ADVANCED SECURE CAMPUS NETWORK SYSTEM DESIGN AND IMPLEMENTATION USING CISCO PACKET TRACER

[1]K. Balakrishna Maruthiram, [2]Jalagam Mahesh,

[1]Assistant Professor of CSE, JNTU Hyderabad, [2]Student of JNTU Hyderabad
[1]Department of IT, JNTU Hyderabad, [2]Department of IT, JNTU Hyderabad
[1]JNTU Hyderabad, India, [2]JNTU Hyderabad, India

Abstract: Computer Network specialists are in great demand these days. Determining the effectiveness of Cisco Packet Tracer as a teaching aid is the aim of this study. Colleges of higher learning believe that this state of affairs is essential to guaranteeing that each candidate has sufficient IT skills. Tools for network simulation could be recommended as a remedy for this problem because network design requires knowledge of both theory and practical application.

1. INTRODUCTION

Learning about computer networks and receiving instruction in them is a crucial component of a computer science degree. But because this subject is frequently theoretical and advanced, learning might be difficult. The use of simulation-based education can improve the teaching of networking issues by providing a secure and welcoming environment. This will help students understand the ideas more easily and gain a better understanding of the functioning. The use of Cisco Packet Tracer, a tool for simulation known for its efficacy in learning environments, is covered in this study.

Network experts may design, configure, and debug networks in a secure virtual environment with Cisco Packet Tracer, a popular network modeling tool. By simulating network protocols and components, this software enables users to investigate various network configurations, architectures, and scenarios without the need for actual hardware.

2. PROJECT GOAL

This project aims to address the unique challenges and requirements of each campus while ensuring resource exchange and seamless communication throughout the three tiers of the network. The main goal is to use Cisco Packet Tracer, a useful tool for network simulation, to develop, implement, and verify the network layout for both separate university campuses.

3. LITERATURE-REVIEW

In recent years, colleges and universities have increasingly adopted digital technologies for communication, learning, and administration. The core infrastructure of these educational bodies is essential for guaranteeing smooth interactions, safe data exchange, and the effective functioning of services and processes. This research seeks to examine recent findings on university networks, offering a perspective on the expansion, obstacles, and creative approaches in this important area.

3.1 KEY FINDINGS:

Several important conclusions are drawn from the literature research on university networks utilizing Cisco Packet Tracer.

- **Network Architecture:** A Network's establishment and operation are essential to the operation and security of an organization's IT infrastructure. This approach necessitates a delicate balancing act between technological expertise, planning for strategy, and future needs assessment.
- **Network topology:** Selecting the right network layout is a tactical choice based on the unique needs and constraints of the organization. Every design has a different set of benefits and drawbacks, thus the decision should be evaluated in relation to the objectives and features of the network.
- **Network security:** Network security is an ongoing project requiring technology instruments, rules, and user education. To create a strong defense against evolving internet threats, businesses need to continuously modify and enhance their security procedures.

4. CAMPUS ARCHITECTURE:

For my project, I constructed two distinct campuses that were connected by an Internet service provider (ISP) in both locations. Every campus has a demilitarized zone (DMZ) network in addition to its individual personal network.
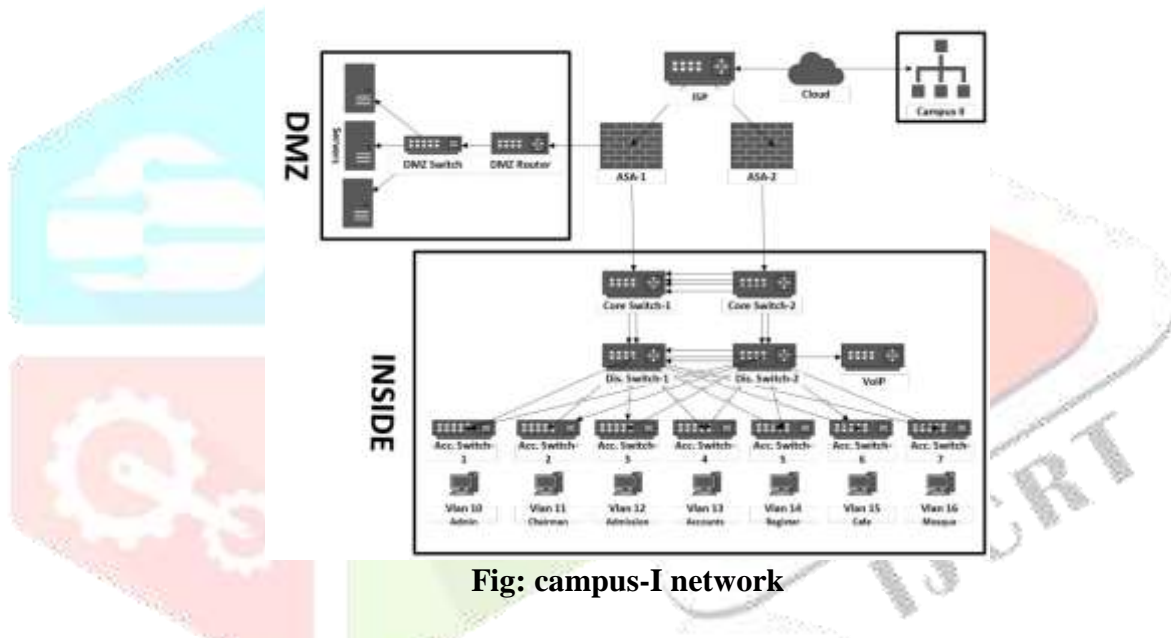
4.1 Campus Network-I:

