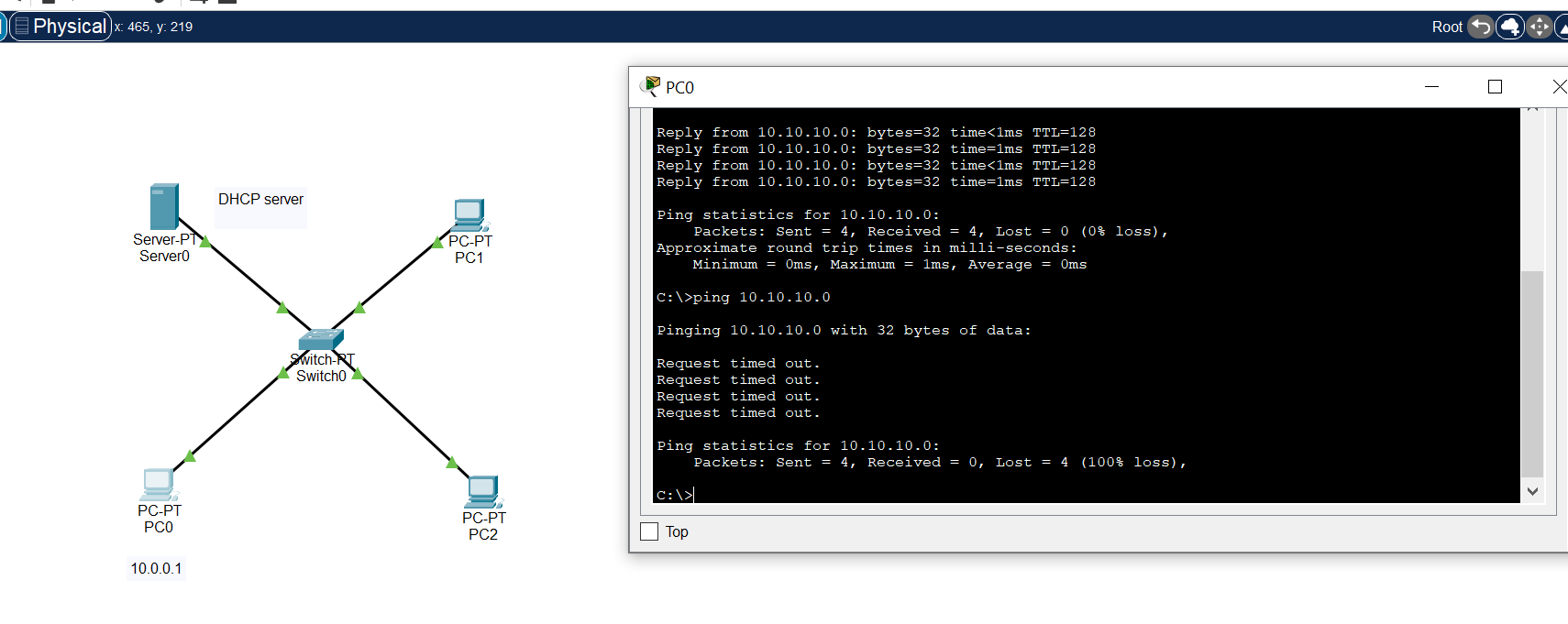
* + Study the principles of network security and reliability mechanisms.
  + **Design and implement security measures such as firewalls, encryption, and access control lists (ACLs) to protect the network from unauthorized access and cyber threats.**

Ans:  
**Firewall**:



