Batch: B-1   **Roll Number: 16010422234**   **Name: Chandana Ramesh Galgali**

Experiment Number: 8 - Network Design using Simulation software

---

Aim of the Experiment: Network Design using Simulation software

---

Program/ Steps:

Write a problem statement clearly indicating the network requirement and then design the Network diagram for the same using any Simulation Software.

Problem Statement: \

Network Requirement for a Research Laboratory

The research laboratory is facing network-related challenges that hinder efficient collaboration and data sharing among researchers. The current network infrastructure is outdated, resulting in slow data transfer speeds and limited connectivity options. Additionally, there is a need to ensure the security and integrity of sensitive research data. To address these issues, the research laboratory requires a modern and robust network infrastructure.

The network diagram for the research laboratory's network infrastructure is designed using Packet Tracer Cisco. It includes the following components:

1. Internet Service Provider (ISP): The ISP provides the research laboratory with a high-speed internet connection.

2. Router: The router connects the research laboratory's internal network to the ISP, serving as the gateway for all incoming and outgoing network traffic.

3. Firewall: The firewall is placed between the router and the internal network to provide advanced security measures, including intrusion detection and prevention, to safeguard sensitive research data.

4. Core Switch: The core switch acts as the backbone of the network, connecting various switches and routing network traffic within the research laboratory.

5. Distribution Switches: Multiple distribution switches are strategically placed across the laboratory to provide network connectivity to different research departments and areas.

6. Access Switches: Access switches are connected to the distribution switches and provide network connectivity to individual research workstations, servers, and equipment.

7. Wireless Access Points (WAPs): WAPs are deployed throughout the laboratory to provide wireless network access, enabling researchers to connect their devices and access network resources from anywhere within the facility.

8. Research Servers: Specialized research servers, such as data storage servers, computational servers, and virtualization servers, are connected to the network to support data-intensive research activities.

9. Research Workstations: High-performance workstations equipped with advanced processing capabilities are connected to the network to facilitate data analysis, simulations, and collaboration among researchers.

10. Research Equipment: Various research equipment, such as scientific instruments and data acquisition devices, are connected to the network to enable data collection, monitoring, and control.

11. Virtual Private Network (VPN): A VPN is implemented to provide secure remote access to the laboratory's network resources, allowing researchers to work from off-site locations while maintaining data confidentiality.

12. Network Monitoring System: A network monitoring system is deployed to continuously monitor the network infrastructure, detect any performance issues or security threats, and ensure optimal network performance.

Network Design:
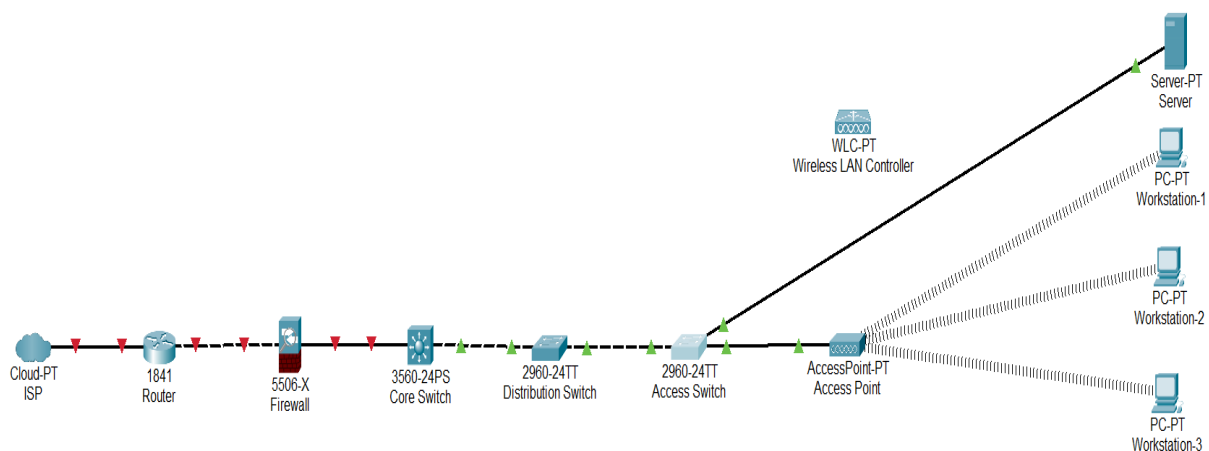
Explanation:

1. Internet Service Provider (ISP): The ISP provides the research laboratory with a high-speed internet connection. This connection is crucial for accessing online resources, collaborating with external partners, and staying updated with the latest research developments.

2. Router: The router acts as the gateway between the research laboratory's internal network and the ISP. It manages the flow of data between the internal network and the internet, ensuring efficient and secure communication.

3. Firewall: The firewall is placed between the router and the internal network to provide advanced security measures. It monitors and filters incoming and outgoing network traffic, protecting the research laboratory's sensitive data from unauthorized access, malware, and other cyber threats.

4. Core Switch: The core switch serves as the backbone of the network, connecting various switches and routing network traffic within the research laboratory. It ensures reliable and high-speed communication between different departments and areas of the laboratory.

5. Distribution Switches: Multiple distribution switches are strategically placed across the laboratory to provide network connectivity to different research departments and areas. These switches help in distributing network traffic efficiently and provide flexibility for future expansion.

6. Access Switches: Access switches are connected to the distribution switches and provide network connectivity to individual research workstations, servers, and equipment. They enable researchers to connect their devices to the network and access shared resources, such as data storage and computational power.

7. Wireless Access Points (WAPs): WAPs are deployed throughout the laboratory to provide wireless network access. Researchers can connect their laptops, tablets, and other wireless devices to the network, allowing them to work from anywhere within the facility while maintaining connectivity and access to network resources.

8. Research Servers: Specialized research servers, such as data storage servers, computational servers, and virtualization servers, are connected to the network. These servers support data-intensive research activities, provide storage for research data, and offer computational power for complex simulations and analyses.

9. Research Workstations: High-performance workstations equipped with advanced processing capabilities are connected to the network. These workstations enable researchers to perform data analysis, run simulations, and collaborate effectively on research projects.

10. Research Equipment: Various research equipment, such as scientific instruments and data acquisition devices, are connected to the network. This connectivity allows researchers to collect, monitor, and control data from these devices, facilitating their experiments and data-driven research.

11. Virtual Private Network (VPN): A VPN is implemented to provide secure remote access to the laboratory's network resources. Researchers can connect to the laboratory's network from off-site locations, ensuring secure communication and access to sensitive research data.

12. Network Monitoring System: A network monitoring system is deployed to continuously monitor the network infrastructure. It detects any performance issues, security threats, or anomalies in the network, allowing network administrators to take proactive measures to ensure optimal network performance and security.

Overall, this network infrastructure design for the research laboratory aims to provide reliable, secure, and high-performance connectivity to support the research activities, collaboration, and data-intensive requirements of the laboratory.

Outcomes: Understand the data communication systems, network topologies and network devices.

Conclusion (based on the Results and outcomes achieved):
The experiment with network design using simulation software proved to be a valuable tool in the planning and implementation of network infrastructures. It provided a safe and controlled environment for testing different configurations, optimizing network performance, and ensuring the network design met the specific requirements of the establishment. The outcomes achieved through this experiment have demonstrated the effectiveness and benefits of utilizing simulation software in network design processes.

References:

Books/ Journals/ Websites:

1. [Cisco Packet Tracer - Networking Simulation Tool (netacad.com)](netacad.com)