Integrated University Network Infrastructure Simulation

E.M.S. EKANAYAKE

2025-12-03

1. Introduction

This project aims to design and simulate a robust network infrastructure for a University Faculty using **Cisco Packet Tracer**. The proposed design connects key operational areas including the Administration Department, Laboratory Complex, Lecture Halls, Auditorium, and Student areas. The network utilizes a **Hierarchical Design Model** (Core, Distribution, and Access layers) to ensure scalability, manageability, and high performance.

2. Project Objectives

The primary goals of this network design are:

- **Centralized Connectivity:** To establish a reliable connection between the Administration building (Central Hub) and all other departments.

- **Network Segmentation:** To implement **VLANs** (Virtual LANs) to isolate traffic between Students, Staff, Management, and Guests for enhanced security and traffic management.

- **Data Services:** To deploy a centralized **Server Farm** hosting DHCP, DNS, Web, and Database services.

- **Wireless Accessibility:** To provide secure Wi-Fi access in designated areas such as the Canteen, Workshops, and specific Labs.

- **Security:** To protect the internal network from external threats using a **Firewall** at the gateway.

3. Network Topology & Architecture

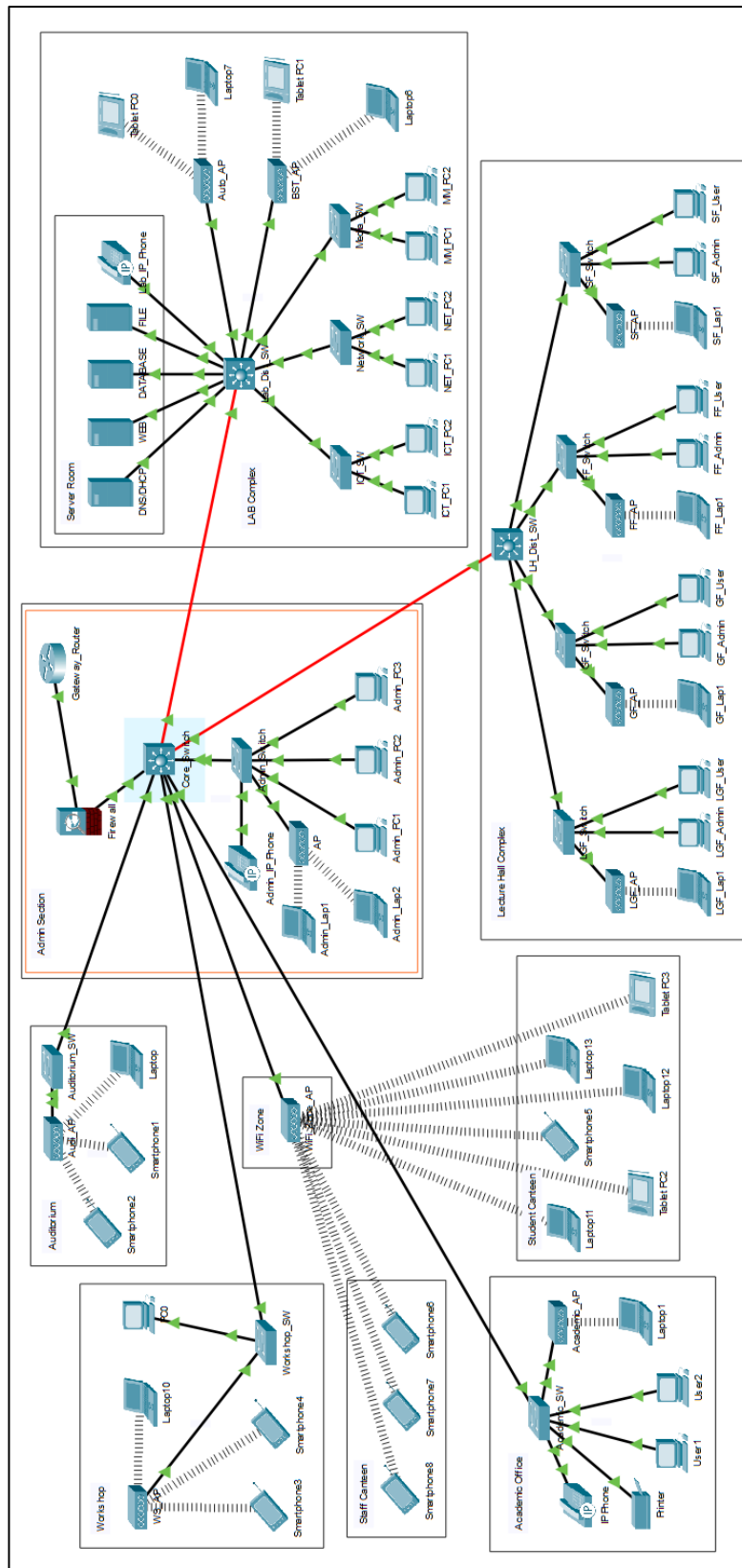The network follows a **Three-Layer Hierarchical Design** to ensure stability and efficiency.

