# The Department of Computer Science & Engineering (CSE)

(Odd Sem 2025-26)

Project Report On

**"Optimising QoS for IoT Traffic in 4G/LTE ISP Networks"**

**(Minor project, Course Code)**

**Submitted to**

**The Department of CSE**

In partial fulfilment of the requirements for the award of the

**Bachelor of Computer Application (BCA)**

By

Mahi (SBU234012), Sem-5 , Section-B
Ankit (SBU234025), Sem-5 , Section-B
Saloni kumari singh (SBU234041), Sem-5 , Section-B

Under the guidance of

**Ms Bikram Pratap Singh**
Coordinator, Departmental Project
& Internship Committee, Dept of CSE,

Sarala Birla University, Ranchi

# Certificate

Certified that ***Mahi(SBU234041), Ankit(SBU234025)*** and ***Saloni Kumari Singh (SBU234041)*** *of* ***BCA, Sem-5 & 2023-26****,* have carried out the research work presented in this project entitled "**Optimizing QoS for IoT Traffic in 4G/LTE ISP Networks"** for the award of (**BCA degree**) from **Sarala Birla University, Ranchi,** under my supervision during **Odd Sem 2025-26 session**. The project embodies the result of original work and studies carried out by the student themselves, and the contents of the project do not form the basis for the award of any other degree to the candidate or to anyone else.

Sign: _____

Date:

(**Bikram Pratap Singh**)
Coordinator, Departmental Project
& Internship Committee, Dept of CSE,

Sarala Birla University, Ranchi

# Declaration

We, **Ankit (SBU234025)**, **Mahi(SBU234012)**, and **Saloni kumari singh (SBU234041)**, student of **Program BCA, Sem-5, Batch(2025-26),** hereby declare that the report titled "**Optimizing QoS for IoT Traffic in 4G/LTE ISP Networks** which we submit to the department of CSE, Sarala Birla University Jharkhand, in partial fulfillment of the requirement for the award of degree/ diploma in "**BCA**", has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition. We further declare that we wrote the report, and that no part of it is copied from any source(s) without being duly acknowledged.

| | | |
|---|---|---|
| Signature: | Signature: | Signature: |
| Date: | Date: | Date: |
| **ANKIT** | **MAHI** | **SALONI KUMARI SINGH** |
| **SBU234025** | **SBU234012** | **SBU234041** |

# Acknowledgement

We express our sincere gratitude to my project guide, **Ms Bikram Pratap Singh,** for his able guidance, continuous support and cooperation throughout my project, without which the present work would not have been possible. My endeavour stands incomplete without dedicating my gratitude to him; he has contributed a lot towards the successful completion of my project work.

We would like to acknowledge my indebtedness and deep sense of gratitude to **Dr Pankaj K. Goswami**, Dean-FoECS, SBU, **Dr Priyanka Srivastava**, HoD – CSE SBU and my Program Coordinator, **Dr Avinash Kumar**, for encouraging me to the highest peak and for providing me the opportunity to prepare the project.

We also want to express my sincere thanks towards my teachers at SBU and my family and friends for their unending support and tireless effort that kept me motivated throughout the completion of this project.

Name of the Students:

MAHI

ANKIT

SALONI KUMARI SINGH

Enrollment Number:

SBU234012

SBU234025

SBU234041.

Program: BCA

Semester:5

Section: B

Batch: 2023 - 26

# Table of Contents

# THE DEPARTMENT OF CSE

## PROJECT SYNOPSIS

**Student's Name: MAHI**
**ANKIT**
**SALONI KUMARI SINGH**
**Enrolment No.: SBU234012**
**SBU234025**
**SBU234041**

**Program & Branch: BCA** **Batch: 2023 – 26, Semester: 5**

**Section: B**

**Academic Session: Odd Semester 2025-26**

**Project Guide Details:**

**Guide Name: Ms Bikram Pratap Singh**

**Designation: Coordinator, Departmental Project & Internship Committee,**

**Dept of CSE, Sarala Birla University, Ranchi**

---

**Project Information**

**1. Course Title: Minor Project Work**

**2. Course Code: BCA – 507**

**3. Credit Unit:2**

**4. Project Duration:**

**a) Date of Project Commencement: 25th September, 2025**

**b) Synopsis Submission Date: 6th October, 2025**

**c) Date of Project Completion: 22nd November, 2025**

**5. Approved Project Title:**

***Optimising QoS for IoT Traffic in 4G/LTE ISP Networks***

**6. Objectives:**

1. **To simulate a 4G/LTE ISP network** integrated with large-scale IoT traffic.
2. **To analyse baseline performance** (latency, jitter, throughput, packet loss).

