Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2024), B.Sc. in CSE (Eve)

Smart University Network Design Using Cisco Packet Tracer

Course Title: Data communication Lab
Course Code: CSE 104
Section: 222 EA/EB

Students Details

Name	ID
Adnan al-emran ontor	222015033

Course Teacher's Name: Sudip Chandra Ghoshal
Designation::Lecturer

Lab Project Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Introduction

1.1 Overview

Now a days every University have a network to communicate internally and externally. But there are few where there is a smart system. Where the work can be done more efficiently and also in smart way. For example, to take attendance of students a teacher needs at least 20 minutes. If the student number is large then i know how much it takes. But what if i install an IOT device to each class room. This IOT will able to read students ID card or face or any kind of unique identity data and upload the data to a server where a database will maintain the data. Like form 10:00 am to 11:30 am is the networking class of 222EA batch and course teacher is Sudip Chandra Ghoshal then the IOT device will send the data to server and the server will count the attendance for this class. It will save a lot of time for a large number of students. From this concept i thought how to make a network like this. i didn't implement this concept in this project but this was a great motivation. Not attendance is the only case. Smart devices are changing our life. To communicate between them networks must be developed. Maybe in near future IOT devices and other network component will be more affordable to users. Then i will able to implement this types of networks anywhere i want.

1.2 Design Goals/Objectives

The primary goals and objectives of this project are as follows:

- **Efficient Network Design:** Develop a reliable and scalable network architecture that interconnects multiple campuses with seamless communication.
- **IoT Integration:** Incorporate IoT devices to automate processes such as attendance tracking, resource management, and environmental control.
- **Centralized Control:** Establish centralized servers for mail, FTP, DNS, and IoT management to ensure efficient resource utilization.
- **Security and Accessibility:** Ensure that the network is secure while maintaining high accessibility for authorized personnel.

- **Smart Resource Management:** Enable real-time monitoring and control of devices like air conditioners, lights, and sprinklers for energy efficiency and convenience.
- **Remote Connectivity:** Facilitate remote access to IoT devices and network resources for authorized users.

These goals are aligned to showcase a practical and innovative network infrastructure that can transform a conventional university into a smart, technology-driven institution.

1.3 Application

This project has significant real-world applications, including but not limited to:

1.3.1 Smart Campus Management

By integrating IoT devices, the proposed network design facilitates the efficient management of resources like electricity, air conditioning, and lighting, ensuring an eco-friendly and cost-effective operation.

1.3.2 Enhanced Educational Experience

Students and staff can benefit from a technology-rich environment, where virtual access to classrooms and resources is available. Features like automated attendance and virtual exam monitoring enhance productivity and reduce manual work.

1.3.3 Remote Monitoring and Control

With IoT-enabled devices connected to the internet, critical functions such as security monitoring, environmental control, and administrative management can be accessed and managed remotely.

1.3.4 Disaster Management and Safety

Smoke detectors and security cameras integrated into the network provide real-time alerts for emergencies, enhancing campus safety.

1.3.5 Future Scalability

The modular nature of the network allows for the addition of new buildings, devices, and features as the campus grows, ensuring long-term adaptability.

Chapter 2

Design/Development/Implementation of the Project

2.1 Introduction

In this chapter, i will discuss the design, development, and implementation of the smart university network project. The primary goal of this project is to design a network infrastructure that integrates IoT devices to create a smart campus environment. The network architecture and its components were simulated using Cisco Packet Tracer, which is a powerful network simulation tool that allows the creation and simulation of a variety of networking topologies.

The project involves setting up a network that connects various university resources, such as classrooms, administrative offices, and IoT devices like smart sensors and attendance tracking systems. The simulation models the behavior of these devices and demonstrates the functionalities of the network, such as automated attendance, resource management, and centralized control.

2.2 Project Details

The network design for the smart university system was developed in stages, beginning with the physical topology and network components, followed by the logical configuration and IoT integration. This section outlines the various aspects of the project, including the hardware, software, and network configurations used in the simulation.

2.2.1 Network Architecture

The network architecture is designed to provide scalability, reliability, and security across multiple campuses. It consists of a central server that handles various services such as email, FTP, DNS, and IoT management. Additionally, several IoT devices, such as smart attendance systems and environmental sensors, are connected to the network to automate university operations.

The network utilizes Cisco routers, switches, and wireless access points to ensure robust communication across all network segments. The network is divided into different subnets for security and management purposes.

2.2.2 Hardware Components

The simulation in Cisco Packet Tracer uses several key components to build the network, including:

- **Routers:** To route traffic between different network segments and connect the university's internal network to the internet.
- **Switches:** To connect multiple devices within the same network and ensure efficient data transmission.
- **Access Points:** To provide wireless connectivity for IoT devices and other mobile devices on campus.
- **IoT Devices:** Sensors, cameras, smart attendance systems, and environmental control devices connected to the network.
- **Servers:** To host services like DNS, FTP, mail, and manage IoT data.

2.2.3 Software Components

The project utilizes Cisco Packet Tracer as the primary simulation tool to model the network and simulate device behavior. In addition, several scripts were created within the Packet Tracer environment to simulate IoT functionality, such as automated attendance tracking.