3.1 Hierarchical Structure

- **Core Layer:** Located in the **Admin Department**. It consists of the Main Router, Firewall, and a Layer 3 Core Switch (Cisco 3650) that connects all other buildings.

- **Distribution Layer:** Used in high-traffic areas like the **Lab Complex** and **Lecture Hall Complex**. Layer 3 Switches aggregate traffic from multiple access switches before sending it to the Core.

- **Access Layer:** Consists of Layer 2 Switches (Cisco 2960) located in individual departments (Academic, Auditorium, Workshop) and specific floors/labs to connect end devices like PCs, IP Phones, and Access Points.

3.2 Building Layout & Equipment

- **Admin Department:** The central hub housing the Gateway Router and Campus Firewall. It includes wired connections for staff and a Wi-Fi zone.

- **Lab Complex:** Contains the **Server Farm** (hosting DNS, DHCP, Web, and File servers) and connects 5 specialized laboratories (ICT, Network, Multimedia, Automobile, and BST).

- **Lecture Hall Complex:** A 4-story building utilizing a main distribution switch and separate access switches for the Lower Ground, Ground, 1st, and 2nd floors.

- **Workshop:** Connected directly to the Core Switch via a wired backbone link to ensure stable connectivity for remote workshop areas.

- **Auditorium & Canteen:** Dedicated zones for guest access and student recreation, primarily served by Wireless Access Points (APs).

Network Diagram

4. IP Addressing & VLAN Configuration

To ensure efficient traffic management and security, the network uses **VLANs (Virtual Local Area Networks)**. A logical IP addressing scheme was designed using the **192.168.x.x /24** private address block, where the third octet corresponds to the VLAN ID for easy identification.

4.1 VLAN Allocation Table

VLAN ID	VLAN Name	Network Address	Gateway IP	Usage / Department
10	Management	192.168.10.0/24	192.168.10.1	Network Devices
20	Server Farm	192.168.20.0/24	192.168.20.1	Servers
30	Admin Staff	192.168.30.0/24	192.168.30.1	Admin PC & Wi-Fi
40	Academic	192.168.40.0/24	192.168.40.1	Academic Staff
50	Student Wired	192.168.50.0/24	192.168.50.1	Lecture Halls & ICT Labs
60	Student WiFi	192.168.60.0/24	192.168.60.1	Automobile & BST Labs
70	Workshop	192.168.70.0/24	192.168.70.1	Workshop Complex
80	Canteen	192.168.80.0/24	192.168.80.1	Staff & Student Area
90	Guest	192.168.90.0/24	192.168.90.1	Auditorium Guest Wi-Fi
100	Voice	192.168.100.0/24	192.168.100.1	IP Telephony Services

4.2 IP Assignment Strategy

- **Gateway:** The Core Switch acts as the default gateway for all VLANs (Inter-VLAN Routing enabled).

- **DHCP:** A centralized **DHCP Server** located in the Lab Complex automatically assigns IP addresses to end devices.

- **IP Helper:** The ip helper-address command was configured on the Core Switch SVIs to relay DHCP requests from different VLANs to the central DHCP server.