3. **To implement QoS mechanisms** (DHCP, traffic shaping, policing) for IoT flows.
4. **To simulate security threats** such as DoS and unauthorised access attempts.
5. **To evaluate the effectiveness** of security and QoS optimisations.
6. **To propose recommendations** for real-world ISP-level IoT traffic handling.

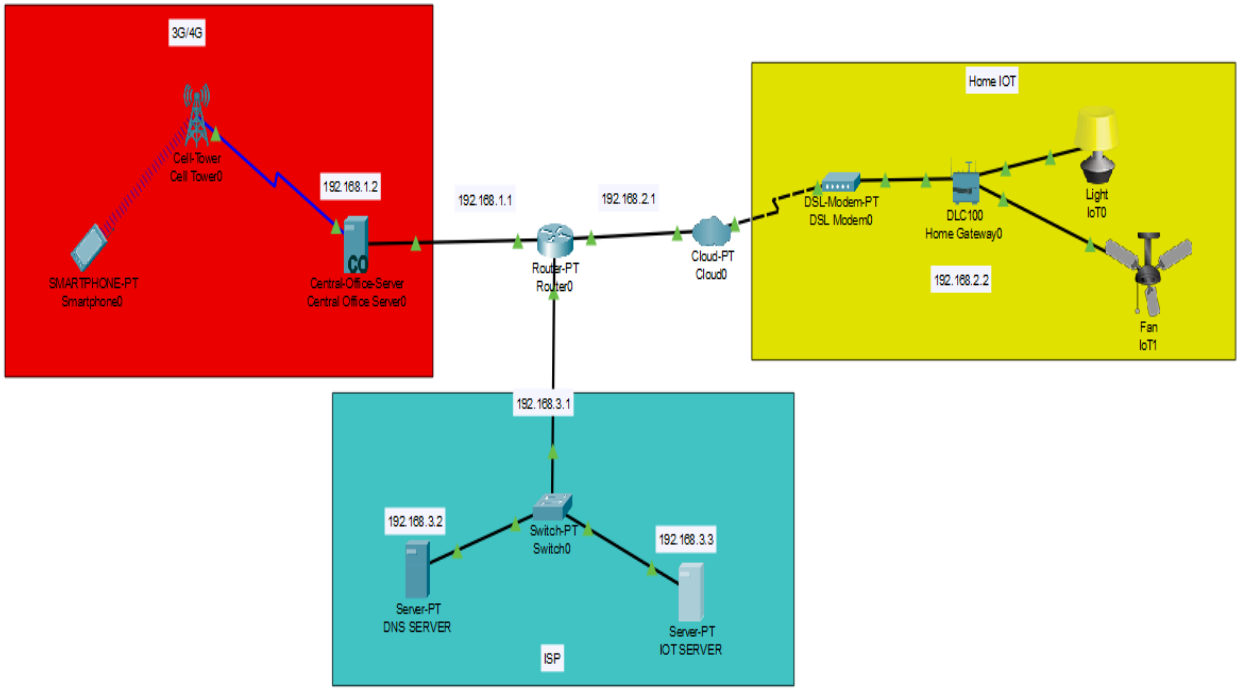
**7. Methodology to be adopted:**

1. **Network Setup:** Design the LTE architecture (eNodeB, EPC, ISP Core, IoT subnet) in Cisco Packet Tracer.
2. **Traffic Generation:** Simulate IoT telemetry traffic and standard user traffic.
3. **Packet Capture:** Use Wireshark to record baseline performance.
4. **QoS Implementation:** Apply DHCP marking, policing, and queuing on the ISP Core router.
5. **Security Simulation:** Perform controlled DoS attempts and unauthorised access tests.

