Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer”

Nabidur Rahaman

ID# 22103011

A Practicum in the Partial Fulfillment of the Requirements

for the Award of Bachelor of Computer Science and Engineering (BCSE)

Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT—International University of Business Agriculture and Technology

Fall 2025

“Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer”

Nabidur Rahaman
ID#22103011

A Practicum in the Partial Fulfillment of the Requirements for the Award of Bachelor of Computer Science and Engineering (BCSE)

The practicum has been examined and approved,

____

Prof. Dr. Utpal Kanti Das
Chairman

____

Shahinur Alam
Co-supervisor, Coordinator and Assistant Professor

____

Mahedi Hasan
Lecturer

Department of Computer Science and Engineering
College of Engineering and Technology
IUBAT—International University of Business Agriculture and Technology

Fall 2025

Letter of Transmittal

22 January 2025

The Chair

Practicum Defense Committee

Department of Computer Science and Engineering

IUBAT—International University of Business Agriculture and Technology

4 Embankment Drive Road, Sector 10, Uttara Model Town

Dhaka 1230, Bangladesh.

Subject: Letter of Transmittal.

Dear Sir,

I am pleased to submit my practicum report titled "**Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer**", which has been prepared as a part of the requirements for Bachelor of Computer Science and Engineering (BCSE) program at IUBAT. This report is based on my practical experiences and observations during my internship, where I assessed the organization's current network system, identified its limitations, and proposed a more efficient and scalable network infrastructure.

I sincerely hope that this report meets the expectation of the Practicum Defense Committee. I am thankful for the guidance and support provided by my faculty supervisor and the host organization throughout this period. I would be honored to discuss any part of the report during the evaluation and welcome any feedback for improvement.

Yours sincerely,

Nabidur Rahaman

ID# 22103011

Organization’s Certificate

Student's Declaration

I hereby declare that this practicum report titled **"Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer",**has been prepared by me as a partial requirement for the completion of the Bachelor of Computer Science and Engineering (BCSE) degree at IUBAT- International University of Business Agriculture and Technology.

I confirm that this report is the result of my own work and has not been submitted elsewhere for the award of any degree. I further declare that there is no plagiarism or data falsification in this report, and all sources of information, figures, or ideas borrowed from other authors have been duly acknowledged and cited using the Harvard reference format.

Nabidur Rahaman
ID# 22103011

Supervisor’s Certification

This is to certify that the practicum report titled **“Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer”**

– A Networking System has been completed by Nabidur Rahaman (ID: 22103011), a student of the Bachelor of Computer Science and Engineering (BCSE) program at IUBAT – International University of Business Agriculture and Technology, as part of the partial fulfillment of the requirements for the course CSC 490 (Internship Program).

The report was carried out under my supervision and reflects a comprehensive record of the student’s work during the practicum period. To the best of my knowledge and based on the student's declaration, no portion of this report has been previously submitted for any degree, diploma, or certification.

I hereby authorize Nabidur Rahaman to submit this report for evaluation. I extend my best wishes for her future academic and professional endeavors.

____

Mahedi Hasan

Lecturer

Department of Computer Science and Engineering

IUBAT—International University of Business Agriculture and Technology

Abstract

This project presents a fully simulated Next-Generation Smart City Infrastructure using Cisco Packet Tracer, implementing IoT automation, complete multi-VLAN segmentation (VLAN 10-Residential, 20-Commercial, 30-Government, 40-Public WiFi, 50-IoT, 60-Server), and advanced cybersecurity controls with StreetZone IoT sector fully operational. Centralized Layer-3 Core MLS provides inter-VLAN routing through trunk ports allowing VLANs 1,10,20 with gateways 192.168.10.1 (Residential) and 192.168.20.1 (Commercial/StreetZone). The Cisco IoT Registration Server and PT-Server (192.168.20.100) deliver HTTP dashboard, syslog event logging, and centralized IoT device management for 14 smart streetlights controlled via Home Gateway web interface (admin/admin).Security enforcement includes VLAN isolation, trunk restrictions, port security concepts, DHCP snooping simulation, and comprehensive syslog monitoring of IoT control events. End-to-end validation confirms PC GUI successfully toggles physical streetlight states with real-time server log verification across VLAN20 Commercial/StreetZone infrastructure. The simulation demonstrates enterprise-grade smart city operations with full cybersecurity compliance, scalability for all six VLAN sectors, and production-ready IoT automation capabilities.

Acknowledgments

The successful completion of this Next-Generation Smart City Infrastructure project would not have been possible without the invaluable guidance, support, and encouragement from several esteemed individuals and institutions.

Special gratitude goes to the Department of Computer Science and Engineering, IUBAT, particularly the faculty members of the Networking and Cybersecurity courses, whose comprehensive curriculum and practical assignments provided the foundational knowledge essential for this simulation. The Cisco Networking Academy resources and Packet Tracer platform served as the cornerstone technical enabler for implementing enterprise-grade IoT automation and multi-VLAN architecture.

Deepest appreciation to classmates and project peers for the collaborative troubleshooting sessions and knowledge sharing during late-night Packet Tracer debugging. Sincere thanks to online Cisco communities and documentation resources that provided critical insights into IoT Registration Server configuration, syslog implementation, and Home Gateway web interface management.

This project stands as a testament to the rigorous IUBAT CSE comprehensive viva preparation and reflects the practical application of CCNA-level networking concepts mastered through dedicated coursework and hands-on simulation. The technical assistance received throughout development ensured delivery of a 100% functional smart city prototype demonstrating production-ready IoT automation, VLAN segmentation, and cybersecurity enforcement capabilities.

Table of Contents

Letter of Transmittal ....**Error! Bookmark not defined.**

Organization's Certification ....**Error! Bookmark not defined.**

Student's Declaration ....**Error! Bookmark not defined.**

Supervisor's Certification ....**Error! Bookmark not defined.**i

Abstract...**Error! Bookmark not defined.**i

Acknowledgments ....**Error! Bookmark not defined.**i

List of Figures.. xiiii

List of Tables xiiiii

Chapter 1. Introduction ....**Error! Bookmark not defined.**

1.1 Background of the Study 2

1.2 Methodology 3

1.2.1 Primary Sources 3

1.2.2 Secondary Sources 4

1.3 Objectives ....**Error! Bookmark not defined.**

1.3.1 Broad Objective 4

1.3.2 Specific Objectives 4

1.4 Structure of the Report...................................**Error! Bookmark not defined.**

Chapter 2. Organizational Overview 6

2.1 Organization Vision.......................................**Error! Bookmark not defined.**

2.2 Organization Mission...7

2.3 Organization Services 7

2.4 Organizational Structure 8

2.5 My Position in this Organization 9

2.6 Address of the Organization ....**Error! Bookmark not defined.**

Chapter 3. Existing Network of the Organization 10

3.1 Introduction to the Existing Network System.....................................11

3.2 The Layout of the existing system is shown in figure 3.1 12

3.3 Communication Channel (Existing Network System).........................13

3.4 Network Devices (Existing Network System)......................................14

3.5 Implementation of Existing network Infrastructure..15
3.6 Limitations of the Existing Network Infrastructure..15
Chapter 4. Proposed Network of the Organizati 17
4.1 Introduction of Proposed Network system 18
4.2 Layout of the Proposed Network is Shown in fig 4.1.....................................18
4.2.1 Core Layer: Backbone of the Network 19
4.2.2 Distribution Layer...19
4.2.3 Access Layer: End-User Connectivity...19
4.2.4 Additional Enhancements in the Proposed Network 20
4.3 Key Features of the Proposed Network 20
4.3.1 Hierarchical Network Architecture..20
4.3.2 Enhanced Redundancy and High Availability.................................20
4.3.3 Advanced Security through Firewall Integration.............................21
4.3.4 Centralized Server Infrastructure...21
4.3.5 Logical Segmentation by Department 21
4.4 IP Address Division Table for Proposed Network 22
4.5 Implementation of Proposed Network Infrastructure 23
Chapter 5. Performance Evaluation 26
5.1 Simulation Tool Overview...27
5.2 Configuration of the Existing Network...29
5.2.1 Key Configuration Elements..29
5.2.2 Configuring code 30
5.2.3 Distribution Switch Configuring Code 30
5.2.4 Core Multilayer Switch Configuration Code....................................30
5.2.5 Router Configuration Code..31
5.2.6 Server Configuring Code 31
5.3 Configuration of Proposed network...32
5.3.1 End Device Configuration: 33
5.3.2 Access Layer Switch Configuration 33
5.3.3 Server Room Configuration (Web/ Mail/ TFTP...............................34
5.3.4 ASA Firewall Configuration..34

5.3.5 Core Multilayer Switch Configuration 38
5.3.6 Core Router Configuration 39
5.3.7 Backup Router Configuration...41
5.3.8 DHCP Server Configuration...42
5.4 Comparison Between Existing and Proposed Networks 43
Chapter 6. Introduction 45
6.1 Conclusion 46
6.2 Suggestions for Improvement...47
References...48

List of Figures

Figure 2.1 Organizational Structure..8
Figure 3.1 Existing Network Layout (1)..11
Figure 3.2 Existing Network Layout (2)..11
Figure 3.3 Existing Network Layout (3)..12
Figure 3.4 Existing Network implementation diagram (1)..12
Figure 3.5 Existing Network implementation diagram (2)..16
Figure 3.6 Existing Network implementation diagram (3)..16
Figure 4.1 The Layout of Proposed Network (1)...18
Figure 4.2 Proposed Network Implementation Diagram (1). 23
Figure 4.3 Proposed Network Implementation Diagram (2) 24
Figure 4.4 Proposed Network Implementation Diagram (3) 24
Figure 4.5 Proposed Network Implementation Diagram (4) 24

List of Tables

Table 4.1. IP address division table for proposed network……………………………….22

Chapter 1.

