International Journal of
Computational Learning & Intelligence
Vol. 02, Issue 04 (October) 2023

RESEARCH ARTICLE OPEN ACCESS

Campus Network Design and Implementation using Cisco Packet Tracer

Preetham N Varne . Priyanka J . Snehith Shetty V . Tejus A K . Naveen Chandra Gowda

School of Computer Science and Engineering
REVA University, Bengaluru, India.

DOI: **10.5281/zenodo.10254264**
Received: 11 October 2023 / Revised: 24 November 2023 / Accepted: 01 December 2023

Abstract – A thorough campus network design and implementation project using Cisco Packet Tracer is presented in this technical paper. The project's goal is to establish an effective and capable of being expanded network infrastructure for a made-up university that will accommodate the various connectivity requirements of its academic staff, administrative personnel, and students. To guarantee peak performance and dependability, the design integrates industry best practices in network architecture, security, and scalability. Cisco Packet Tracer is used to implement this project. Studying computer networking and technology gives one an understanding of several concepts, including topology design, IP address configuration, and how to send data in the form of packets within a single network. Virtual local area networks (VLANs) are also used to divide traffic generated by various departments.

Index Terms – Campus Network, Cisco Packet Tracer, Network Design, VLAN, DHCP, Quality of Service, Network Security, Wireless Integration, Management and Monitoring.

I. INTRODUCTION

A vital aspect of the present organizational and educational environment, the campus network facilitates communication, cooperation, and resource access within an established environment. It functions like a digital circulatory system, facilitating easy communication between different departments, structures, and people. In simple terms, the campus network functions as a foundation for essential services that are necessary for regular activities, like voice over internet protocol (VoIP) telephony, email communication, and collaborative tools. Beyond effortless connectivity, it makes resource sharing less difficult by allowing users to access databases, file servers, and printers, encouraging collaboration and efficiency quickly and easily in the workplace.

Simplifying the management of IT resources is another essential element: centralized network management. Administrators can effectively manage and monitor network devices, enact security regulations, and adhere to the general health of the network thanks to this centralized control. Any network environment must prioritize security and access control, and the campus network is no different. It makes it possible to set effective safety measures in place to protect sensitive data and guarantee the accuracy of information, including firewalls, intrusion detection systems, and access controls. The campus network customizes this evolution in the workplace by offering seamless connectivity for a range of devices, such as laptops, tablets, and smartphones. Serving as an entry point to the internet, it facilitates external connectivity for online service access, research, and staying up to time. Essentially, the campus network is more than just a group of networked gadgets; it serves as the foundation for contemporary educational institutions, fostering creativity, cooperation, and expansion. For an environment to promote productivity, security, and adaptability to the rapidly changing technological landscape, it must be properly designed and implemented.

Applications

- Networking Courses: Students studying networking courses may utilize a simulated environment through the Cisco Packet Tracer. Without that demand physical hardware, it enables them to design, configure, and troubleshoot intricate network configurations.
- IT Certification Preparation: Packet Tracer can be utilized by individuals to gain hands-on expertise with Cisco devices and protocols as a way for preparing for Cisco certifications, such as CCNA (Cisco Certified Network Associate) or CCNP (Cisco Certified Network Professional).
- New Infrastructure Deployment: Administrators can use Packet Tracer to simulate the recommended layout before physically implementing a new campus network. This facilitates the identification of possible problems, configuration testing, and validation that the network meets security and performance requirements.
- Upgrades and Changes: Without disrupting the live environment, Packet Tracer permits network administrators to test and validate alterations or upgrades to the present network infrastructure.

Where it is required

- University Campuses: A well-designed and implemented campus network is frequently necessary for large university campuses that have multiple buildings, departments, and thousands of users. This makes it easier for students to work together, communicate, and access educational resources.
- Schools and Colleges: To support the connectivity needs of students, faculty, and administrative staff, educational institutions throughout all levels can benefit from a campus network.

Why it is required.

Designing and implementing campus networks alongside Cisco Packet Tracer is essential for creating scalable, secure networks. It offers a simulated setting for configuration testing, troubleshooting, and providing outstanding performance. This tool is particularly useful for educational

institutions and organizations because it allows for useful learning and supplies a cost-effective way of recording, approving, and designing prototypes network infrastructures before they are deployed.

