University Campus Networking

*Pooja Shekhar  
Department of Computer Science  
California State University, Los Angeles, USA  
psheka2*[*@calstatela.edu*](mailto:dpatel112@calstatela.edu)

*Anisha Agarwal*

*Department of Computer Science*

*California State University, Los Angeles, USA*

*aagarw12*[*@calstatela.edu*](mailto:dpatel112@calstatela.edu)

*Abstract*—— In the contemporary digital era, universities are heavily dependent on robust and efficient campus networks to support their instructional, administrative, and research activities. The purpose of this abstract is to present a comprehensive design and optimization methodology for a university campus network to enhance connection, scalability, and security.

Keywords— Virtualization, VLAN, VPN, Cisco Packet Tracer, Distribution Switches.

Introduction (University Campus Network)

The design, deployment, and management of computer networks on a university or college campus are referred to as university campus networking. To support numerous academic, administrative, and research activities, it entails building a strong and dependable network infrastructure. Providing seamless and fast communication to students, teachers, staff, and administrators across various campus sites is the main goal of university campus networking. This makes it possible to communicate, work together, and utilize digital tools and services effectively. Supporting a variety of activities, such as online learning, research data transmission, administrative systems, multimedia streaming, and communication platforms, requires a well-designed campus network. It serves as the foundation for providing intranet services, internet connectivity, and other network-based applications.

Factors affecting university campus networking are:

* Connectivity
* Scalability
* Security
* Network Management
* Resource Optimization
* User Experience

# ***Problem Statement***

Universities’ instructional, administrative, and research operations must be supported by reliable and efficient campus networking. But a lot of challenges and issues need to be fixed in order to ensure the optimum network performance and user experience. The networking conundrum at colleges is best summarized by the following:

* Poor Network Connectivity
* Scalability Problems
* Vulnerabilities
* Complex Network Management
* Limited Support for Mobility

1. Inefficient Resource Utilization

# ***Abbreviations And Definitions***

VLAN-

* A VLAN (Virtual Local Area Network) is a network topology that allows logical networks to be created within a physical network infrastructure. VLANs enable network managers to group devices together based on their functional functions or locations, regardless of where they are physically located on the network.
* In a VLAN, devices in the same logical network can communicate with one another as if they were physically connected to the same switch, even if they are physically linked to different switches. This is accomplished by tagging packets with a VLAN ID, allowing switches to determine which devices belong to which VLAN.

RIP

* RIP is a protocol that allows routers in a network to communicate routing information and find the most efficient paths for data to go from one network to another.
* Because RIP version 1 is a classful protocol, it only supports the original IP addressing scheme and its default subnet mask.
* RIP version 2 is a classless protocol that supports variable-length subnet masks (VLSM) and makes better use of IP address space.

Static Routing

* A routing protocol used in computer networks in which network administrators manually establish the routes on each network device rather than depending on dynamic routing protocols to find the optimum path for data to take.
* In the routing table of each router in the network, the network administrator specifies the next hop router for each network destination. This information is then used by the router to route packets to the correct destination.

DHCP SERVER

* DHCP (Dynamic Host Configuration Protocol) is a network management protocol that automates the assigning of IP addresses and other network configuration parameters to network devices. A server distributes IP addresses to devices as they connect to the network via DHCP, removing the need for manual IP address configuration.

## When a device connects to a DHCP-enabled network, it sends a request to a DHCP server for network configuration information. The DHCP server then provides an available IP address from a pool of addresses that it administers to the device. Other network setup information provided by the DHCP server to the device includes the subnet mask, default gateway, and DNS server addresses.