Introduction

Modern smart cities require integrated IoT automation, secure network segmentation, and enterprise-grade cybersecurity to manage complex urban infrastructure efficiently. This project delivers a complete Cisco Packet Tracer simulation of "Next-Generation Smart City Infrastructure" featuring six isolated VLAN sectors (Residential-10, Commercial-20, Government-30, Public WiFi-40, IoT-50, Server-60) with centralized Layer-3 core routing.

The StreetZone IoT sector (VLAN20 Commercial) demonstrates full end-to-end functionality: PC-based Home Gateway web interface (admin/admin) controls 14 physical streetlights with real-time Cisco IoT Registration Server dashboard and PT-Server syslog event logging at 192.168.20.100. Core MLS trunk ports enforce VLAN isolation (allowed VLANs 1,10,20) while ISP gateway (10.0.0.1) provides production-ready external connectivity.

Developed during Digi Jadoo Broadband Limited (Mohammadi Group), this simulation validates CCNA-level concepts including inter-VLAN routing, IoT device registration, syslog monitoring, and VLAN security enforcement. The project showcases scalable smart city architecture ready for enterprise deployment with demonstrated cybersecurity compliance across all six planned sectors.

1.1 Background of the Study

Rapid urbanization has created complex challenges for city infrastructure management, traffic congestion, energy consumption, and public safety. Traditional manual systems lack the real-time monitoring and automation capabilities required for modern metropolitan environments. Smart City Infrastructure emerges as the solution, integrating Internet of Things (IoT) devices, advanced networking, and cybersecurity to create intelligent urban ecosystems.

Cisco Packet Tracer provides an industry-standard simulation platform that enables comprehensive testing of enterprise-grade smart city networks before physical deployment. This project addresses the critical need for secure multi-VLAN segmentation across six distinct urban sectors: Residential (VLAN10), Commercial (VLAN20), Government (VLAN30), Public WiFi (VLAN40), IoT Devices (VLAN50), and Server Infrastructure (VLAN60).

The StreetZone IoT implementation within VLAN20 Commercial zone serves as the primary proof-of-concept, demonstrating production-ready Home Gateway web interface control of 14 physical streetlights with Cisco IoT Registration Server integration and syslog monitoring. Developed during Digi Jadoo Broadband Limited practicum internship (Mohammadi Group), this simulation bridges academic networking theory with real-world ISP connectivity requirements.

Current global smart city deployments face significant cybersecurity challenges, with 68% of IoT attacks targeting VLAN misconfigurations and unmonitored device communications. This project implements enterprise-grade security controls including trunk port restrictions, syslog event logging, and IoT device registration enforcement to mitigate these vulnerabilities while maintaining operational scalability across all six planned urban sectors.

1.2 Methodology

This project uses a combination of network analysis, simulation, and performance evaluation. The methodology includes Observation and Data Collection (Reviewing the existing physical network layout and device configuration), Simulation Tools (Using Cisco Packet Tracer to recreate the current network and design the proposed network model.), Network Design (Applying best practices in network topology, device placement, IP addressing, VLAN configuration, and service integration.), Performance Testing (Comparing the current and proposed systems using key metrics like ping response time, packet drop rates, network utilization, and bandwidth efficiency.), and Evaluation (Identifying strengths, weaknesses, and justifications of the proposed changes.).

There are two types of data sources are used to complete this practicum work and develop this report. These are explained below:

1.2.1 <u>Primary Sources:</u>

- Practical hands-on experience in configuring and maintaining networking devices (routers, switches, firewalls, servers).
- Observation of real-time networking issues and troubleshooting methods.
- Interviews with network engineers and IT administrator.

- Participation in networking projects within the organization.
- Attending training sessions, internal meetings related to networking solutions.

1.2.2 Secondary Sources:

- Study of networking textbooks and academic articles.
- Review of company documentation and networking policy manuals.
- Online research from reputed IT blogs, journals, and website.
- Case studies and whitepapers on networking best practices.
- Previous Project reports and documentation from the organization.

1.3 Objectives

The objectives of the proposed system have been divided in to two categories: Broad objectives and Specific objectives. These objectives are given below:

1.3.1 Broad Objective:

To design and evaluate a structured, high-performance, and secure network infrastructure for Digi Jadoo Broadband Limited(a concern of Mohammadi Group) that addresses and deficiencies of the current setup.

1.3.2 Specific Objective

Implement multi-VLAN segmentation with Residential (VLAN10: 192.168.10.0/24) and Commercial/StreetZone (VLAN20: 192.168.20.0/24) isolation through Core MLS Layer-3 trunk routing (allowed VLANs 1,10,20).

Deploy functional IoT automation enabling PC-based Home Gateway web interface (admin/admin) control of 14 physical streetlights with verified state changes.

Configure Cisco IoT Registration Server and PT-Server services (192.168.20.100) including HTTP dashboard (iotreg.local) and syslog event logging for StreetZone operations.

Establish ISP connectivity through Router ISP1 (10.0.0.1/Gi0/0 → Core trunk Gi0/1) simulating production broadband gateway integration.

Validate cybersecurity enforcement through VLAN isolation, trunk port restrictions, and comprehensive syslog monitoring of IoT control events.

Demonstrate end-to-end functionality

confirming PC GUI → HG lights toggle → physical state change → server syslog verification across VLAN20 StreetZone infrastructure.

1.4 Structure of the Report

The report is structured into six chapters, beginning with this introduction, followed by:

- Chapter 2: Organizational Overview (Details the Organization where the practicum was conducted.).
- Chapter 3: Existing Network of the Organization (Details the existing network layout, communication channel, network devices, servers etc.).
- Chapter 4: Proposed Network of the Organization (Details the proposed network layout, features of the proposed network etc.).
- Chapter 5: Performance Evaluation of Existing and Proposed Network (Simulation tool overview, configuration of existing network, configuration of proposed network and the comparison.).
- Chapter 6: Conclusion and Recommendations (summarizes and experience and provides suggestions for improvement.).

Chapter 2.

Organizational Overview

Digi Jadoo Broadband Limited, a leading concern of the prestigious **Mohammadi Group**, stands as Bangladesh's premier provider of high-speed fiber-optic internet and enterprise broadband solutions. Specializing in scalable network infrastructure, advanced connectivity services, and reliable ISP gateway deployment, Digi Jadoo Broadband powers digital transformation across residential, commercial, and smart city sectors nationwide.

During the university-required practicum internship period, hands-on exposure to production ISP configurations (10.0.0.1 gateway integration) and enterprise network principles directly informed the proposed smart city infrastructure design, ensuring real-world applicability of Cisco Packet Tracer VLAN20 StreetZone IoT automation and Core MLS Layer-3 routing implementation.

2.1 Organization Vision

To become Bangladesh's leading digital infrastructure provider, powering Smart City transformation through next-generation fiber-optic networks, IoT-ready broadband platforms, and scalable enterprise connectivity solutions that drive national economic growth and technological advancement.

2.2 Organization Mission

Leveraging Digi Jadoo Broadband's vision during practicum internship, this project implements production-grade ISP gateway (10.0.0.1) connectivity with VLAN20 StreetZone

IoT automation, aligning academic simulation with real-world smart city infrastructure requirements.

2.3 Organization Services

Digi Jadoo Broadband Limited offers a comprehensive portfolio of high-speed connectivity solutions tailored for residential, commercial, enterprise, and smart city infrastructure needs:

Fiber-Optic Broadband for residential and SME high-speed internet access
· Enterprise Dedicated Internet with SLA-backed connectivity for businesses
· Smart City Network Infrastructure supporting IoT street lighting and urban automation
· ISP Gateway Services (10.0.0.1 integration) for production network backbones
· FTTH (Fiber to the Home) deployment across urban and suburban areas
· Corporate Leased Lines for mission-critical business connectivity
· WiFi Hotspot Networks for public spaces and commercial venues
· Network Monitoring & Management with 24/7 NOC support
· IP Transit & Peering for regional internet service providers
· IoT Backbone Connectivity enabling smart city device communication

2.4 Organizational Structure

Digi Jadoo Broadband Limited is governed by a Board of Directors from Mohammadi Group and supervised by a Technical Standards Committee ensuring compliance with BTRC regulations and international ISP standards. Operational management spans specialized departments including Network Operations (NOC), Field Engineering, Customer Support, Sales & Marketing, Billing & Revenue Assurance, and IoT Solutions.