II. LITERATURE SURVEY

In their paper [1], "Enhancing the College Network," Jagdish K.P. and Pavan Kumar talked about how to create an advanced network through integrating IOT devices with traditional devices and replicating Cisco-PACKET Tracer version 7.0. This paper addresses IOT devices that include software sensors and actuators for wireless communication, in addition to virtual local area networks (VLANs). Since there are more devices than there are devices, we are replacing the router with layer 3 switches in order to avoid getting too many devices. which will lower the total number of switches and routers and, in consequently, the network's cost. Md. Matiullah wrapped an assortment of security concerns and common threats in wireless LANs in his paper [2], "Wireless LAN security Threats and Vulnerabilities." Information regarding attacks on confidentiality, integrity, availability, access control, and authentication is provided in this paper. Therefore, safeguarding the network from hackers and unauthorized access was the main goal. Nevertheless, using a WLAN increases the risk of hacking and other threats.

To mitigate this risk while enhancing the safety of networks, we may employ Network Address Translation (NAT), which hides the private IP address. Shivam Adke and Rutujia Bhawar's paper [3], "College Campus Network Design and Security," centered on network security to protect digital information by installing a local area network (LAN) and using a firewall to prevent unauthorized users out of the network. The use of hardware firewalls can complicate network design; to tackle such an issue, we can use procedures like Access Control Lists (ACLs), which are used to filter network traffic from appliances like routers and firewalls. The authors of the paper [4], "Design and Implementation of Secure Campus Network," Mohamed Nadir Bin Ali, Mohamed Emran Hossain, and Md. Masud Parvez, focused on the primary issues about the network architecture protection.

To maintain the network along with increase protection as a result of it, they also try to put into effect basic network design. They concentrated on LAN and WAN technology, and they utilized firewalls for security so that we could use extra protocols. In this paper, we investigated at different university designs for networks that use WLAN technology to guarantee that only authorized individuals have access to data. These layouts offer high security and low cost via the use of DHCP. By utilizing a variety of protocols, the network can be improved and, as a result, a longer network lifespan, and more secure encryption. Through analysis, we developed a solution that includes a better routing protocol (EIGRP), as well as several other protocols like NAT, ACL, HSRP, and PORT SECURITY.

III. PROPOSED WORK

The Objectives of the work are:

- Establish a scalable and resilient network architecture.
- Provide seamless connectivity for students, faculty, and staff.
- Implement security measures to safeguard network resources.
- Integrate technologies such as VLANs, DHCP, and QoS for optimized performance.
- Ensure ease of management and future scalability.

- **Network Topology:** The proposed network topology encompasses core, distribution, and access layers. Core switches interconnect various distribution switches, which in turn connect to access switches located in different buildings. This hierarchical design facilitates efficient traffic flow and reduces congestion.
- **VLAN Implementation:** To enhance network segmentation and resource optimization, Virtual LANs (VLANs) are deployed. VLANs are utilized to logically group devices based on their functions, such as separating administrative traffic from student traffic. This segmentation improves network performance and security.

