Premier University

Chattogram

Project Proposal

Design and Simulation of an IPv6 Smart City IoT Network

with Quality of Service and Resilient Routing

Submitted by

Name	**ID**
MD Nishadul Islam Chy Shezan	0222220005101014
MD Sakib	0222220005101019
Rimjhim Dey	0222220005101039

Section: A
Batch: 42
Session: Spring 2025

Submitted to

Dr. Shahid Md. Asif Iqbal
Professor
Department of Computer Science and Engineering
Associate Dean
Faculty of Engineering

August 2025

Contents

Contents

Introduction

Modern cities deploy a wide range of interconnected sensors to gather valuable data about traffic, air quality, waste management, and infrastructure usage. However, most existing municipal networks still depend heavily on IPv4, which faces serious address limitations and lacks native support for large-scale IoT deployments. This project aims to design a smart city network in Cisco Packet Tracer using IPv6 for virtually unlimited addressing and Quality of Service (QoS) for prioritizing critical emergency traffic.

The proposed network will illustrate how these technologies can improve the reliability, scalability, and responsiveness of city-wide sensor systems, especially under failure scenarios. Current IPv4 constraints—such as address exhaustion requiring complex NAT configurations and limited IoT integration—will be overcome by our hierarchical IPv6 architecture.

Objectives

2.1 Design a scalable smart city network in Cisco Packet Tracer with access, distribution, and core layers

2.2 Implement IPv6 across all segments to remove address exhaustion issues

2.3 Configure Quality of Service to guarantee priority for emergency traffic

2.4 Separate IoT, public Wi-Fi, and administrative devices using VLANs and ACLs

2.5 Create automated email alerts through SMTP for critical network events

Scope

This project focuses on the design, simulation, and testing of a smart city IoT network prototype in Cisco Packet Tracer. It covers:

- A robust three-tier network architecture with structured IPv6 addressing
- Security enforcement through VLAN segmentation and ACL policies
- Deployment of basic network services (SMTP, HTTP) to support system monitoring
- Simulation of multiple IoT devices, including traffic sensors, air quality monitors, and smart waste bins
- Failover validation and QoS performance testing for critical traffic

Physical installation details, advanced encryption frameworks, large-scale application development, and deep real-time analytics platforms are excluded to keep the scope focused on essential networking concepts.

Tools and Technologies

Primary Platform: Cisco Packet Tracer 8.2.x with IoT device templates and simulation features

Networking Protocols:

- IPv6 (RFC 8200) for addressing
- IEEE 802.1Q for VLAN trunking

Services: SMTP, HTTP

Security: Extended ACLs, VLAN segmentation, port security for device control

Key Features

5.1 **IPv6 Implementation:** Fully native IPv6 addressing with /48 for sites and /64 for subnets, removing NAT complexity and enabling future scalability

5.2 **Quality of Service:** Four-tier traffic classification ensuring mission-critical and emergency services are always prioritized

5.3 **Security:** VLAN-based isolation between different device types, reinforced with ACL-based access control

5.4 **Monitoring:** Automated SMTP alerts for critical events and an HTTP dashboard for centralized status viewing