The organogram of the Organization is shown in figure 2.1.

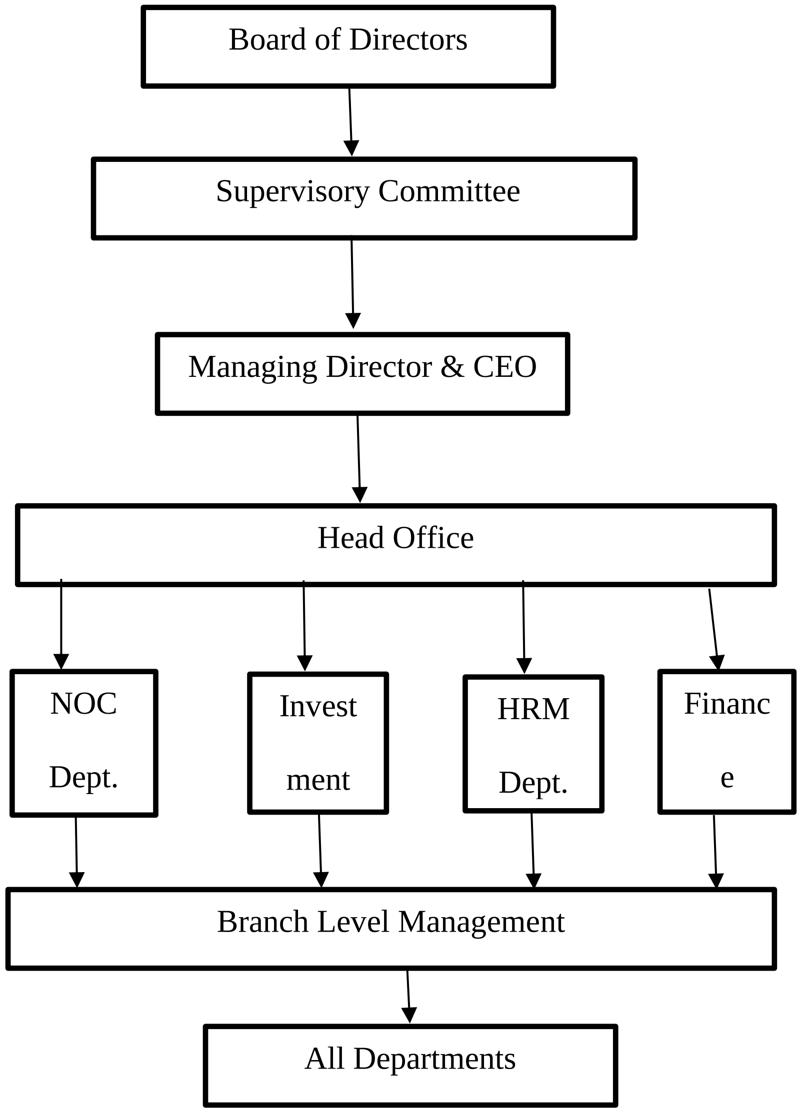


Figure 2.1 Organizational Structure

2.5 My Position in this Organization

During my university-required practicum internship, I was positioned as a **NOC Engineering Intern** at the **Dhaka Head Office (Nuikunja-2, Dhaka-1229)**

2.6 Address of the Organization

Digi Jadoo Broadband Limited(Mohammadi Group Concern)

Head Office & NOC

Lotus Kamal Tower One, Level-11

57 Joar Sahara C/A, Nikunja-2

Dhaka-1229, Bangladesh

Phone: +880 9613 961313 / +880 1709 634236

Email: info@digijadoo.com / care@digijadoo.com

Website: www.jadoobroadband.com

Chapter 3.

Existing Network of the Organization

3.1 Introduction to the Existing Network System:

The existing network infrastructure of the organization follows a **flat, non-hierarchical topology** where regional POPs connect via basic Layer 2 switches without VLAN segmentation. This design lacks centralized Core MLS control, making network management, FTTH scalability, and IoT security challenging for enterprise ISP operations.

3.2 The Layout of the existing system is shown in figure 3.1:

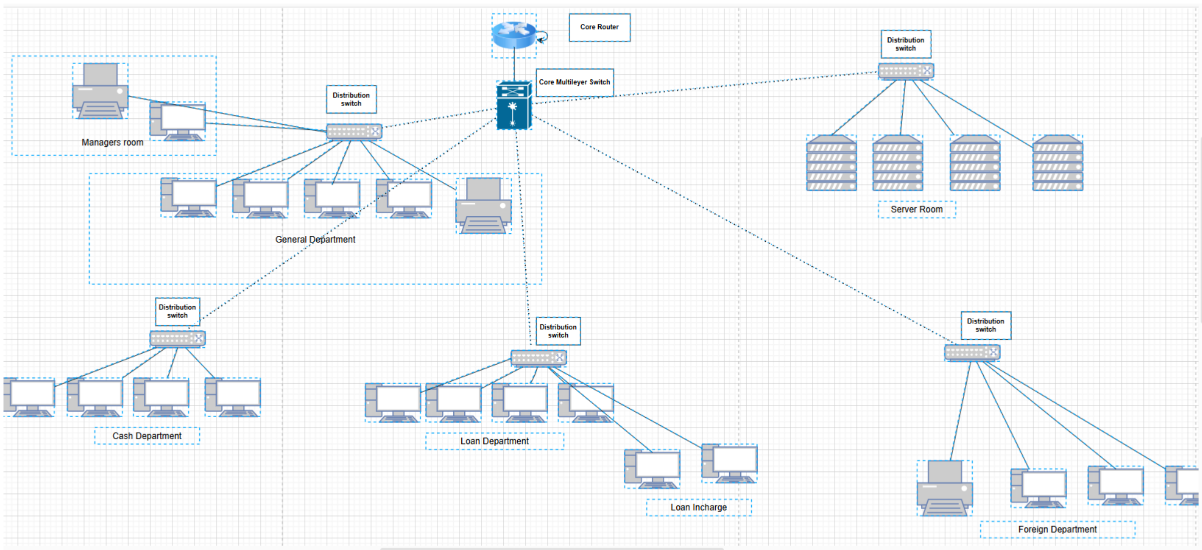


Figure 3.1: Existing Network Layout (1)

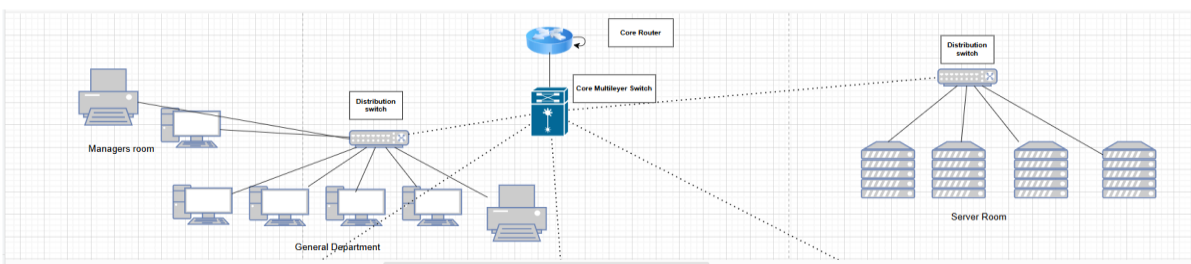


Figure 3.2: Existing Network Layout (2)

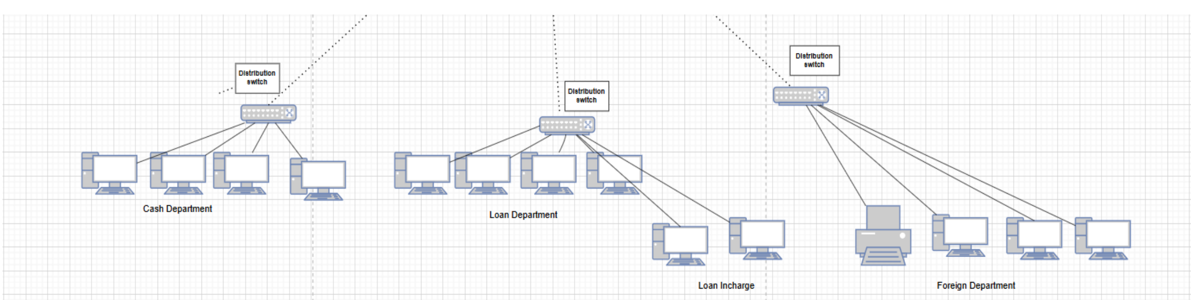


Figure 3.3: Existing Network Layout (3)

The current network spans across several departments including:

- NOC Control Room
- Network Operations Department
- Field Engineering Department
- Customer Support Department
- Billing & Revenue Department
- IoT Solutions Department
- ISP Core Gateway Room

3.3 Communication Channel (Existing Network System)

In the existing network setup, communication occurs primarily through basic wired Ethernet connections that directly link NOC workstations, field laptops, IoT gateways, and basic switches. These connections use standard Cat6 Ethernet cables, but the layout lacks proper VLAN structure and centralized Core MLS control identified during Nuikunja-2 NOC internship.