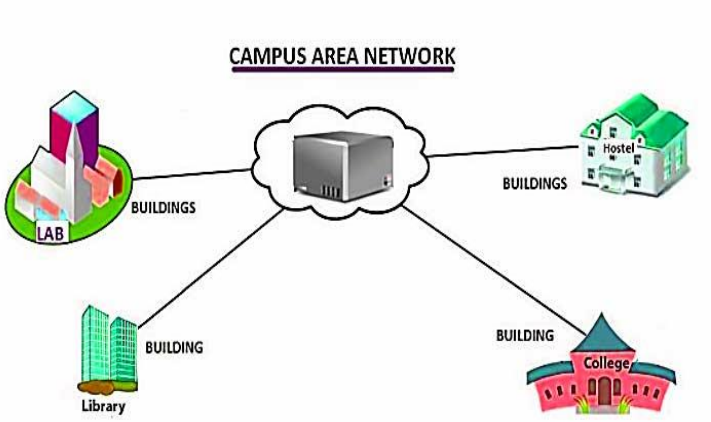

Fig. 1: Work Flow diagram

- **IP Addressing and DHCP:** A comprehensive IP addressing scheme is established to efficiently manage the allocation of IP addresses within the campus network. Dynamic Host Configuration Protocol (DHCP) is implemented to automate IP address assignment, reducing administrative overhead and ensuring efficient resource utilization.
- **Quality of Service (QoS):** To prioritize network traffic and optimize bandwidth utilization, Quality of Service (QoS) mechanisms are implemented. This is crucial for ensuring that real-time applications, such as video conferencing or online lectures, receive the necessary bandwidth without interruption.
- **Network Security:** Security measures are implemented to protect the campus network from unauthorized access and potential threats. This includes the deployment of firewalls, intrusion detection/prevention systems, and access control lists (ACLs) to control traffic flow and restrict unauthorized access to sensitive resources.
- **Wireless Network Integration:** With the increasing reliance on mobile devices, a wireless network is integrated into the campus infrastructure. This provides flexibility and mobility for users while maintaining the same level of security as the wired network.
- **Management and Monitoring:** The network is equipped with robust management and monitoring tools to ensure proactive identification and resolution of issues. Network administrators can use tools like SNMP (Simple Network Management Protocol) to monitor device performance and respond to potential problems swiftly.