Fig: campus-I network

The above figure shows system's entry point, seven distinct layer-2 switches are installed, which correspond to the various divisions or VLANs that the system covers. computers are the final devices, which include printers, computers, and other devices. 'Campus I' and 'Campus II' are linked via the Internet service provider.
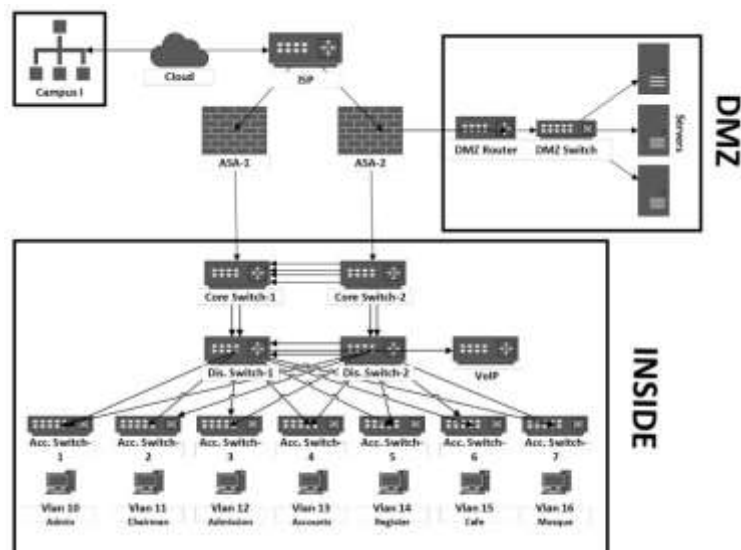
4.2 Campus network-II:

Fig: campus-II network

The above figure shows system's gateway is equipped with seven distinct layer-two switches, each of which represents a different division or virtual region that the system covers. These are the last-mile gadgets, which include PCs, printers, IP phones, smart devices, and other products. 'Campus II' is linked to 'Campus I' via the Internet service provider.

5. DEVICES AND DETAILS:

The need for network access is growing, and computer networks are becoming more complex systems. Due to the increasing demand, the network is now an essential part of the Internet, which has had tremendous success recently. This change is explained by the fact that Network Components in Cisco IOS Software have evolved from a passive to an active role, making them a vital component of every network. Network elements are now just as important as the network its own, even though network connection has always been a critical component for any business.

The Network Components are:

- Switch
- Router
- Endpoint
- Server
- Access points (AP)
- Wireless LAN Controller (WLC)
- Firewall

6. IP ADDRESSING:

One of the most important components of network configuration is IP (Internet Protocol). It entails giving every machine on a network a unique IP address so they may speak with one another.

There are two main versions of IP Addressing:

- Internet Protocol version 4 (IPv4): IPv4 addresses are 32-bit, or 4 bytes, long. IPv4 is still often utilized.
- Web Protocol version 6 is known as IPv6. 128-bit addresses, or six bytes, are used with IPv6. As IPv4 addresses run out, IPv6 is becoming more and more significant.

6.1 IPv4 (Internet Protocol version 4):

In my Thesis, I'm assigned a network address in IPv4. Here are some essential details regarding IPv4 addressing.