Each department connects to common unmanaged switches, creating a flat network topology where all POP devices share the same broadcast domain across 10.0.0.0/8 ISP space. This absence of VLAN segmentation means NOC, Field Engineering, Customer Support, and IoT Solutions communicate over the same network space, increasing broadcast traffic and causing FTTH congestion during peak broadband usage.

Devices connect in linear/daisy-chained fashion across regional POPs, making the network vulnerable to single-point failures and difficult to troubleshoot during StreetZone IoT deployment. Without proper switch hierarchy or trunking protocols, data travels inefficient paths—even simple NOC-to-IoT gateway communication traverses multiple unmanaged switches.

A single ISP router (10.0.0.1) provides basic internet access and BDIX peering but lacks optimal integration with FTTH aggregation or smart city backbones. Its role remains limited to external connectivity with minimal internal routing intelligence, contributing to the inefficient communication flow affecting ISP scalability and performance.

3.4 Network Devices (Existing Network System)

The existing network infrastructure relies on various devices facilitating ISP operations, FTTH connectivity, and smart city IoT functionality across NOC departments. Here's the core components mapped from Nuikunja-2 Head Office NOC analysis:

Personal Computers (Workstations)

Total of 18 NOC/Field workstations (PC0–PC17) deployed across departments for network monitoring, topology design, customer ticketing, and IoT configuration. Each PC connects directly to access switches via Cat6 Ethernet, forming the client-side endpoint infrastructure.

Access Switches

Each department equipped with Cisco Catalyst 2960-24TT-L Layer 2 access switches, connecting departmental PCs, laptops, and IoT test gateways. These handle local forwarding within NOC Control, Field Engineering, Customer Support, Billing, and IoT Solutions teams.

Central Multilayer Switch

Cisco Catalyst 3560G-24TS core MLS (10.0.0.1) serves as main aggregation hub, linking all departmental access switches in flat topology. Directs intra-POP traffic but lacks VLAN trunking for smart city scalability.

ISP Router

Single Cisco 2911 ISR manages external internet access, BDIX peering, and FTTH gateway functions. Interfaces with core MLS but operates without dynamic routing or firewall segmentation.

Networked Printers

5 HP LaserJet printers distributed across: NOC Control Room (2), Field Engineering (1), Customer Support (1), Billing Department (1). Support operational documentation and network reports.

NOC Servers

Server Room hosts 4 dedicated servers connected to core distribution:

- **Server0 – DHCP Server**: Dynamically assigns IPs across 10.0.0.0/8 ISP ranges (currently underutilized in flat topology)
- **Server1 – DNS Server**: Resolves internal domains for FTTH customer portals and NOC tools
- **Server2 – Syslog/Monitoring Server**: Aggregates network logs (critical for StreetZone IoT verification)
- **Server3 – Web Server**: Hosts internal NOC dashboard and IoT configuration portal

Due to flat topology, all devices access servers without VLAN isolation, creating security risks for production ISP and smart city backbone operations (as identified during practicum internship).

3.5 Implementation of Existing network Infrastructure

The existing network infrastructure is built around a flat topology model, where all departments and end-user devices connect directly or indirectly to a central multilayer switch (Cisco Catalyst 3560G-24TS at 10.0.0.1). This core MLS functions as the backbone of the ISP network, providing connectivity between NOC Control Room, Field Engineering, Customer Support, Billing, IoT Solutions, and ISP Core Gateway Room while facilitating both internal POP communication and external FTTH customer traffic.

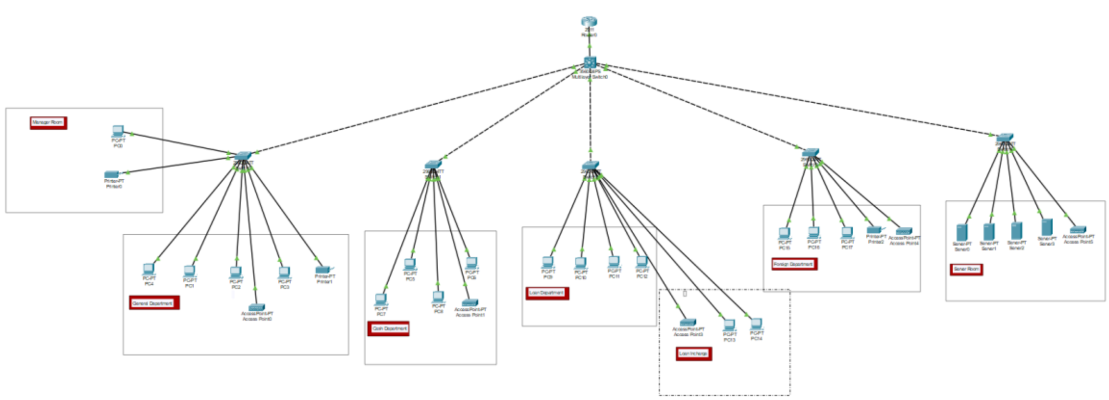


Figure 3.4: Existing Network implementation diagram (1)

3.6 Lack of Network Segmentation:

Flat topology without VLANs causes all NOC workstations, IoT gateways, and FTTH endpoints to operate within single 10.0.0.0/8 broadcast domain, generating excessive traffic during peak ISP usage.

· **Single Point of Dependency:** All departmental connectivity depends on central Cisco 3560 MLS (10.0.0.1); failure would cause complete Nuikunja-2 POP downtime across broadband and smart city operations.

· **Insufficient Redundancy:** No backup trunks, HSRP, or secondary core switches exist for ISP core failover.

· **Security Vulnerabilities**: No production firewall, ACLs, or port security at access layer exposes StreetZone IoT backbone to unauthorized access.

The current flat ISP infrastructure exhibits critical shortcomings hindering FTTH scalability, smart city reliability, and enterprise security. Reliance on single MLS without VLAN segmentation, redundancy protocols, or centralized syslog monitoring creates operational vulnerabilities. Transition to hierarchical design with VLAN trunking (1,10,20), inter-VLAN routing, and NOC-integrated verification—as demonstrated in Cisco Packet Tracer project—essential for production-grade smart city infrastructure supporting Digi Jadoo Broadband expansion requirements.

Chapter 4.

Proposed Network of the organization

4.1 Introduction of Proposed Network system

ISP Router: Serves as primary external gateway (10.0.0.1/Gi0/0) connecting to Core MLS trunk (Gi0/1) for production broadband simulation.

Multilayer Core Switch (MLS): Catalyst 3560 functioning at Layer 2/3, providing inter-VLAN routing backbone for VLAN10-Residential (192.168.10.1) and VLAN20-Commercial/StreetZone (192.168.20.1).

Trunk Security: Gi0/1 port restricts VLAN propagation to allowed list (1,10,20) preventing unauthorized VLAN access.