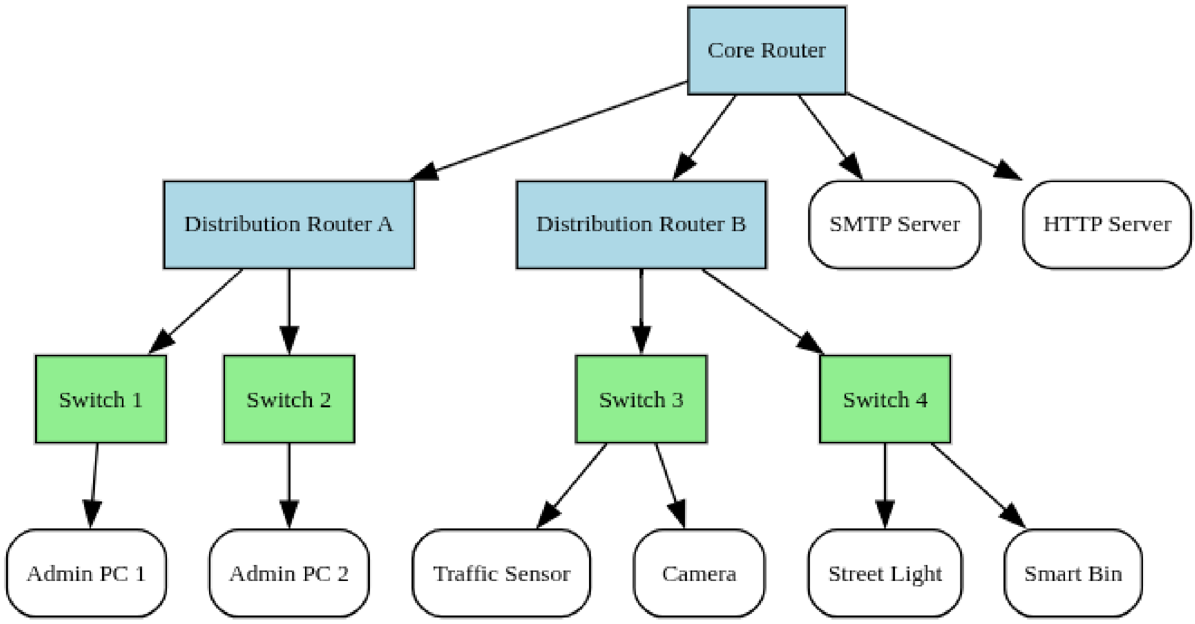

Figure 1: Proposed Smart City IoT Network Architecture with IPv6 and QoS

Project Timeline

Weeks	**Phase**	**Key Activities**
Weeks 1–2	Literature Review	Research smart city networks and IPv6 deployments
Weeks 3–4	Project Planning	Finalize objectives, system design choices, and submit proposal
Weeks 5–6	Network Design	Create detailed topology in Packet Tracer
Weeks 7–8	Configuration	Implement IPv6, VLANs, and QoS policies
Weeks 9–10	Testing	Validate failover capabilities and security configurations
Week 11	Documentation	Compile findings, results, and technical report
Week 12	Submission	Submit project files and deliver final presentation

Expected Outcomes

7.1 A fully functional smart city network supporting over 15 IoT devices
7.2 Proven failover capability during router or link failures
7.3 Verified QoS performance ensuring emergency traffic priority
7.4 Comprehensive network documentation with step-by-step configuration templates
7.5 Practical hands-on experience with advanced enterprise networking technologies
7.6 A reference model adaptable to larger-scale real-world smart city deployments

The results will confirm that IPv6 effectively addresses the connectivity, scalability, and performance requirements of modern smart cities.

Complex Engineering Problem Attributes

Attribute	**How Project Meets It**
Conflicting Requirements	Efficiently allocating network bandwidth so emergency communications receive top priority while maintaining acceptable service quality for IoT devices and public users
Multiple Stakeholders	IoT sensors, city staff, administrative PCs, and public network users share infrastructure with differing needs
Depth of Analysis	Requires knowledge of IPv6 addressing, VLAN segmentation, ACL rules, and QoS policies
Extensive Knowledge	Combines advanced networking, security, and IoT integration concepts into a unified system
Interdependence	All network components, services, and configurations depend on each other for proper operation

Limitations

- **Simulation constraints:** Packet Tracer cannot perfectly replicate all real-world network conditions
- **Scale:** Limited to 15–20 devices compared to the thousands used in real cities
- **Wireless:** Unable to model actual interference and signal propagation complexities
- **Services:** Basic SMTP and HTTP functionality compared to production-grade platforms
- **Security:** No use of encryption or advanced cyber threat countermeasures

Despite these limitations, the prototype successfully demonstrates scalable concepts that can be expanded for real-world smart city networks.

Conclusion

This project addresses key networking challenges faced by modern smart cities through an IPv6-based IoT network design enhanced with QoS capabilities. The simulation showcases practical solutions for address exhaustion, prioritized traffic handling, and improved network resilience. By combining existing standards with thoughtful architecture, we present a blueprint for building efficient municipal sensor networks that enhance operational efficiency and emergency responsiveness.

The technical skills gained, along with the documented best practices, will be valuable for future deployments. While simulation limitations exist, the demonstrated concepts and configurations are directly applicable to larger-scale, production-grade smart city environments.