# ***HISTORY***

The history of university campus networking begun in the late 1960s and early 1970s when early versions of computer networks were developed to facilitate information sharing and collaboration among universities and research institutions. The advent of ARPANET and the establishment of NSFNET in the 1980s played pivotal roles in the growth of campus networking, connecting academic institutions and expanding connectivity. The adoption of LAN technologies and the emergence of the internet in the 1990s brought faster data transfer speeds and global connectivity to universities. The introduction of wireless networking technologies in the late 1990s further enhanced mobility and flexibility within campus environments. Recent advancements include high-speed fiber-optic networks, Wi-Fi 6, virtualization, and cloud-based services, which have transformed campus networking to meet the increasing demand for bandwidth, multimedia applications, and security. Today, university campus networking encompasses various technologies and services, enabling a digitally connected and collaborative academic environment.

# ***Proposed Idea and Solutions***

In this proposal, we offer a fresh concept and approach to develop and deploy a cutting-edge campus network for universities. The goal is to meet the academic community's changing needs, improve connectivity and collaboration, and provide strong security measures. The following are the list of advanced technologies used for building cutting-edge infrastructure.

* High-Speed and Scalable Connectivity
* Robust Wireless Network
* Network Segmentation and Virtualization
* Advanced Security Measures
* Network Management and Monitoring

There are various benefits and impact of the proposed idea such as:

* Enhanced Connectivity and Collaboration
* Improved Security
* Scalability and Future-Readiness
* Efficient Resource Utilization
* Streamlined Network Management

The suggested concept and solution for a next-generation university campus network include increased connectivity, collaboration, and security capabilities. By deploying this solution, the institution will be able to build a technologically sophisticated environment that supports academic excellence, stimulates creativity, and satisfies the changing demands of students, teachers, and staff.

# ***Simulation Tools***

The simulation tool used for University Campus Network is Cisco Packet Tracer.

What is Cisco Packet Tracer?

* Cisco Packet Tracer is a network engineering simulation tool developed by Cisco Systems for designing, configuring, and troubleshooting network infrastructures. It enables users to establish virtual networks using various network equipment such as routers, switches, hubs, and PCs, as well as simulate communication between these devices.
* Packet Tracer has an easy-to-use interface for constructing and configuring networks, and it supports a variety of protocols like TCP/IP, DHCP, DNS, OSPF, EIGRP, VLANs, and others. It also enables users to imitate network device behavior, test connectivity, and troubleshoot network issues.