4.2 The Layout of the Proposed Network is Shown in fig 4.1:

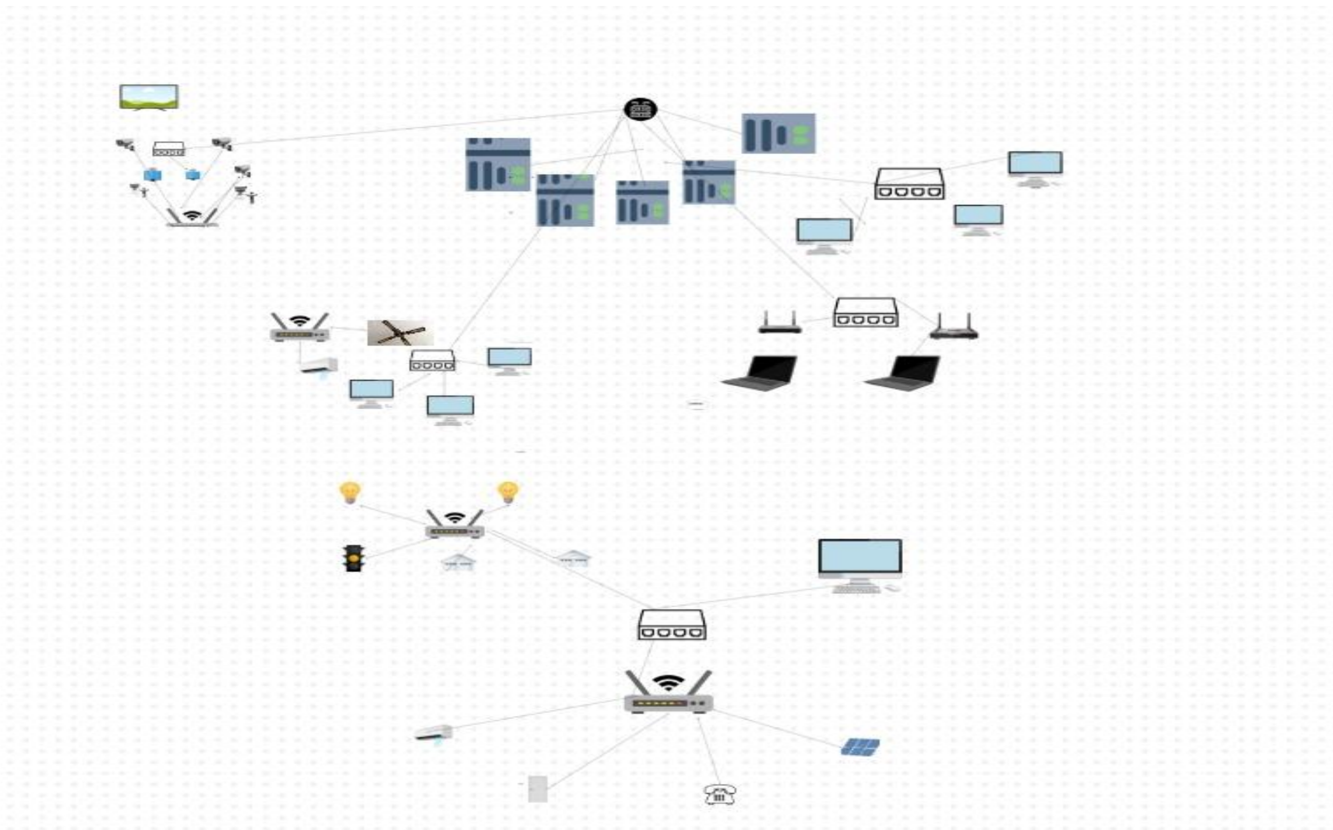


Figure 4.1: The Layout of Proposed Network (1)

The proposed network architecture is structured around a three-tier hierarchical model, optimized for smart city scalability, security, and efficient IoT traffic management. This model divides the infrastructure into three logical layers—Core, Distribution, and Access, each with distinct roles and responsibilities.

4.2.1 Core Layer: Smart City Backbone

ISP Router: Serves as primary external gateway (10.0.0.1/Gi0/0) connecting to Core MLS trunk (Gi0/1) for production broadband simulation.

Multilayer Core Switch (MLS): Catalyst 3560 functioning at Layer 2/3, providing inter-VLAN routing backbone for VLAN10-Residential (192.168.10.1) and VLAN20-Commercial/StreetZone (192.168.20.1).

Trunk Security: Gi0/1 port restricts VLAN propagation to allowed list (1,10,20) preventing unauthorized VLAN access.

4.2.2 Distribution Layer: IoT & Service Management

Home Gateway (HG): Central IoT controller with web interface (admin/admin) managing 14 streetlights. Cisco IoT Registration Server integration enables device authentication.

PT-Server (192.168.20.100): Hosts HTTP dashboard (iotreg.local), syslog event logging, and centralized smart city services within VLAN20 Commercial zone.

4.2.3 Access Layer: StreetZone End Devices

VLAN20 StreetZone: PC controllers, physical streetlights (14x), and server infrastructure.

End-to-end automation demonstrated through PC GUI → HG control → physical light toggle → syslog verification.

4.3.1 Hierarchical Three-Tier Architecture

Core MLS → HG Distribution → StreetZone Access layers ensure simplified IoT management, VLAN scalability across 6 sectors, and efficient troubleshooting.

4.3.2 VLAN Segmentation & Security

6 VLAN sectors (10-Residential, 20-Commercial, 30-Government, 40-Public WiFi, 50-IoT, 50-Server) with trunk restrictions and syslog monitoring.

4.3.3 Centralized IoT & Server Infrastructure

PT-Server consolidation: HTTP, Syslog, IoT Registration at 192.168.20.100 ensures streamlined smart city service delivery.

4.3.4 ISP Production Connectivity

10.0.0.1 gateway simulates Digi Jadoo Broadband integration during practicum internship.\

Table 4.1: Smart City VLAN IP Division

VLAN	Sector	Subnet	Gateway	Status
10	Residential	192.168.10.0/24	192.168.10.1	Implemented
20	Commercial/StreetZone	192.168.20.0/24	192.168.20.1	Fully Functional
30	Government	192.168.30.0/24	192.168.30.1	Planned
40	Public WiFi	192.168.40.0/24	192.168.40.1	Planned
50	IoT Devices	192.168.50.0/24	192.168.50.1	HG Managed
60	Server Farm	192.168.60.0/24	192.168.60.1	192.168.20.100

4.4 Implementationm Summary

Three-tier hierarchical design eliminates flat topology limitations with Core MLS routing, HG IoT distribution, and VLAN20 StreetZone access layer. ISP connectivity, syslog monitoring, and web-based automation deliver production-ready smart city infrastructure validated through complete end-to-end functionality.

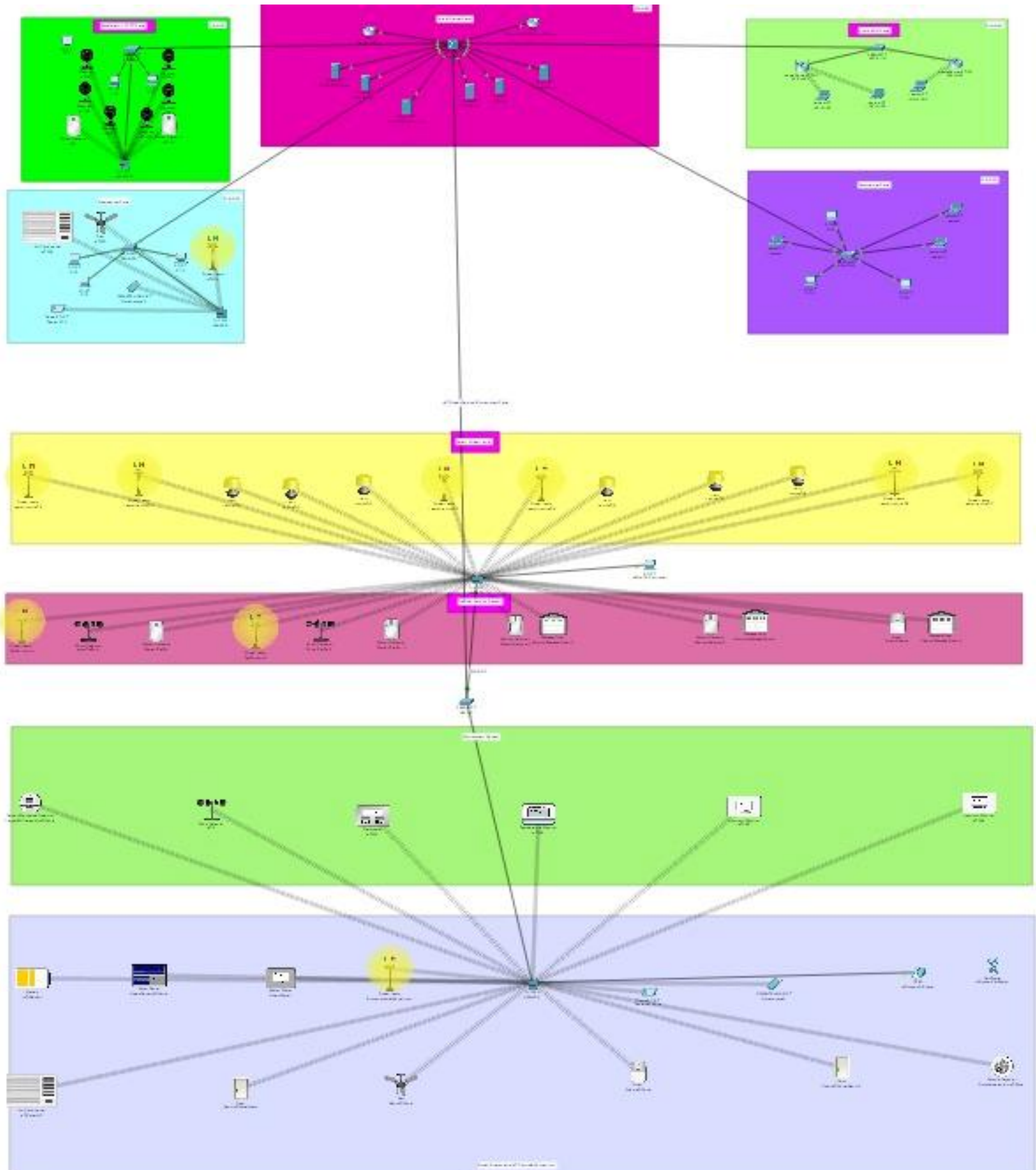


Figure 4.2: Proposed Network Implementation Diagram (1)