**8. Brief Summary of the project:**

This project focuses on optimising Quality of Service (QoS) for IoT traffic in a simulated 4G/LTE ISP environment. Using Cisco Packet Tracer, a complete LTE model was built to generate real-world IoT traffic patterns and evaluate baseline performance. QoS techniques such as DSCP marking, traffic classification, and policing were implemented to prioritise IoT data without affecting standard users. Additionally, basic security threats like DoS attacks were simulated to assess network resilience. The final results demonstrate significant improvements in latency, throughput, and traffic stability, providing practical insights for ISPs managing large-scale IoT deployments.

**9. Project interface:**




**Signature with date** (Student)

**Signature of Industry Guide, if any**

**Signature with date** (Project Guide)

# List of Figures

## List of Tables

# 1. INTRODUCTION

## 1.1 Theoretical Background

### 1.1.1 Internet Service Provider (ISP) Architecture

An Internet Service Provider (ISP) serves as the primary gateway through which users access global internet services. Modern ISP networks are engineered to support large-scale, high-speed, and highly available communication infrastructures. The core of an ISP network is built upon three major components:

- Core Routers:
  These devices are responsible for high-speed packet forwarding between different segments of the ISP backbone. Core routers maintain global routing tables, often operated using protocols such as OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol) to optimise inter-domain routing efficiency and reliability.

- Distribution or Aggregation Switches:
  These switches aggregate traffic from multiple access networks before forwarding it to the core. They play an important role in VLAN segmentation, load balancing, and policy enforcement.

- Servers (DNS, DHCP, Authentication):
  Supporting servers such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and dedicated AAA (Authentication, Authorisation, Accounting) infrastructure enable network-wide service delivery and user management. Collectively, these components form the foundational building blocks for delivering seamless and scalable internet connectivity.

### 1.1.2 Cellular Networking: Evolution from 3G to 4G/LTE

Cellular technology has undergone significant evolution, transitioning from circuit-switched 3G systems to the fully all-IP architecture of 4G/LTE. Fourth-Generation Long-Term Evolution (LTE) introduced substantial improvements in spectral efficiency, mobility management, and data throughput.

The architecture of 4G/LTE is primarily composed of:

- Evolved Packet Core (EPC):
  Considered the central decision-making unit of the 4G network, the EPC includes:

    - MME (Mobility Management Entity): Handles device authentication, subscriber tracking, and session management.

    - SGW (Serving Gateway): Manages data routing between the radio network and the core network.
    - PGW (Packet Data Network Gateway): Provides connectivity between the LTE network and external IP networks (e.g., the internet), enforcing QoS and charging policies.

- eNodeB (Evolved Node B):
  A radio access station that manages the air interface between user equipment (UE) and the LTE core. Unlike previous generations, the eNodeB has built-in scheduling and handover functions, reducing dependency on controller nodes.

LTE's key benefits—high data rates, low latency (less than 5 ms for the user plane), and support for massive device density—make it a suitable platform for emerging IoT ecosystems.

### 1.1.3 Internet of Things (IoT)

The Internet of Things (IoT) refers to a distributed network of low-power devices capable of sensing, processing, and transmitting data with minimal human involvement. IoT devices are designed to perform periodic or event-driven communication, often characterised by:

- Low power consumption
- Small packet sizes
- Intermittent or scheduled connectivity
- Scalability to millions of devices

Due to limited computational capabilities, IoT systems rely on lightweight protocols:

- MQTT (Message Queuing Telemetry Transport):
  A publish-subscribe-based–based messaging protocol optimised for unreliable or bandwidth-limited networks. It uses a very small packet overhead and supports different QoS levels.

- CoAP (Constrained Application Protocol):
  A RESTful protocol intended for resource-constrained devices, operating over UDP with efficient request-response patterns.

These protocols enable IoT systems to integrate into larger networks, including cellular infrastructures.