# ***Simulations***

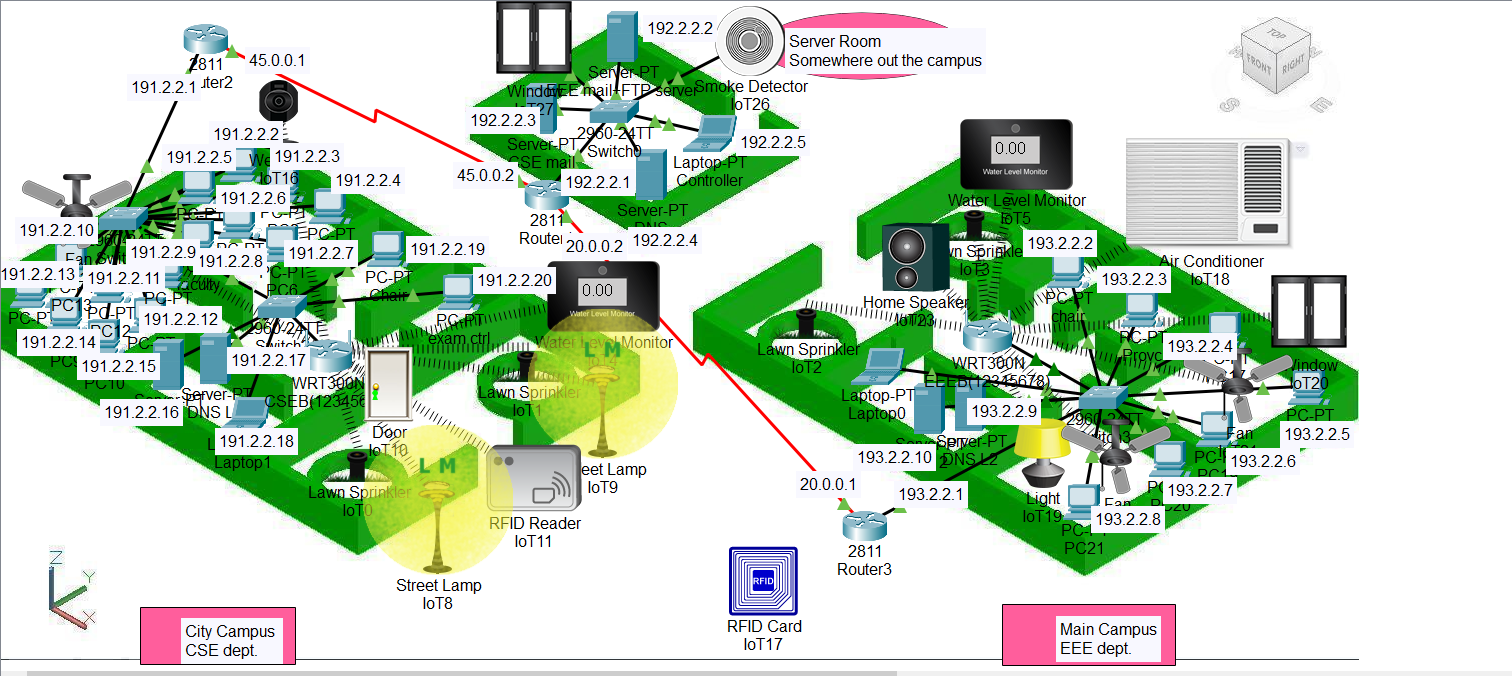
Diagram

Description automatically generated

Figure 1simulation1

Diagram

Description automatically generated



# ***Commands***

Graphical user interface, text, application

Description automatically generated

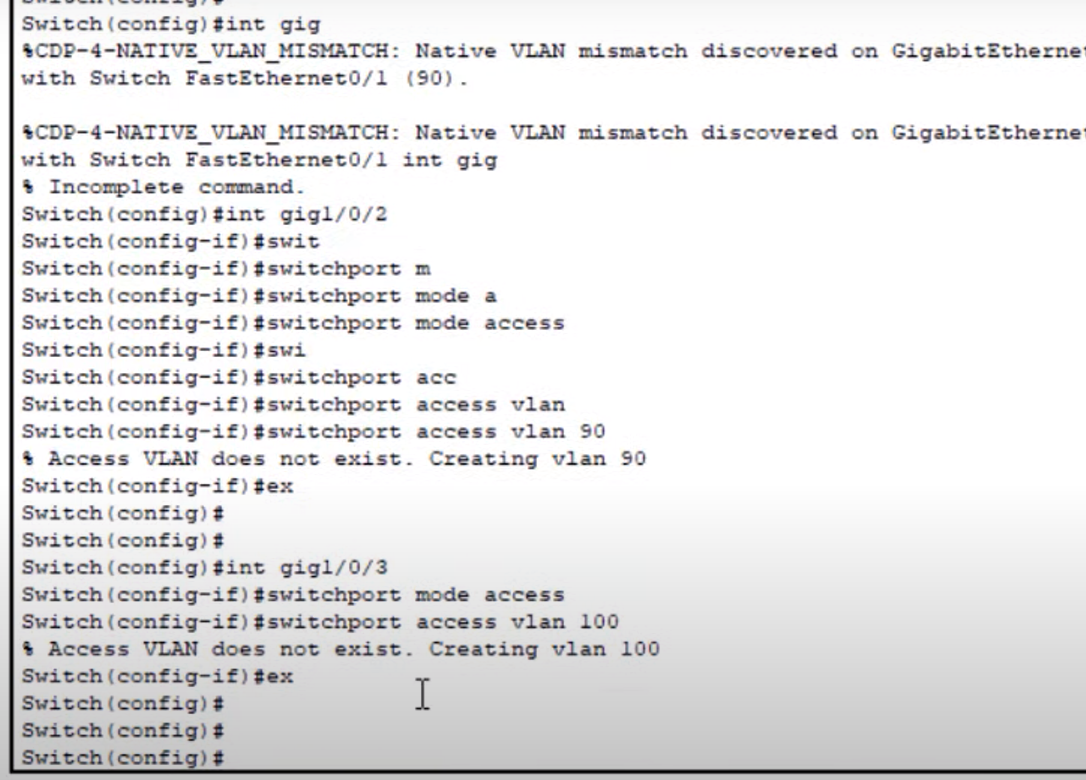
Graphical user interface, text

Description automatically generated



Text

Description automatically generated



Text

Description automatically generated

# ***Steps for Implementing***

Step 1: Design the network topology:

In this phase, we must establish the number and type of devices to be used, as well as how they will be connected.

Step 2: Adding Devices to the Topology:

After designing, we must add devices like as switches, routers, and wireless access points.

Step 3: Configure Devices:

Once the devices have been added, they must be configured using the device configuration interface. This includes characteristics such as IP addresses, subnet masks, routing protocols, and security settings.

Step 4: Test the network:

Once the network has been configured, we must test the traffic flow and analyze the network performance. It is possible to use the built-in tool, Packet Tracer Activity Wizard, or the simulation mode to accomplish this.

Step 5- Network optimization-

Based on the findings of network testing, adjustments can be made to optimize network configuration. This could include changing device settings, altering network topologies, or regulating traffic flow.

# ***Comparision Between The Network Topologies***

* In the first image or example, we can see that all the devices are linked to the main router, which is linked to the cloud. As a result, we can easily ping devices on different campuses. And if the data is lost for any reason, we can quickly recover it.
* In the second example, we see that there are many routers/ access points which are not required. Due to which the efficiency of the topology decreases.
* In the third example, we have simulated the network topology in 3D view.

# ***Conclusion***

We can conclude by saying,