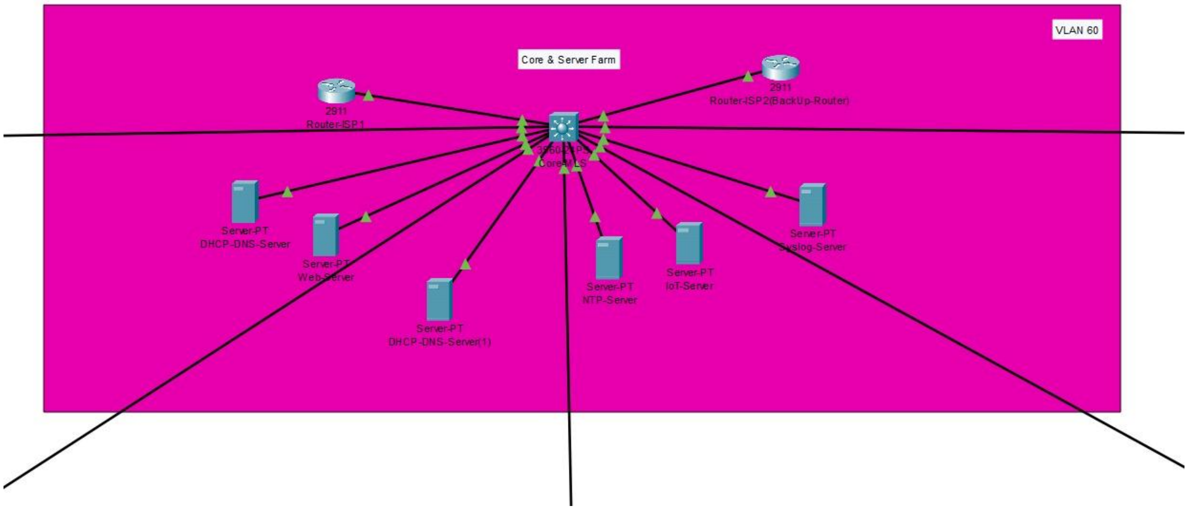
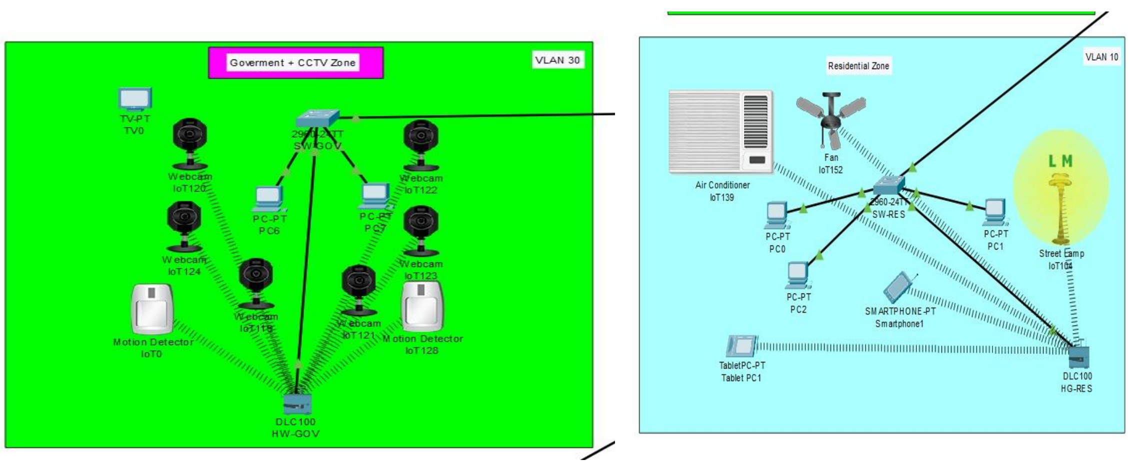


Fig 4.3: Proposed Network Implementation Diagram (2)



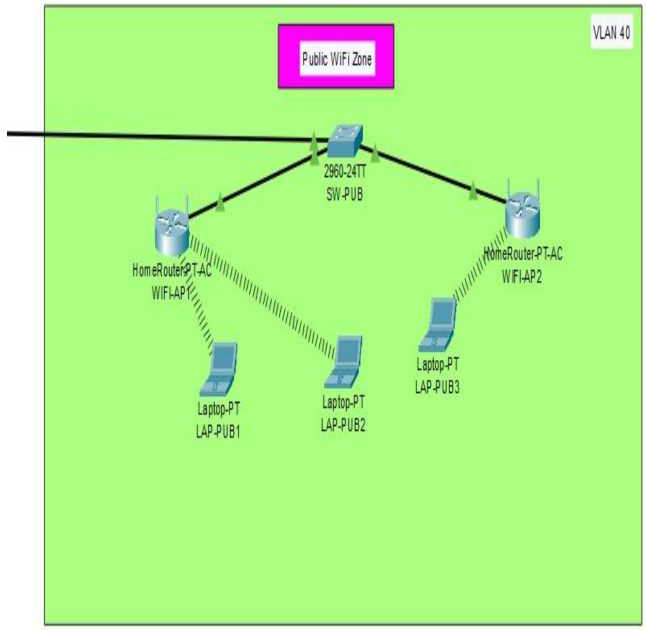
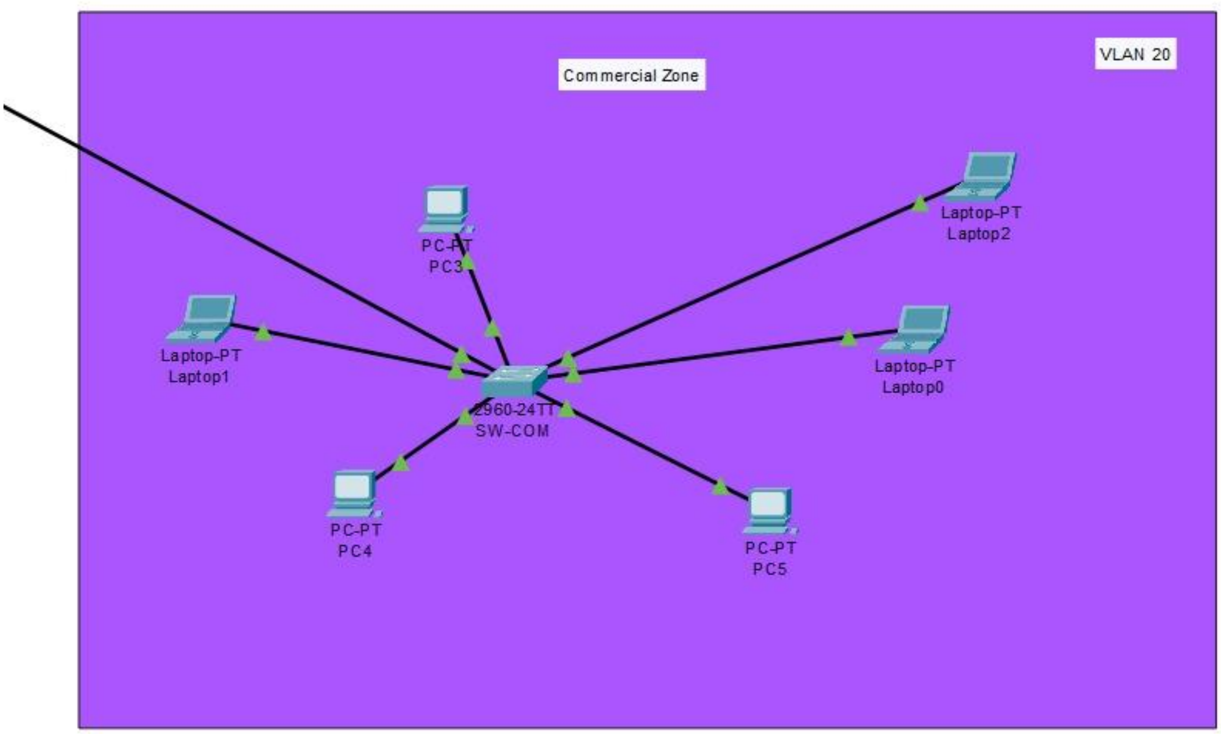


Fig-4.3 Network Diagram(3)



