Smart Campus Network Design Using Cisco Packet Tracer

Your Name

February 24, 2025

1 Introduction

This report outlines the design and implementation of a smart campus network using Cisco Packet Tracer, a network simulation tool developed by Cisco Systems. The project encompassed software installation, network topology design, device configuration, connectivity testing, and a critical analysis of the design choices. The primary objective was to establish a secure and operational network tailored to a campus setting while acquiring hands-on experience with network simulation.

2 Installation Process

Cisco Packet Tracer was sourced from the Cisco Netacad website following the creation of a free self-learner account. Version 8.2.2 was downloaded and installed on a 64-bit Windows 10 system. The installation followed a standard procedure, including accepting license agreements and selecting an installation directory. The software launched successfully after login with Netacad credentials.

3 Network Design

The network was engineered to support a smart campus comprising four key buildings: student dormitory, faculty offices, library/common areas, and administrative offices. Each building was equipped with a dedicated switch, linked via trunk connections to a central core router. The core router connected to a firewall router, which interfaced with an ISP router to simulate internet access.

An IP addressing scheme was devised using the 192.168.0.0/16 network, detailed in the table below:

Building	**Subnet**
Student Dormitory	192.168.10.0/24
Faculty Offices	192.168.20.0/24
Library/Common Areas	192.168.30.0/24
Administrative Offices	192.168.40.0/24

Table 1: IP Addressing Scheme

VLANs were employed to segment traffic by user groups (e.g., students, faculty, guests). For example, the student dormitory utilized VLAN 10 for students and VLAN 20 for guests. The Open Shortest Path First (OSPF) protocol was chosen for its scalability and efficiency in dynamic routing.

4 Configuration Steps

4.1 VLANs and Switches

Switches in each building were configured with appropriate VLANs. For the student dormitory, the configuration included:

- VLAN 10 for student devices
- VLAN 20 for guest devices

Ports were assigned to their respective VLANs, and trunk links to the core router facilitated multi-VLAN traffic.

4.2 Core Router Configuration

The core router was set up with subinterfaces for inter-VLAN routing. For the student dormitory, subinterfaces such as GigabitEthernet0/0.10 (VLAN 10) and GigabitEthernet0/0.20 (VLAN 20) were assigned IP addresses within their subnets. OSPF was activated to enable dynamic routing across the network.

4.3 Firewall and Internet Access

A firewall router was positioned between the core router and the ISP router. Network Address Translation (NAT) mapped private campus IPs to a simulated public IP (e.g., 203.0.113.1). Access Control Lists (ACLs) were implemented to allow specific traffic, such as HTTP and HTTPS, while restricting unnecessary services.

4.4 Wireless Configuration

Wireless access points were deployed in each building, with SSIDs tied to VLANs (e.g., "Student_WiFi" for VLAN 10). WPA2 encryption was applied to secure wireless connections.

5 Connectivity Tests

The following tests verified network performance:

- **Ping Tests:** Successful pings within and across VLANs confirmed effective routing.
- **Internet Access:** Devices reached the ISP router, validating NAT and internet connectivity.
- **Wireless Tests:** Wireless devices connected to their SSIDs and communicated with the network and internet.

Initial configuration errors, such as misassigned VLAN ports, were corrected to ensure full functionality.

6 Critical Analysis

The design was assessed for strengths and areas for improvement:

- **Routing Protocol:** OSPF was selected for scalability, though static routing might have been sufficient for this simulation.
- **VLAN Implementation:** VLANs enhanced security and traffic management effectively.
- **Security Measures:** ACLs and NAT were utilized, but a DMZ or 802.1X authentication could bolster security further.
- **Wireless Security:** WPA2 was implemented, though WPA3 could provide superior protection if available.

This project offered practical insights into network design, with potential for future enhancements via advanced security and routing options.

7 Conclusion

This project successfully demonstrated network design principles using Cisco Packet Tracer, achieving a secure and functional campus network. The process underscored the value of meticulous planning and configuration, while identifying opportunities to incorporate advanced features in subsequent designs.