Scalable Campus Network Infrastructure Design

Author: Anthony Efemena Edjenuwa

Student ID: C2548409

Project Date: April 2024

Platform: Cisco Packet Tracer & GNS3

Project Overview

This project presents a comprehensive campus network infrastructure designed to support over 20,470 end-users across multiple academic departments. The design ensures high availability, security, scalability, and compliance with enterprise networking standards. The architecture supports future growth beyond 10 years.

Core Features

- Hierarchical Network Design (Core, Distribution, Access)
- IPSec VPN Tunneling for secure remote access
- WLAN Controller with SSIDs per department (Eduroam, TU Staffs, UNI Guest)
- Centralized DHCP servers in the DMZ
- Firewall segmentation with DMZ for public-facing servers
- OSPF routing across routers and ASA firewalls
- VLAN segmentation for each academic department
- Access Control Lists (ACLs) to enforce security policies
- Spanning Tree Protocol (STP) with PortFast and BPDU Guard
- High Availability Ready with EtherChannel and IP Addressing Plans

Device Configuration Snapshots

- ASA Firewalls: Configured for Inside/Outside/DMZ with OSPF and Access Rules
- L3 Switches: VLAN trunking, EtherChannel, Inter-VLAN Routing
- WLC: Managing access points across both campuses
- Wireless: Eduroam, TU Staffs WiFi, and UNI Guest configured per user role
- DHCP: Two servers serving all departments, located in DMZ

- Static IPs: Assigned to critical infrastructure (e.g., DNS, Web, Email servers)

Testing and Verification

- Ping tests performed across:
  - Main to Branch
  - Main to DMZ
  - Branch to DMZ
  - Wireless to Core
- See attached screenshots in the 'PINGING TEST SCREENSHOTS' document

Supporting Files

- Configuration Files: All device CLI configs (Configuration Files and Passwords.pdf)
- Network Diagram: New Network Design.png
- Screenshots: Setup interfaces, WLC, DHCP, Routing (Configuration Screenshots.pdf)
- Ping Tests: Connectivity validated (PINGING TEST SCREENSHOTS.pdf)

Summary

This design aligns with Cisco enterprise architecture standards and supports advanced features like IPSEC VPN, dynamic routing, centralized DHCP, and secure wireless management. It reflects best practices for real-world campus environments and prepares the institution for seamless expansion.