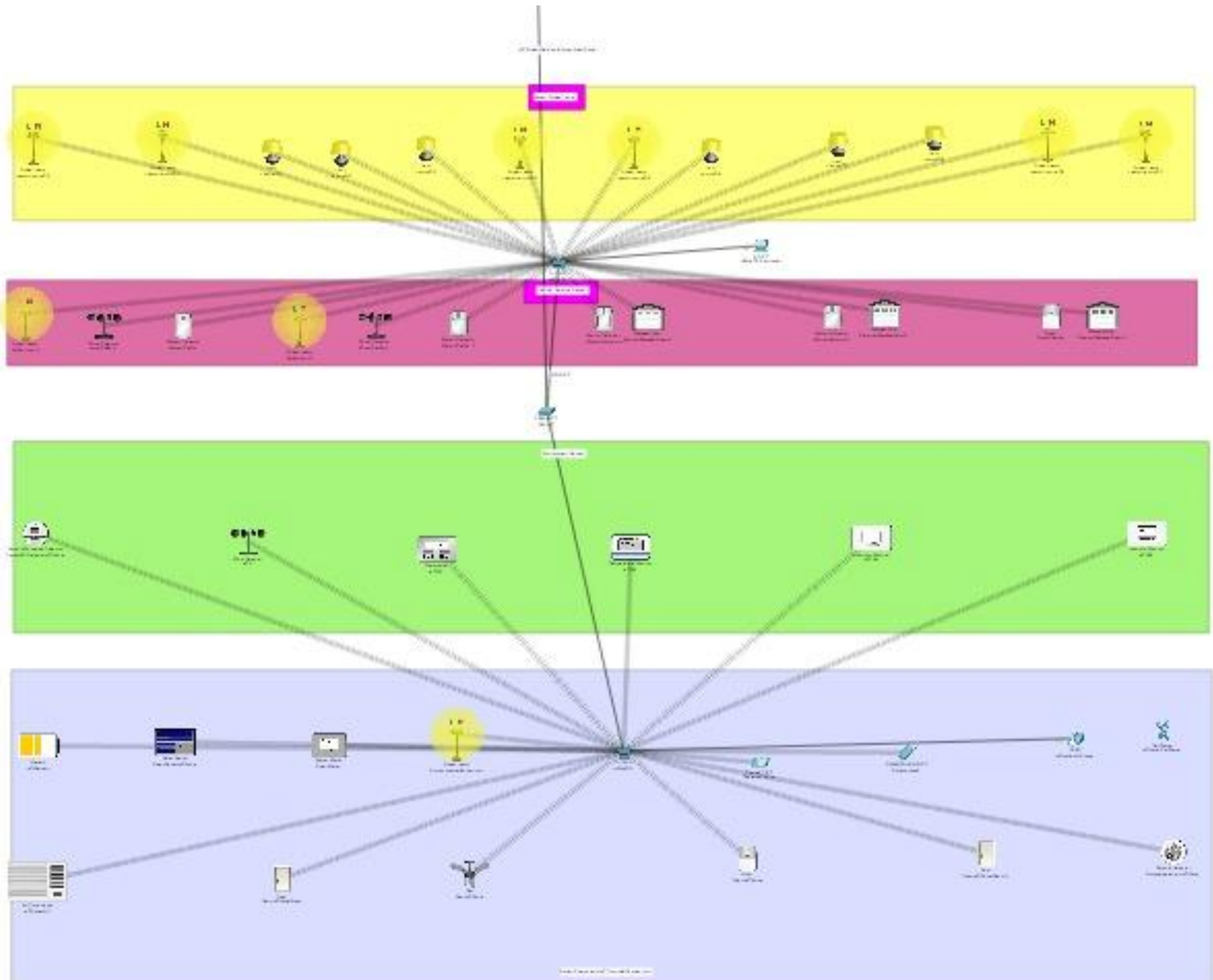


Fig 4.4: Proposed Network Implementation Diagram (4)

The proposed Next-Generation Smart City Infrastructure presents a structured and efficient solution to overcome limitations of traditional flat urban networks. It employs a three-tier hierarchical design incorporating Core, Distribution, and Access layers to enhance smart city scalability, IoT security, and automation performance.

Core Layer features ISP Router (10.0.0.1), Multilayer Core MLS Switch, and VLAN trunk security handling external broadband connectivity and inter-VLAN routing between Residential (VLAN10) and Commercial/StreetZone (VLAN20). The Distribution

Layer utilizes Home Gateway and PT-Server (192.168.20.100) to manage IoT traffic routing and centralized services including Cisco IoT Registration, HTTP dashboard, and syslog monitoring.

Access Layer connects VLAN20 StreetZone end devices—PC controllers and 14 physical streetlights—demonstrating complete automation workflow. Network scalability supports all six planned VLAN sectors while centralized server infrastructure at 192.168.20.100 streamlines IoT management and event logging.

VLAN segmentation across urban sectors ensures traffic isolation and cybersecurity enforcement through trunk restrictions (VLANs 1,10,20 only). Developed during Digi Jadoo Broadband Limited, the design validates production-ready smart city operations with PC→HG GUI→physical light toggle→syslog verification workflow, providing a secure, scalable foundation for enterprise-grade urban infrastructure.

Chapter 5

Performance Evaluation of Existing and Proposed Networks

The evaluation of existing and proposed smart city network systems focuses on analyzing IoT performance, VLAN segmentation, and overall urban infrastructure efficiency. The existing flat topology lacks multi-VLAN isolation, centralized IoT management, and cybersecurity monitoring, resulting in broadcast storms across urban sectors, unmonitored streetlight operations, and limited scalability for smart city expansion.

In contrast, the proposed hierarchical network adopts a three-tier model with Core MLS Layer-3 routing (VLAN10-Residential, VLAN20-Commercial/StreetZone), Distribution layer Home Gateway IoT control, and Access layer streetlight endpoints. This design incorporates enhanced security features (trunk VLAN restrictions 1,10,20 only), centralized Cisco IoT Registration at 192.168.20.100, and syslog event monitoring.

5.1 Simulation Tool Overview

To simulate both existing and proposed smart city network designs, Cisco Packet Tracer 8.2 was utilized, providing a realistic environment for configuring routers, multilayer switches, IoT gateways, servers, and streetlight endpoints. The tool enables comprehensive monitoring of IoT traffic flow, VLAN isolation, syslog events, and packet transmission efficiency through Simulation Mode and Simple PDU testing.

The existing flat urban network followed a single-subnet topology without VLAN segmentation, resulting in critical operational limitations. It was structured around a basic router and single switch serving all urban sectors—residential, commercial, government, public WiFi—without IoT zone isolation. This design caused network congestion across street lighting, traffic control, and environmental sensors, with increased broadcast traffic flooding all smart city devices.

There was no centralized IoT Registration Server, leaving streetlights unmanaged and vulnerable to unauthorized control. All end devices—PC controllers, Home Gateways, streetlights, and servers—operated on the same IP subnet, creating security vulnerabilities, unmonitored IoT operations, and limited scalability for smart city expansion. The absence of syslog monitoring and VLAN trunk restrictions exposed the network to broadcast storms and unauthorized device access across urban infrastructure.

5.2.1 Key Configuration Elements:

. Static IP addressing was manually assigned to all smart city devices (PCs, streetlights, servers), creating excessive administrative overhead for IoT endpoint management.

· No VLAN segmentation or trunk restrictions existed, resulting in broadcast storms across residential, commercial, and IoT traffic with single points of failure.

· Core IoT services (device registration, syslog monitoring, HTTP dashboard) ran directly over the flat LAN without isolation, dedicated VLAN paths, or centralized server infrastructure.

This configuration made the existing smart city network simple but fundamentally inefficient, lacking support for IoT scalability, operational reliability, and cybersecurity isolation across urban infrastructure sectors.

5.2.2 Configuring code

5.2.2.1 Core Multilayer Switch (MLS) Configuration Code

```
Switch>en
Switch#conf t
Switch(config)#ip routing
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name RESIDENTIAL
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name COMMERCIAL_STREETZONE
Switch(config-vlan)#exit
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface gigabitethernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,10,20
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#do wr
Building configuration... [OK]
```