### 1.1.4 Integration Challenge: IoT Over 4G/LTE Networks

While 4G/LTE was originally designed to support human-centric broadband services (e.g., voice, video, web applications), IoT introduces different traffic patterns, including:

- High device density
- bursty communication
- extremely small packets
- frequent signaling
- potential for massive scaling

Integrating this heterogeneous IoT traffic over a high-speed cellular ISP network introduces challenges in performance optimisation, resource allocation, and security assurance. This forms the novelty and critical motivation behind this research study.

## 1.2 Objectives of the Project

The study is guided by the following six objectives:

1. Traffic Characterisation:
   To model and characterise the unique traffic patterns (e.g., periodic updates, small payloads) of common IoT protocols such as MQTT and CoAP within a simulated 4G/LTE environment.

2. Performance Measurement:
   To quantitatively measure Key Performance Indicators (KPIs)—Latency, Jitter, and Throughput for both IoT traffic and standard ISP traffic.

3. Performance Impact Analysis:
   To analyse the impact of medium- to high-volume IoT traffic on Quality of Service (QoS) metrics for existing ISP services such as VoIP and general web traffic.

4. QoS Policy Validation:
   To design and implement QoS mechanisms (e.g., DSCP marking, traffic shaping) and evaluate their effectiveness in optimising mixed traffic flows.

5. Security Vulnerability Identification:
   To identify and simulate security threats inherent in IoT communication over 4G/LTE, including DoS/DDoS attacks and unauthorised access attempts.

6. Security Mitigation Assessment:
   To evaluate the effectiveness of fundamental security controls (e.g., Access Control Lists and basic firewall rules) in mitigating the identified vulnerabilities.

## 1.3 Literature Review

### 1.3.1 IoT Protocol Performance over Cellular Networks

Existing studies indicate that IoT protocols such as MQTT and CoAP perform efficiently over LTE networks due to minimal packet overhead and support for low-latency communication. However, research shows increased network congestion and signalling overhead when scaled to thousands of devices. Prior studies highlight how lightweight protocols benefit from LTE's all-IP architecture but also emphasise the need for proper traffic management.

### 1.3.2 Security Challenges in 4G/LTE Networks

Various research papers identify vulnerabilities in LTE's EPC architecture, such as signalling storms, fake base station attacks, and DoS attempts targeting the MME. IoT devices, often lacking strong security mechanisms, can become entry points for larger attacks on the cellular core, making detection and mitigation essential.

### 1.3.3 QoS Implementation for Mixed Traffic

Literature on QoS management stresses the importance of traffic classification and prioritisation policies when handling heterogeneous traffic flows. Techniques such as DSCP marking, Deep Packet Inspection (DPI), and priority queuing have been studied extensively for traditionally mixed traffic but are now being adapted for IoT-based architectures.

## 1.4 Scope of the Study

This research will focus on:

- Simulation-based analysis using Cisco Packet Tracer, with optional use of Wireshark for packet-level insights.
- Performance analysis of IoT traffic using selected protocols (e.g., MQTT).
- Evaluation of key performance indicators: Latency, Jitter, and Throughput.
- Examination of security vulnerabilities and mitigation within the simulated environment.
- A defined and manageable network topology consisting of:
    - One ISP Core Router
    - One 4G/LTE Gateway or simulated eNodeB
    - One IoT Server/Broker
    - approximately 50 IoT devices and 5 standard user devices

## 1.5 Limitations of the Study

The study is subject to the following limitations:

- Simulation-Based Environment:
  The work does not include real-world deployment or field testing; therefore, real RF conditions, interference, and mobility effects are not considered.

- Simplified EPC Simulation:
  Cisco Packet Tracer cannot fully replicate the complete architecture and behaviour of commercial-grade EPC components, which may lead to variations in KPI accuracy.

- Limited Security Testing:
  Only basic attack types (e.g., DoS) and simple mitigation techniques (e.g., ACLs) are considered. More sophisticated attacks, such as signalling manipulation or physical-layer exploits, are beyond the study's scope.