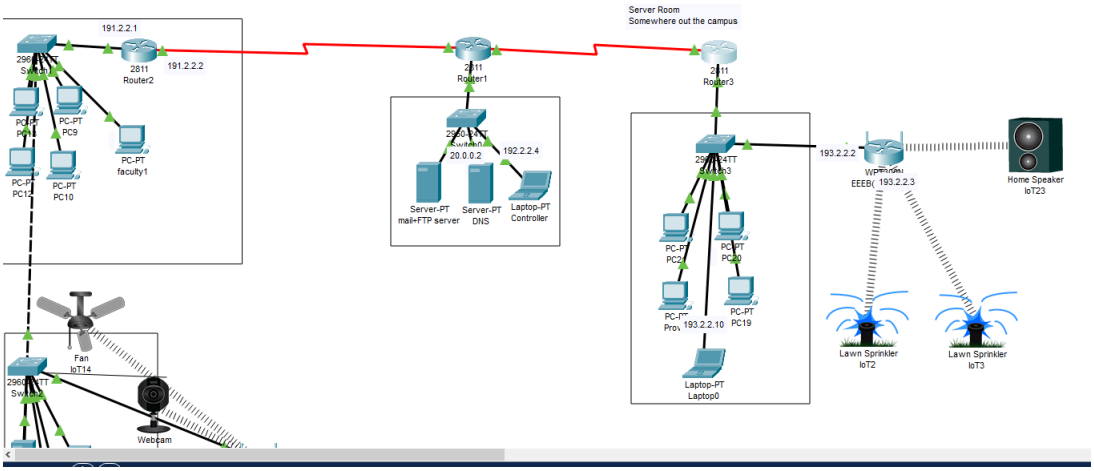

Figure 2.1: Network Topology of the Smart University Network

The network topology consists of routers connected to switches, with IoT devices and computers on each campus segment. The simulation also models the behavior of the IoT devices, such as automatic attendance tracking when students enter the classroom.

2.3 Implementation

The implementation phase of the project involves configuring each network component to work together seamlessly. Below are the detailed steps involved in the implementation of the smart university network using Cisco Packet Tracer.

2.3.1 Step 1: Network Setup

The first step is to set up the physical and logical network. This includes placing routers, switches, and access points in their respective positions, and connecting them with the necessary cables (Ethernet or fiber optic cables). The logical network configuration involves assigning IP addresses, subnet masks, and default gateways to the network devices.

2.3.2 Step 2: Server Configuration

The next step is to configure the servers that will manage the various services, such as DNS, FTP, email, and IoT management. Each server is configured with the appropriate services, and IP addressing is set up to ensure that all devices can communicate with the servers.

2.3.3 Step 3: IoT Device Integration

IoT devices, such as smart sensors and attendance systems, are integrated into the network. Each device is connected to the network, and their communication protocols are configured to send data to the central server. For example, the smart attendance system communicates with the server to record student attendance based on their ID cards or facial recognition.

2.3.4 Step 4: Network Security

Security measures are implemented to protect the network from unauthorized access. This includes setting up access control lists (ACLs), enabling encryption for sensitive data, and configuring firewalls to block unwanted traffic. The security of IoT devices is also a critical consideration, ensuring that the devices are protected from external threats.

2.3.5 Step 5: Testing and Simulation

After all components are configured, the network is tested and simulated in Cisco Packet Tracer. Various test scenarios are executed to ensure that the network performs as expected. These tests include checking the connectivity between devices, verifying that the IoT devices are functioning correctly, and simulating network traffic to ensure optimal performance.

The Workflow

The workflow of the smart university network begins when a student enters a classroom. The smart attendance system scans the student's ID card and sends the data to the central server. The server then records the attendance and updates the database. Simultaneously, environmental sensors monitor the classroom temperature, humidity, and lighting, and adjust these parameters based on preset conditions. These processes occur automatically, requiring minimal human intervention and improving operational efficiency.

2.4 Conclusion

The design, development, and implementation of the smart university network have demonstrated the potential of integrating IoT technologies with traditional networking. The simulation provided valuable insights into the feasibility of building a smart campus network that automates several functions such as attendance tracking, resource management, and security monitoring. The project also highlighted the importance of network security and the need for scalable infrastructure as IoT devices continue to proliferate.

Chapter 3

Conclusion

3.1 Discussion

The project successfully designed and simulated a smart university network that integrates IoT technologies with traditional networking. The system demonstrated enhanced operational efficiency through features like automated attendance and centralized resource management. The simulation environment validated the feasibility and performance of the proposed design.

3.2 Limitations

While the project achieved its primary objectives, several limitations were identified:

- The simulation environment did not include real-world factors such as hardware constraints or unpredictable network loads.
- Advanced IoT functionalities, like facial recognition, were not implemented due to scope limitations.
- Security measures were limited to basic ACLs and did not include advanced intrusion detection systems.

3.3 Scope of Future Work

Future iterations of this project could focus on:

- Real-world implementation of the network design using actual hardware.
- Incorporation of advanced IoT technologies and artificial intelligence for predictive analytics.
- Enhanced security measures, including firewalls, VPNs, and intrusion detection systems.

- Development of mobile applications for real-time monitoring and control.

References

[1] Andrew S. Tanenbaum, *Computer Networks*, 5th Edition, Pearson Education, 2013.

[2] Cisco Systems, *Cisco Packet Tracer Student Guide*, Cisco Networking Academy, 2020.

[3] James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach*, 7th Edition, Pearson, 2016.

[4] Ovidiu Vermesan and Peter Friess, *Internet of Things: From Research and Innovation to Market Deployment*, River Publishers, 2014.

[5] Priscilla Oppenheimer, *Top-Down Network Design*, 3rd Edition, Cisco Press, 2010.

[6] David MacKay, *Sustainable Energy Without the Hot Air*, UIT Cambridge Ltd., 2009.