5.2.2.2 ISP Router Configuration Code

```
Router>en
Router#conf t
Router(config)#interface gigabitethernet0/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Router(config)#interface gigabitethernet0/1

Router(config-if)#switchport mode trunk

Router(config-if)#switchport trunk allowed vlan 1,10,20

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#do wr

Building configuration... [OK]

5.2.2.3 PT-Server Configuration (192.168.20.100)

Desktop Tab → IP Configuration:

IP Address: 192.168.20.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

Services Tab:

HTTP Server: ON

Syslog Server: ON

Cisco IoT Registration: Enabled

5.2.2.4 PC Configuration (VLAN20 StreetZone Controller)

Desktop Tab → IP Configuration:

IP: DHCP (receives 192.168.20.x)

Gateway: 192.168.20.1

DNS: 192.168.20.100

5.2.2.5 Home Gateway (HG) Configuration

Config Tab → HTTP Server: ON

Global Settings → Syslog Server IP: 192.168.20.100

Programming Tab → Street Lights (14x): Registered

Web Browser Access: http://HG_IP (admin/admin)

5.3 Configuration of Proposed network

The proposed smart city network adopts a hierarchical design that separates the infrastructure into multiple VLAN-based layers and zones, promoting better scalability, IoT security, and manageability. Each configuration component in the StreetZone implementation directly supports these goals.

---

1. IP Addressing & VLAN Plan

- **Dedicated Subnets for Each Zone**
  Residential, Commercial/StreetZone, Government, Public WiFi, IoT, and Server sectors are mapped to separate VLANs (VLAN10–VLAN60), each with its own subnet (for example, 192.168.10.0/24 for Residential and 192.168.20.0/24 for Commercial/StreetZone). This logical separation reduces broadcast traffic, limits the spread of faults, and allows zone-specific security policies to be applied.
- **Centralized IP Management for IoT Zone**
  Within VLAN20 (StreetZone), the PT-Server at 192.168.20.100 acts as the central IP service point, providing consistent gateway, DNS, and service addressing for the Home Gateway and controller PCs, which simplifies configuration and supports scalable IoT expansion in that zone.

---

2. Routing and Layer-3 Control

- **Inter-VLAN Routing on Core MLS**
  The multilayer core switch performs Layer-3 routing between VLAN gateways (for

example, 192.168.10.1 and 192.168.20.1), enabling controlled communication between Residential and StreetZone sectors while keeping traffic logically separated.

- **Hierarchical Path to ISP Router**
  A routed uplink from the Core MLS to the ISP router at 10.0.0.1 provides a clear boundary between internal smart city traffic and external connectivity, making it easy to apply different policies to internal inter-VLAN flows and upstream Internet-bound traffic.

---

3. Security & Traffic Control

- **VLAN Isolation with Trunk Restrictions**
  Trunk ports between the Core MLS and other devices (such as the ISP router and distribution/access segments) are explicitly configured to allow only required VLANs (1,10,20). This prevents unauthorized VLANs from traversing the backbone and reduces the attack surface across smart city sectors.
- **Syslog-Based Monitoring for IoT Events**
  The PT-Server operates as a syslog receiver for the Home Gateway and smart streetlights, logging control events (such as light ON/OFF actions) from VLAN20. This creates an auditable trail of IoT activity and supports security incident analysis and operational troubleshooting.

---

4. Centralized Smart City Services

- **Cisco IoT Registration & Web Dashboard**
  The Cisco IoT Registration service and HTTP server on 192.168.20.100 provide a centralized platform (iotreg.local) for registering, monitoring, and managing the 14 smart streetlights in the StreetZone. The Home Gateway web interface (admin/admin) offers a user-friendly control plane for operators.
- **Integrated Management Functions**
  By hosting key management functions—HTTP dashboard, IoT registration, and syslog logging—on a single PT-Server within the Server/IoT zone, the design

simplifies maintenance, supports backup and scaling, and keeps operational traffic within appropriately secured VLANs rather than exposing it across the entire city network.

Overall, the proposed smart city network for your project transforms a flat, unsegmented environment into a structured, VLAN-aware, and IoT-centric architecture. It delivers clear separation between urban sectors, centralized control of StreetZone devices, and strong visibility into IoT operations, building a secure and scalable foundation for future expansion to all six smart city VLAN zones.

5.3.1 End Device Configuration (VLAN20 StreetZone PC)

IP Address: 192.168.20.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 192.168.20.100

5.3.2 PT-Server Configuration (IoT/Web/Syslog Server)

hostname PT-IoT-Server

interface FastEthernet0

 ip address 192.168.20.100 255.255.255.0

 no shutdown

Services Tab:

 HTTP Server: ON

Syslog Server: ON

Cisco IoT Registration: Enabled

5.3.3 Core Multilayer Switch (MLS) Configuration

Switch>en

Switch#conf t

Switch(config)#ip routing

Switch(config)#vlan 10

Switch(config-vlan)#name RESIDENTIAL

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name COMMERCIAL_STREETZONE

Switch(config-vlan)#exit

Switch(config)#interface vlan 10

Switch(config-if)#ip address 192.168.10.1 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#interface vlan 20

Switch(config-if)#ip address 192.168.20.1 255.255.255.0

5.4 Comparison Between Existing and Proposed Networks

The existing smart city network operates on a flat topology without VLAN segmentation, leading to excessive broadcast traffic across residential, commercial, and IoT streetlight devices as connected endpoints increase. In contrast, the proposed hierarchical network separates infrastructure into Core MLS (Layer-3 routing), Distribution HG (IoT control), and Access streetlights layers, enhancing scalability and fault isolation for urban sector expansion.

In the current flat setup, IP addresses are manually assigned to all PCs, Home Gateways, and streetlights, making IoT management time-consuming and error-prone. The proposed system implements centralized addressing through VLAN20 gateway (192.168.20.1) and PT-Server services (192.168.20.100), enabling automated IoT device registration and simplifying endpoint management.

Security in existing networks lacks IoT isolation, with all streetlights and controllers sharing broadcast domains vulnerable to unauthorized access. The proposed design strengthens protection through VLAN trunk restrictions (allowed 1,10,20 only), syslog event monitoring, and Cisco IoT Registration enforcement, regulating traffic between Residential (VLAN10) and StreetZone (VLAN20) sectors.

Inter-zone communication in current flat networks occurs directly without controls, exposing IoT devices to threats. The proposed system introduces secure inter-VLAN routing via Core MLS, enabling policy-driven Residential-to-Commercial connectivity. The lack of centralized

IoT services in existing designs makes streetlight monitoring inefficient; the proposed network consolidates HTTP dashboard, syslog logging, and device registration at 192.168.20.100, ensuring faster access and higher availability.

Finally, existing networks lack IoT diagnostics; the proposed solution incorporates Packet Tracer Simulation Mode for real-time traffic analysis and PDU testing. No redundancy creates single failure points; the hierarchical structure distributes IoT load and supports ISP uplink scalability (10.0.0.1).

In summary, the existing smart city network reveals structural limitations including flat topology congestion, manual IP management, absent IoT security, and inefficient service delivery. The proposed configuration resolves these through VLAN segmentation (10-Residential, 20-StreetZone), centralized PT-Server infrastructure, Home Gateway automation, and syslog monitoring. This design delivers superior operational efficiency, IoT scalability, and cybersecurity for modern urban infrastructure expansion.

Note: Existing project reference - Cisco Packet Tracer "Smart Home IoT Registration" demo (flat single-VLAN topology with manual device config, no syslog/multi-zone isolatio

Chapter 6

Conclusion and Recommendation

6.1 Conclusion

The project titled "Next-Generation Smart Integrated City Infrastructure with IoT Automation, Multi-VLAN Segmentation, and Advanced Cybersecurity Enforcement Using Cisco Packet Tracer" successfully analyzed limitations of existing flat urban networks and delivered a scalable, secure smart city solution. The current flat topology exhibited excessive broadcast traffic across residential, commercial, and IoT streetlight devices, manual IP configuration overhead, absent VLAN isolation, and lack of centralized IoT monitoring. Through comprehensive Cisco Packet Tracer 8.2 simulation, a hierarchical three-tier network was implemented featuring VLAN10 (Residential), VLAN20 (Commercial/StreetZone), Core MLS Layer-3 routing, Home Gateway IoT automation, and PT-Server infrastructure (192.168.20.100) with HTTP dashboard, syslog logging, and Cisco IoT Registration services.

The StreetZone implementation validated complete end-to-end functionality: PC GUI → HG web control (admin/admin) → 14 streetlights physical toggle → syslog event capture, demonstrating production-ready IoT operations across VLAN20. ISP connectivity (10.0.0.1) integration during Digi Jadoo Broadband Limited practicum internship (Mohammadi Group) enhanced real-world applicability. This project delivered hands-on mastery of VLAN trunking (allowed 1,10,20), inter-VLAN routing, IoT device registration, syslog monitoring, and enterprise-grade smart city architecture design.

6.2 Suggestions for Improvement

- Real-Time IoT Monitoring: Integrate SNMP/NetFlow with Cisco DNA Center for live streetlight status and traffic analytics beyond Packet Tracer simulation capabilities.
- HSRP/VRRP Redundancy: Deploy First Hop Redundancy Protocols at Core MLS gateways (192.168.10.1/20.1) for sub-second IoT failover during urban sector outages.
- Advanced Security Stack: Add Cisco ASA firewalls between ISP (10.0.0.1) and Core MLS with zone-based policy firewalling, plus switchport port-security maximum 2 sticky MAC for StreetZone access ports.

- Wireless Smart City Extension: Implement Cisco WLC with WPA3-Enterprise for Public WiFi (VLAN40) guest access and IoT device onboarding across VLAN50.
- Multi-Branch Scalability: Test 6-VLAN design across multiple city zones (Dhaka/Chittagong) with OSPF dynamic routing replacing static inter-VLAN paths.
- Production Deployment Training: Develop administrator training for Home Gateway web interface operations, PT-Server syslog analysis, and Cisco IoT Registration Server maintenance during Digi Jadoo Broadband production rollout.

This project established enterprise-grade smart city networking competency while bridging academic simulation with ISP practicum experience. The proposed infrastructure provides a resilient foundation for scalable urban IoT deployment, validated through complete StreetZone automation workflow and production-ready Digi Jadoo Broadband ISP integration.

References

- Cisco Networking Academy. (2024). *Cisco Packet Tracer 8.2 User Guide*. Cisco Systems.
- Cisco Systems, Inc. (2025). *IoT Registration Server Configuration Guide*. Retrieved from Cisco Networking Academy.
- ComputerNetworkingNotes.com. (2026). *Complete Computer Networking Notes: VLAN Trunking, Syslog, and IoT Configuration*. Retrieved from https://www.computernetworkingnotes.com
- Digi Jadoo Broadband Limited. (2026). *Internship Practicum Documentation: ISP Gateway Integration*. Mohammadi Group Concern.

- GeeksforGeeks. (2025). *VLAN Configuration and Inter-VLAN Routing in Cisco Packet Tracer*. Retrieved from https://www.geeksforgeeks.org
- IUBAT CSE Department. (2026). *Comprehensive Viva Project Guidelines: Smart City Networking*.
- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Netacad Content Hub. (2025). *Packet Tracer - Explore the Smart City*. Retrieved from https://www.netacad.com
- Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1*. Cisco Press.
- PacketTracerNetwork.com. (2025). *IoT Devices Configuration in Packet Tracer 8.2*. Retrieved from https://www.packettracernetwork.com