ALLOWING AND DENYING DIFFERENT ACTION USING FIREWALL

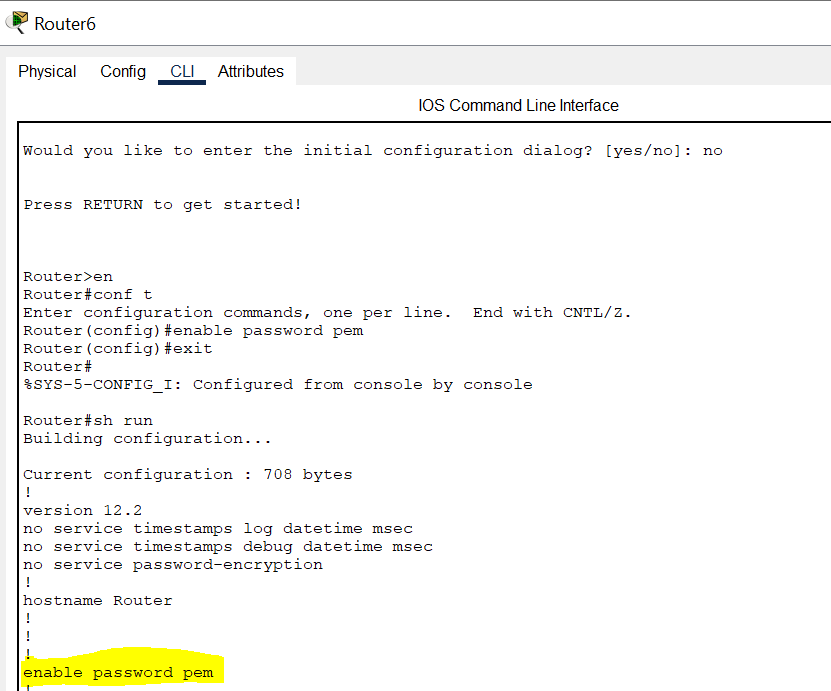




**Encryption**

Encryption is a vital tool for securing network data by converting it into an unreadable format using algorithms and keys. It ensures confidentiality, integrity, and authentication of data during transmission or storage. There are two main types: symmetric (using the same key for encryption and decryption) and asymmetric (using different keys). Encryption is used in VPNs, SSL/TLS, and data storage to protect against unauthorized access. Proper key management is essential for effective encryption.

Implementation:



* + Evaluate the e

### applying encryption:

### 

### Now encrypted:

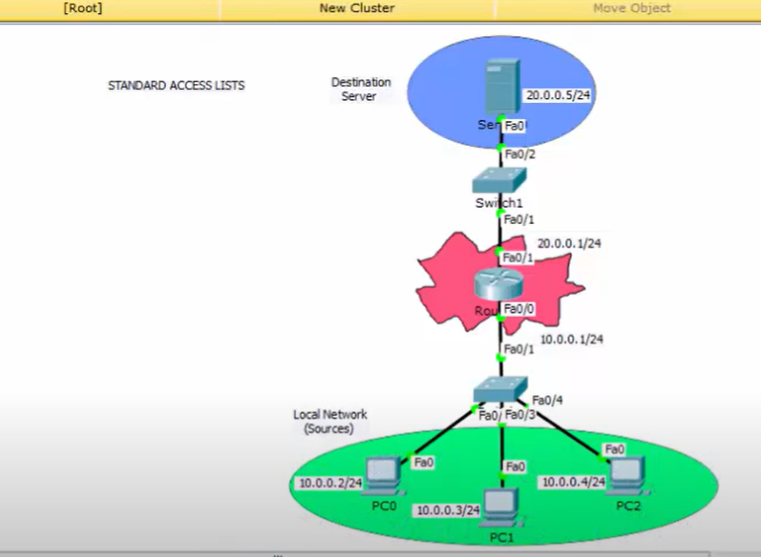
### 

### Access control list”

Access Control Lists (ACLs) are an integral part of network security, allowing administrators to control the flow of traffic in and out of a network device such as a router, switch, or firewall. Here's a detailed overview of ACLs:

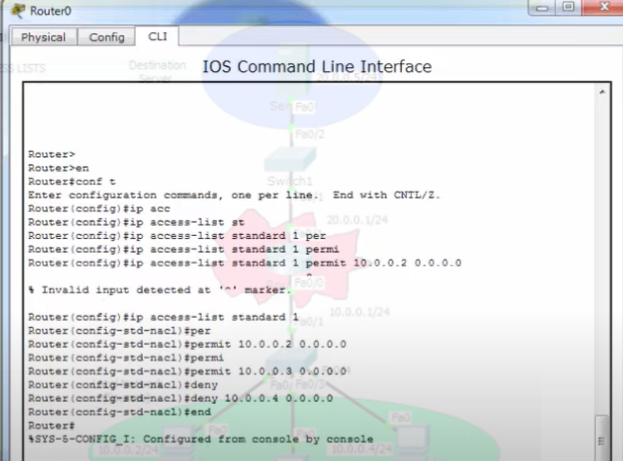
1. Purpose:
   * ACLs serve as a security mechanism to permit or deny traffic based on specified criteria.
   * They help enforce security policies by controlling which packets are allowed to pass through the network device and which are blocked.
   * ACLs can be used to filter traffic at various points in the network, such as at the edge of a network, between network segments, or on individual devices.