- **Static IPs:** Critical devices such as Servers, Switches, and Wireless Access Points were assigned static IP addresses from the Management or Server VLANs to ensure stability.

5. Network Services & Security

5.1 Network Services (Server Farm)

A dedicated Server Farm located in the Lab Complex provides essential network services to all users.

- **DHCP Service:** A centralized DHCP server manages dynamic IP allocation for all VLANs. This ensures that devices in different departments (e.g., Student Labs, Canteen, Admin) automatically receive the correct IP address and Gateway configuration based on their VLAN.

- **DNS Service:** The Domain Name System (DNS) server resolves the faculty's local domain names to IP addresses, allowing users to access internal resources using user-friendly names.

- **Web Server:** An internal Web Server (hosted at 192.168.20.11) hosts the faculty website, which is accessible from any PC or laptop within the network.

5.2 Security Implementation

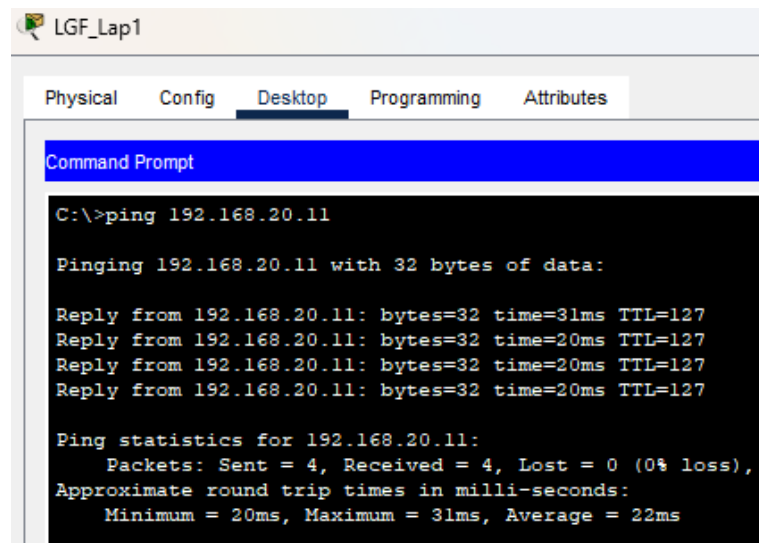Security was a primary focus of the design to protect sensitive faculty data.

- **Perimeter Firewall:** A Cisco ASA Firewall is deployed between the Gateway Router and the Core Switch. This separates the trusted internal network ("Inside") from the untrusted external internet ("Outside"), inspecting incoming and outgoing traffic.

- **VLAN Segmentation:** By separating the network into distinct VLANs, minimizes the risk of unauthorized access to sensitive internal resources.

- **Port Security:** Access ports are configured to prevent unauthorized devices from connecting to critical network segments.

6. Testing & Validation

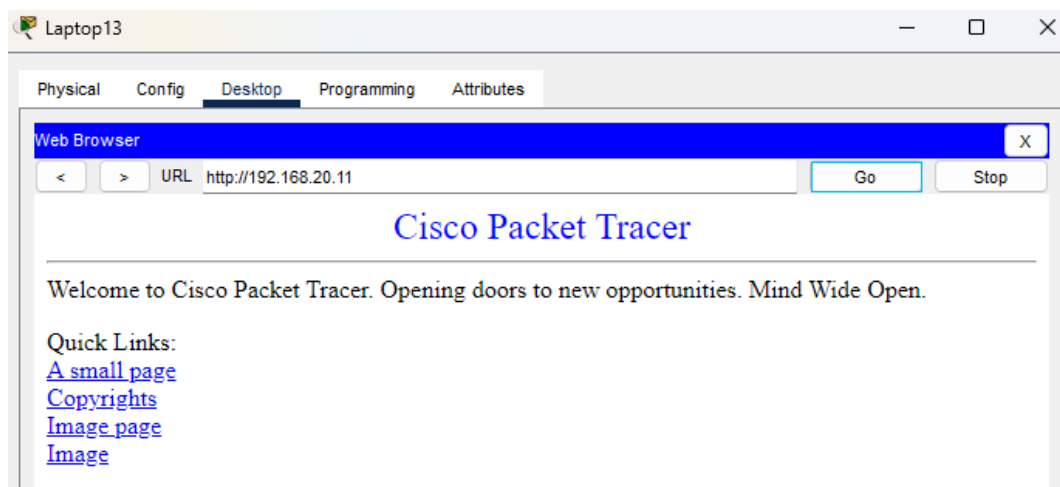The network design was simulated and rigorously tested using **Cisco Packet Tracer**.