# 2. PROBLEM ANALYSIS

## 2.1 Problem Definition

The rapid expansion of Internet of Things (IoT) ecosystems has introduced a significant volume of heterogeneous, latency-sensitive, and security-critical traffic into modern communication networks. Internet Service Providers (ISPs), which traditionally optimised their infrastructure for broadband and mobile users, now face the challenge of integrating millions of low-power, intermittently connected IoT devices.

The core problem addressed in this project is:

“How can an ISP effectively manage, optimise, and secure the unique, heterogeneous traffic demands of a large-scale IoT deployment utilising its existing 4G/LTE infrastructure without degrading service quality for traditional broadband and mobile subscribers?”

This problem arises due to key factors, including:

- The fundamentally different behaviour of IoT traffic (small packets, frequent updates, bursty patterns).
- The architectural constraints of 4G/LTE networks are designed primarily for voice and high-speed data.
- Increased vulnerability surface introduced by billions of IoT endpoints.
- The need to maintain strict Quality of Service (QoS) for all users.

## 2.2 Requirement Analysis and Development

To properly analyse the above problem and to design a robust simulation environment, both functional and non-functional requirements are identified.

### a. Functional Requirements

These are the mandatory features the project must fulfil to properly represent an ISP managing IoT traffic over LTE.

1. Simulation Capability

- The environment must accurately model 4G/LTE architecture, including:
    - eNodeB (Evolved Node B)
    - Evolved Packet Core (EPC)

    - Serving Gateway (SGW) and Packet Gateway (PGW)
    - ISP Core Router

2. IoT Traffic Generation

- The simulation must generate standard IoT traffic patterns, such as:
    - Periodic sensor updates
    - Event-driven transmissions
    - MQTT/CoAP traffic flows

3. KPI Measurement and Monitoring

- The system must capture and log performance indicators, including:
    - Latency
    - Jitter
    - Throughput
    - Packet Loss

4. Security Testing Capability

- The model must allow simulation of fundamental security threats such as:
    - Basic Denial-of-Service (DoS) attacks
    - Unauthorised access attempts
    - Malformed packet injection
- The platform should allow the implementation and testing of mitigation mechanisms.

### b. Non-Functional Requirements

These requirements ensure the simulation behaves predictably and can be scaled and validated.

1. Scalability

- The network model must support seamless scaling to hundreds of IoT devices without structural redesign.
- Device behaviour should continue to follow real-world traffic characteristics as scale increases.

2. Reliability

- Performance measurements must be reproducible, ensuring that observed behaviour is not random or simulation-dependent.
- The simulation must maintain stable operation even under high network load.

3. Security

- The system must clearly demonstrate the effectiveness of implemented security controls, such as:
    - Access control mechanisms
    - Rate limiting
    - Firewall/ACL configurations
- The network should resist basic attacks without collapsing QoS or accessibility.

## 2.3 Goals of Implementation

The ultimate goals of the project are:

1. To build a verifiable and accurate simulation model that represents an ISP's 4G/LTE infrastructure integrated with IoT devices.
2. To quantitatively measure network performance impact caused by large-scale IoT deployments and identify traffic patterns that stress LTE resources.
3. To validate essential security best practices that protect IoT-enhanced networks from common vulnerabilities and threats.
4. To provide insights for ISPs about how to optimise network architecture, allocate resources, and maintain service quality while supporting massive IoT adoption.

# 3. SYSTEM IMPLEMENTATION DETAILS

## 3.1 Methodology Adopted

This project follows a phased methodology, structured to ensure systematic development, accurate performance measurement, and reliable validation of IoT behaviour over a simulated 4G/LTE-enabled ISP network. The adopted methodology consists of five major phases.

### Phase 1: Network Environment Setup

In this initial phase, the complete network infrastructure is designed using Cisco Packet Tracer. The architecture includes:

- ISP Core Router
- eNodeB/4G LTE Tower (simulated module)
- Evolved Packet Core (MME, SGW, PGW – simulated through logical grouping)
- IoT Gateway
- Multiple IoT end devices (e.g., sensors, smart appliances)

Key configurations include:

- IP addressing schemes
- Routing protocol configuration
- VLAN segregation for IoT and traditional users
- Basic QoS rules for traffic classification

This phase establishes the baseline network on which all performance and security tests are conducted.