**CONFIGURE ACL USING ACL:**



In this diagram we will deny the pc2 to the server and access pc0 and pc1 to the server through ACL

Writing ACL ON Router 0:  
We can use 1 to 99 for standard ACL and   
1000 to 1099 for extended ACL



ACL Created

### Applying Acl:

### 

### 

### Verifying Configuration:

### Pc0 and pc1 access the server and pc2 not

### Pc0 is accessing the server

### 

### But pc0 not because of ACL:

### Destination unreachable because of ACL:

### 

### Quality of Service (QoS):

* + Explore the concept of QoS and its importance in network communication.
  + Design and implement QoS policies to prioritize traffic and ensure optimal performance for critical applications (e.g., VoIP, video streaming).
  + Measure the impact of QoS policies on network performance and user experience.
  + Quality of service (QoS) in data communication refers to the capability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. It encompasses various parameters such as reliability, bandwidth, latency, jitter, and packet loss, among others. Here are some key aspects of QoS in data communication:

1. Reliability: Ensuring that data is delivered accurately and consistently without errors or loss.
2. Bandwidth: Providing sufficient network capacity to accommodate the data traffic demands, ensuring that data can be transmitted without congestion.
3. Latency: Minimizing the delay between the transmission and reception of data packets. Low latency is crucial for real-time applications like voice and video conferencing.
4. Jitter: Variation in latency over time. Consistent and predictable latency is essential for applications like streaming media.
5. Packet Loss: Minimizing the number of lost or discarded packets during transmission, which can degrade the quality of communication.
6. Prioritization: Assigning priorities to different types of traffic based on their importance or requirements. For example, voice and video traffic may be given higher priority than email or file transfers.
7. Resource Reservation: Allocating network resources such as bandwidth or buffer space to ensure that certain flows meet their QoS requirements.
8. Traffic Shaping and Policing: Controlling the flow of data to adhere to predefined QoS parameters, such as limiting the rate of traffic to prevent congestion.
9. Congestion Control: Implementing mechanisms to manage network congestion and prevent degradation of service quality during periods of high traffic.
10. End-to-End QoS: Ensuring consistent QoS across the entire network path, from the source to the destination, often requiring cooperation and coordination among network devices and protocols

### Advanced Topics Exploration (Optional):

* + Explore advanced topics in network design and architecture such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Network Automation.
  + Investigate emerging technologies and protocols (e.g., IPv6, 5G networks) and their potential impact on future network design and communication.

## Deliverables:

* Lab report documenting the design, implementation, and analysis of the network topology and protocols.
* Presentation summarizing key findings, insights, and recommendations from the lab.

# Activity :

## Question no#1:

#### Scenario:

A smart home automation company is developing a network infrastructure for its latest automation project. The project aims to connect various smart devices such as thermostats, lights, security cameras, and smart appliances within a home environment. Design a network topology that supports the automation project's requirements and incorporates a few key protocols for efficient communication between devices.

#### Guidelines:

1. Identify Smart Devices: Begin by identifying the types of smart devices that will be connected to the network. These may include thermostats, lights, motion sensors, door locks, security cameras, and smart appliances.
2. Determine Communication Requirements: Consider the communication needs of the smart devices, including real-time control commands, sensor data collection, and remote access for monitoring and management.
3. Select Protocols: Choose a few key protocols that are suitable for the automation project's requirements. Common protocols used in smart home automation include Wi-Fi, Zigbee, Z-Wave, and Bluetooth Low Energy (BLE).
4. Design Network Topology: Based on the selected protocols, design a network topology that facilitates communication between smart devices while ensuring reliability, scalability, and security.
5. Determine Gateway Devices: Identify gateway devices that will serve as intermediaries between different communication protocols. Gateways may be required to bridge communication between devices using different protocols, such as Wi-Fi to Zigbee or Zigbee to Z-Wave.
6. Consider Security: Implement security measures to protect the smart home network from unauthorized access and cyber threats. This may include encryption, authentication mechanisms, and secure access controls.
7. Plan for Integration: Ensure that the network topology allows for seamless integration with other smart home systems and platforms, such as voice assistants (e.g., Amazon Alexa, Google Assistant) or mobile applications.
8. Test and Validate: Test the network topology in a simulated environment to ensure that smart devices can communicate effectively and perform automated tasks as intended. Validate the network's performance, reliability, and scalability under different scenarios.
9. Document the Design: Document the network topology design, including device placement, protocol configurations, security settings, and integration details. This documentation will serve as a reference for installation, troubleshooting, and future expansion of the smart home automation network.
10. Review and Iterate: Review the network topology design to ensure that it meets the automation project's requirements and objectives. Iterate on the design as needed to address any identified issues or optimizations for better performance and usability.

This scenario-based question challenges beginners to design a network topology for a smart home automation project, incorporating a few key protocols and considering various factors such as device communication, security, integration, and testing. It provides a practical exercise for understanding network design principles in the context of real-world applications. **Rubrics:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Completeness** | **Running** | **Complexity** | **Total** |
|  |  |  |  |

Lab Instructor Signature