IV. TOPOLOGY SETUP

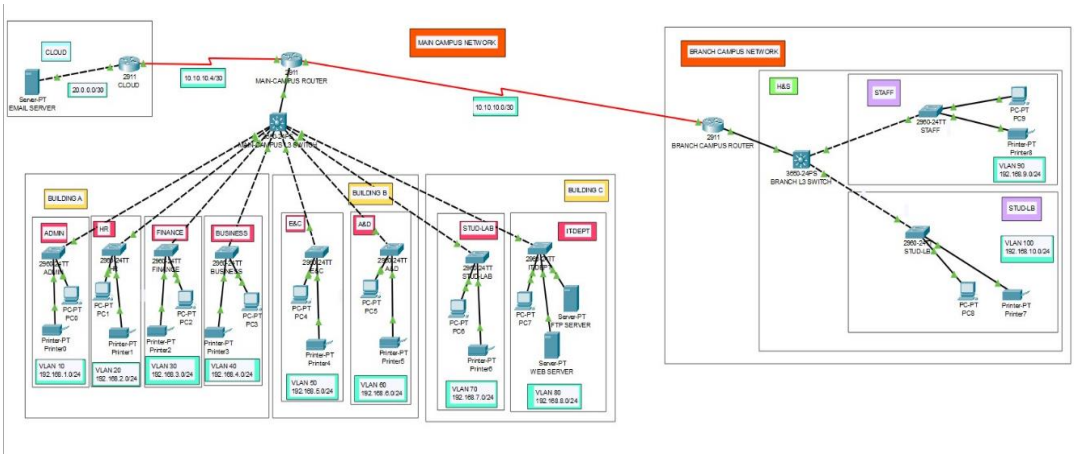

Fig. 2: Network Topology of Campus Network Design and Implementation

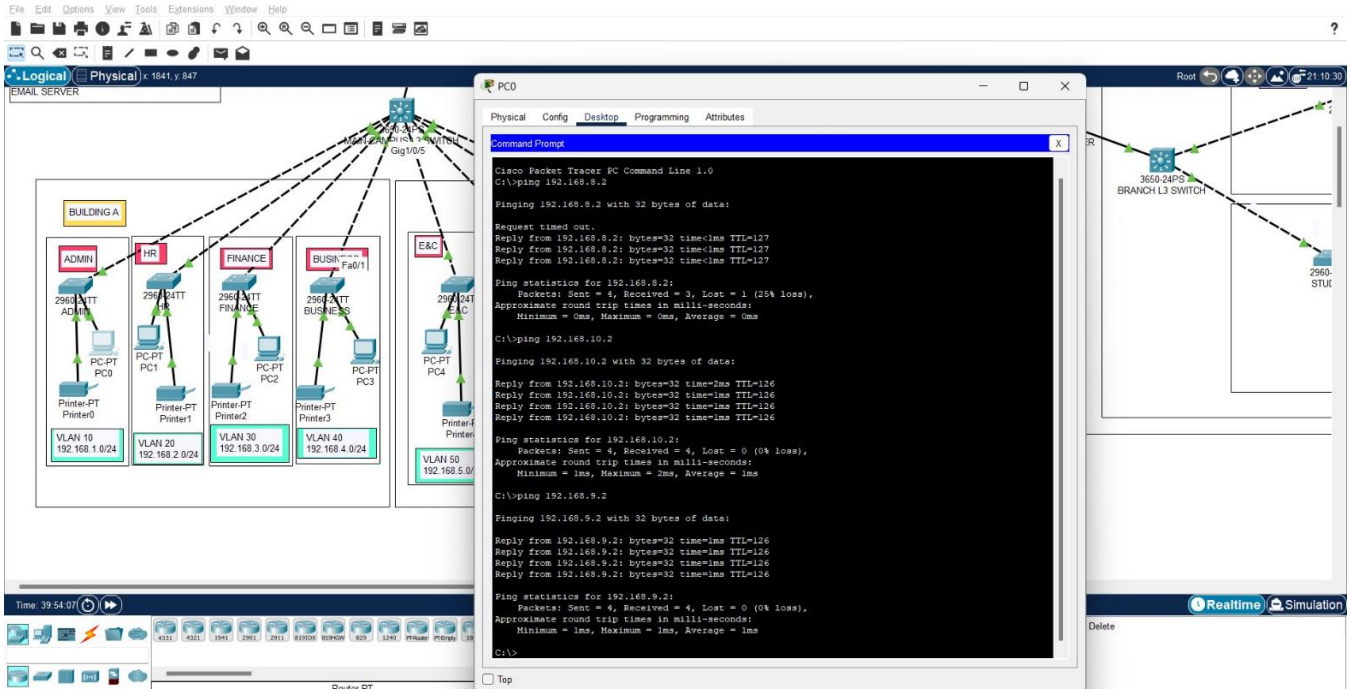

Fig. 3: Checking Network connectivity by pinging in Command Prompt

V. CONCLUSION

In conclusion, utilizing Cisco Packet Tracer in the design and implementation of campus networks is crucial for reaching the highest attainable network performance, scalability, and security. The educators and other professionals can experiment with various network topologies, configurations, and troubleshooting scenarios with this simulation tool, providing a dynamic environment for hands-on learning. It becomes an innovation catalyst through this process, permitting organizations to successfully prototype, validate, and document network infrastructures. The utility is important not only for training, testing, and improving network architectures, but also for corporate settings, educational institutions, and other industries. Cisco Packet Tracer plays an essential role in creating resilient and

flexible campus networks that are useful for real-world and educational applications, even as networking requirements change.

REFERENCES

1. Pawar, S., Ugale, V. D., Nirmal, A., Badgujar, P., & Borade, S. (2020). A Review On: Network Design for College Campus. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *7*(1), 129-130.
2. Waliullah, M., & Gan, D. (2014). Wireless LAN security threats & vulnerabilities. *International Journal of Advanced Computer Science and Applications*, *5*(1).
3. Adke, S., & Bhawar, R. (2018). College Campus Network Design and Security. *Department of Electronics & Telecommunication Engineering, Sandip Institute of Technology & Reserach Centre, Nashik, IJAREEIE-International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (online)*, 2278-8875.
4. Ahmed, S. T., Ashwini, S., Divya, C., Shetty, M., Anderi, P., & Singh, A. K. (2018). A hybrid and optimized resource scheduling technique using map reduce for larger instruction sets. *International Journal of Engineering & Technology*, *7*(2.33), 843-846.
5. Raja, D. K., Kumar, G. H., Basha, S. M., & Ahmed, S. T. (2022). Recommendations based on integrated matrix time decomposition and clustering optimization. *International Journal of Performability Engineering*, *18*(4), 298.
6. Ali, M. N. B., Hossain, M. E., & Parvez, M. M. (2015). Design and implementation of a secure campus network. *International Journal of Emerging Technology and Advanced Engineering*, *5*(7), 370-374.
7. Gaurkar, C., Thul, K., & Jaipurkar, P. COLLEGE CAMPUS NETWORK SCENARIO DESIGN & IMPLEMENTATION BY USING CISCO PACKET TRACER.
8. Basha, S. M., Poluru, R. K., & Ahmed, S. T. (2022, April). A Comprehensive Study on Learning Strategies of Optimization Algorithms and its Applications. In *2022 8th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
9. Thu, D. K. A. (2018). Simulation of Campus Area Network using routing protocols. *International Journal for Advance Research and Development*, *3*(9), 55-59.
10. Sita, K., Akram, P. S., Javvaji, K. H., & Attota, T. P. (2019). Design and implementation of Smart Campus Network. *EasyChair Preprint*.