- **Connectivity:** Ping tests confirmed successful communication between different VLANs (Inter-VLAN routing) and between remote buildings (Workshop) and the Core.

  Ping the WEB server from Lap1 on Lower Ground Floor of Lecture Hall Building.
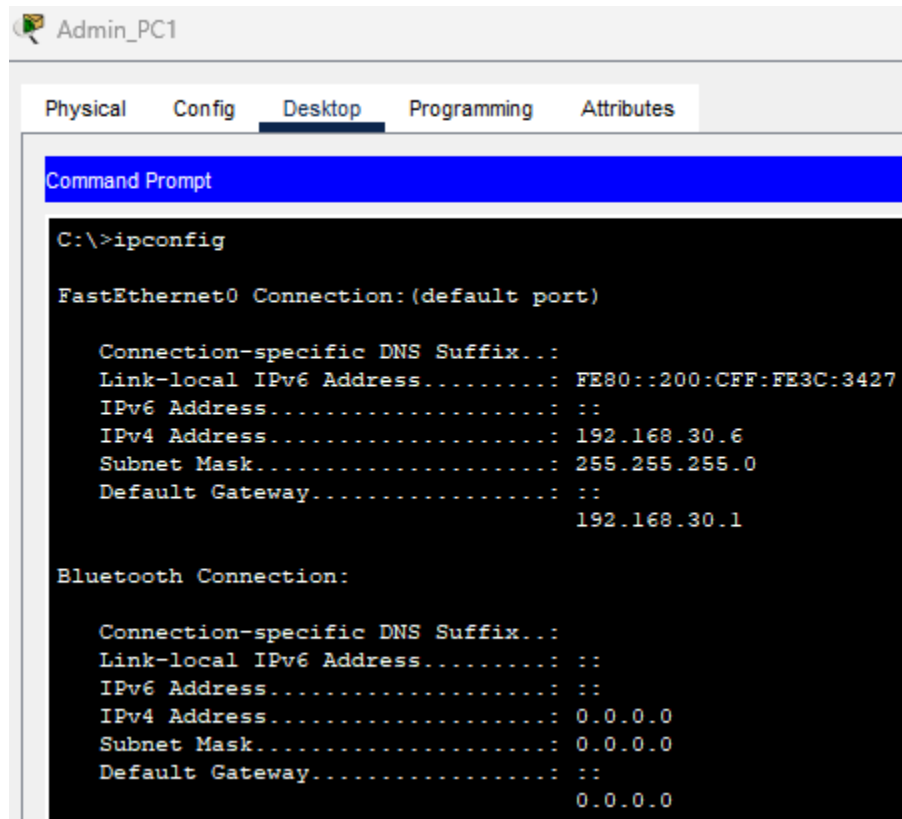

- **Service Availability:** Web browser tests on client PCs confirmed successful access to the Faculty Website.

  Access the WEB server from Laptop connected to VLAN 80 (WiFi Zone)

- **DHCP functionality:** Devices in all zones (Wired and Wireless) successfully obtained IP addresses from the correct VLAN pools.

*IP Configuration check on Admin PC1 using **ipconfig** command*

7. Conclusion

The project successfully demonstrates a scalable, secure, and efficient network infrastructure suitable for Faculty of Technology, University of Sri Jayewardenepura. By utilizing hierarchical architecture and VLAN segmentation, the design meets all user requirements, including centralized management, robust security, and seamless wireless connectivity. The simulation confirms that the network is operational and ready for potential real-world implementation.