* For the creation of an advanced academic environment, a well-designed and optimized university campus network is essential. As, it enables connectivity, collaboration, and security, thereby supporting academic institutions' missions of providing quality education, fostering research, and preparing students for success in a digitally linked society.
* A well-designed university campus network. The network architecture should support high-speed and scalable connection, wireless mobility technologies, secure data transmission, and effective resource use.
* A secure network architecture safeguards sensitive information, prevents illegal access, and mitigates cyber hazards. Network segmentation, virtualization, and enhanced security measures assure digital asset integrity and confidentiality, promoting a safe and trusted environment for academic activity.

# ***References***

1. Virtual local area network technology and applications by [V. Rajaravivarma](https://ieeexplore.ieee.org/author/37298123200) (<https://ieeexplore.ieee.org/document/581577>)
2. Designing a hierarchical DHCP server's model to automatically provide dedicated IP address anywhere in the world with mobility by [Asjad Amin](https://ieeexplore.ieee.org/author/38017376800); [Haseeb Ahmed](https://ieeexplore.ieee.org/author/38238919100) (<https://ieeexplore.ieee.org/document/6148452>)
3. Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP by [Siti Ummi Masruroh](https://ieeexplore.ieee.org/author/37085495098); [Andrew Fiade](https://ieeexplore.ieee.org/author/37945371200)(<https://ieeexplore.ieee.org/document/8319134>)
4. YouTube reference link [(479) Full Cisco Packet Tracer 2021 Tutorial for Beginners - YouTube](https://www.youtube.com/playlist?list=PLVFyjfF2Drdt9hXs37KTPTIqtNVCXFfOG)
5. [Testing Methods for test and factor analysis of system simulation results | IEEE Conference Publication | IEEE Xplore](https://ieeexplore.ieee.org/document/5777785)
6. [Influence and Optimization of Packet Loss on the Internet-Based Geographically Distributed Test Platform for Fuel Cell Electric Vehicle Powertrain Systems | IEEE Journals & Magazine | IEEE Xplore](https://ieeexplore.ieee.org/document/8963939)