6.2 Campus IP Addressing:

| Category	Network & Subnet Mask	Valid Host Addresses	Default Gateway	Broadcast Address
WLAN HQ	10.10.0.0/16	10.10.0.1 to 10.10.255.254	10.10.0.1	10.10.255.254
BR	10.11.0.0/16	10.11.0.1 to 10.11.255.254	10.11.0.1	10.11.255.254
LAN HQ	172.16.0.0/16	172.16.0.1 to 172.16.255.254	172.16.0.1	172.16.255.255
BR	172.17.0.0/16	172.17.0.1 to 172.17.255.254	172.17.0.1	172.17.255.255
Management	192.168.10.0/24	192.168.10.1 to 192.168.10.254	192.168.10.1	192.168.10.255
DMZ	10.10.10.0/27	10.20.20.1 to 10.20.20.30	10.20.20.1	10.20.20.31

6.3 Between the Cloud, ISP, Firewall, Routers and Layer-3 Switch:

No	Network Address
Cloud Area	8.0.0.0/8
HQ-ISP- Internet	20.20.20.0/30
Branch-ISP- Internet	30.30.30.0/30
HQ-FWL- ISP	105.100.50.0/30
Branch-FWL- ISP	205.200.100.0/30
HQ-FWL to MLSW1	10.20.20.32/30
HQ-FWL to MLSW2	10.20.20.36/30
Branch-FWL to MLSW1	10.20.20.40/30
Branch-FWL to MLSW2	10.20.20.44/30

7. CONFIGURATION STEPS:

Step 1: Basic settings to all devices.
Step 2: SSH Configuration on the Routers and Switches.
Step 3: Create VLAN Database and Configure Access and Trunk Ports.
Step 4: Switchport Security to all Switches.
Step 5: Assign IP Address to Switch and Router.
Step 6: OSPF Configuration on Routers and Switches.
Step 7: DHCP Server Configuration.
Step 8: Firewall configurations.

8.NETWORK TOPOLOGY:
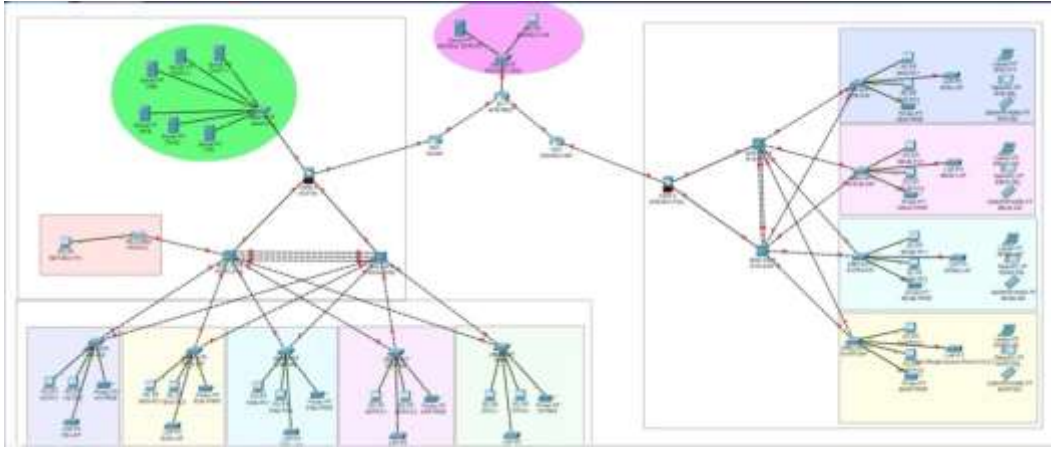
9. CONCLUSION:

　　　　Here, we've created the Advanced Campus topology using the bare minimum of specifications. Through this assignment, we studied how to utilize Cisco Packet Tracer to create a network layout and learn about the different connection types and link statuses. Additionally, we learned how to check for connectivity between two networks.

10. REFERENCES:

[1]. https://www.nwkings.com/what-is-a-cisco-packet-tracer
[2]. https://www.geeksforgeeks.org/
[3]. https://www.javatpoint.com/firewall
[4]. https://www.conceptdraw.com/
[5]. https://www.fortinet.com/resources/cyberglossary/what-is-ip-address
[6]. https://www.scribd.com/document/55877295
[7]. https://gurutechnetworks.otombenard.com
[8]. https://study-ccna.com/