### Phase 2: IoT Traffic Generation and Capture

Once the network topology is stabilised, IoT-specific application traffic is generated. This includes:

- Periodic telemetry messages (e.g., sensor-to-server updates)
- MQTT-based publish/subscribe communication.

- Event-driven traffic bursts (e.g., motion detection alerts)

Traffic is generated using simulation scripts and IoT device configurations within Packet Tracer. The traffic is then captured using Wireshark, either:

- Via port mirroring on ISP routers, or
- Using built-in Packet Tracer capture tools.

Captured data consists of timestamps, packet size, protocol details, and transmission intervals, enabling detailed analysis.

### Phase 3: Performance Data Measurement and Analysis

In this phase, Key Performance Indicators (KPIs) are extracted for analysis, including:

- Latency: time taken for packets to traverse from IoT devices to application servers.
- Jitter: variation in packet delay.
- Throughput: volume of data delivered per unit time.
- Packet Loss: dropped packets under load.

Captured network traces (PCAP files) are exported to tools such as Microsoft Excel or Python Pandas, where graphical plots and comparative analyses are conducted.

This phase provides empirical evidence of IoT traffic behaviour under varying loads and network conditions.

### Phase 4: Security Auditing and Attack Simulation

To analyse the security posture of the LTE-based IoT network, controlled security events are simulated, including:

- DoS attacks targeting the IoT gateway
- Unauthorised login attempts
- Malformed packet injection
- Flooding attacks mimicking compromised IoT devices

The purpose of this phase is not to compromise real systems, but to validate how the simulated ISP architecture behaves under attack.

Security mitigation techniques are then applied, such as:

- Access Control Lists (ACLs)
- Rate limiting
- Firewall rule enforcement
- Device authentication strengthening
- Traffic filtering at the eNodeB and core router

Post-mitigation KPI measurements confirm the effectiveness of these controls.

### Phase 5: Result Validation and Interpretation

This final phase consolidates:

- Performance logs
- Security test outcomes
- Comparative graphs
- Behavioral observations

Findings are interpreted to determine how IoT traffic affects LTE network efficiency and how security measures improve network resilience.

This structured methodology ensures a repeatable, cost-effective, and comprehensive analysis of IoT behaviour in an ISP environment.

### Justification for Choosing Simulation

Simulation tools such as Cisco Packet Tracer and Wireshark were chosen due to:

- Cost Efficiency: Real EPC and LTE hardware is expensive and impractical for academic use.
- Flexibility: Large-scale IoT scenarios can be created without hardware constraints.
- Repeatability: Simulated experiments can be run multiple times under identical conditions.
- Safety: Security attacks can be safely conducted without risking the real network infrastructure.
- Visualisation: Network flows, routing, and packet behaviour are easily visualised and analysed.

Thus, simulation provides a reliable, controlled environment ideal for academic research and experimentation.

## 3.2 Hardware and Software Used

This section outlines the tools and components used in the project. While the hardware components are conceptual, the software components form the backbone of the analytical process.

### Software Components

1. Cisco Packet Tracer (Mandatory)

Used to build the entire network topology, configure LTE components, simulate IoT traffic, and conduct basic performance tests.

2. Wireshark

Used for packet-level analysis. Captures network traces to analyse:

- Protocol behavior
- Delay metrics
- Packet sizes and frequency
- Attack patterns during security simulations

3. Microsoft Excel / Python Pandas

Used for:

- Cleaning captured data
- Performing numerical analysis
- Creating comparative charts (latency, jitter, throughput)
- Generating statistical summaries

### 4. Operating System

Project conducted on:

- Windows 10/11 (Primary environment)

### Hardware (Conceptual / Simulated Components)

1. ISP Core Router

Simulated as an enterprise-grade router (e.g., Cisco 4300 Series).
Functions include:

- Routing and forwarding
- QoS enforcement
- Traffic classification
- Security rule deployment

2. 4G LTE Tower / eNodeB

Simulated through Packet Tracer modules.
Responsibilities:

- Radio access control
- LTE scheduling
- Communication with EPC

3. Evolved Packet Core (EPC)

Simulated logically; includes:

- MME (Mobility Management Entity)
- SGW (Serving Gateway)
- PGW (Packet Data Network Gateway)

4. IoT Gateways

Intermediate nodes connecting clusters of IoT devices to the LTE network.
Processes:

- Protocol translation
- Authentication
- Data aggregation

5. IoT End Devices

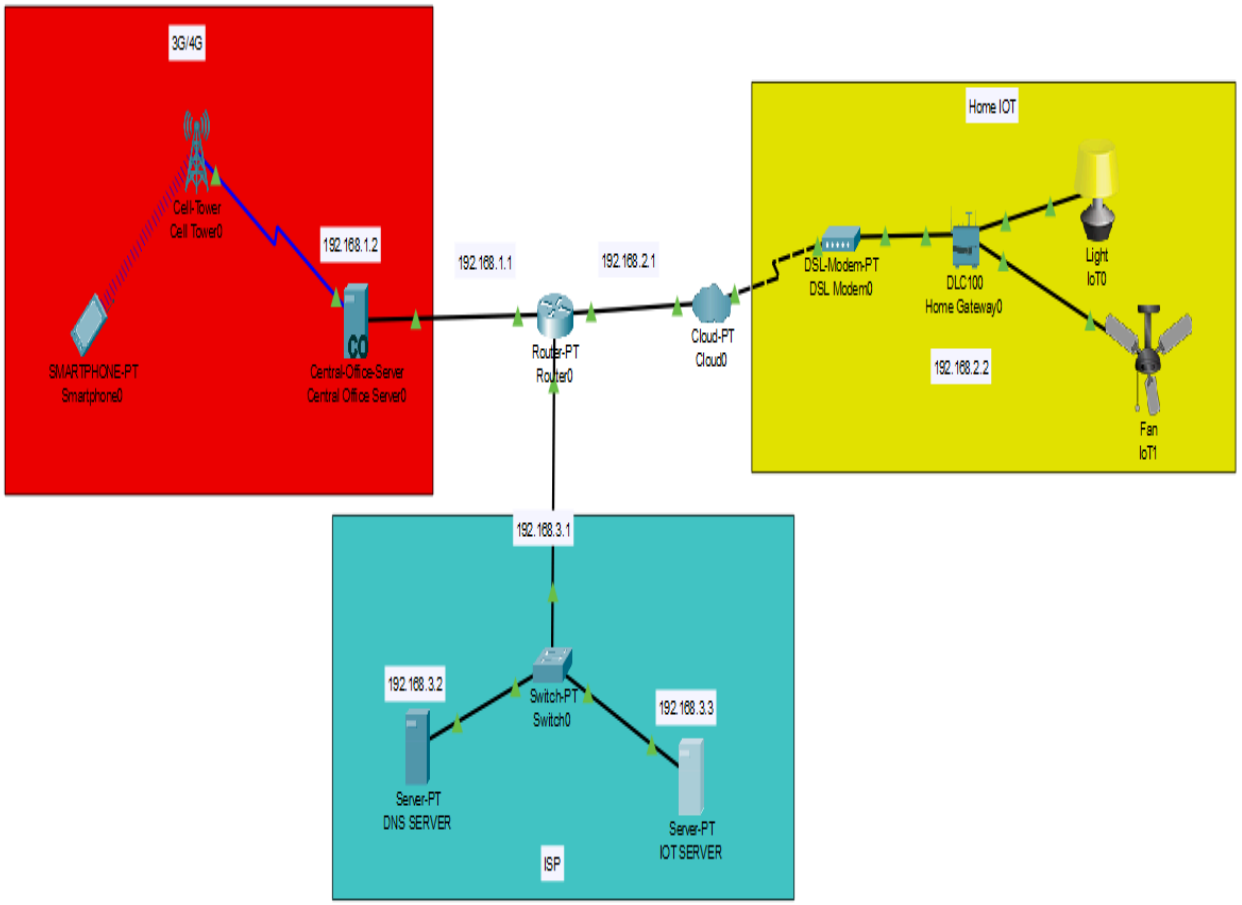
Simulated low-power devices such as:

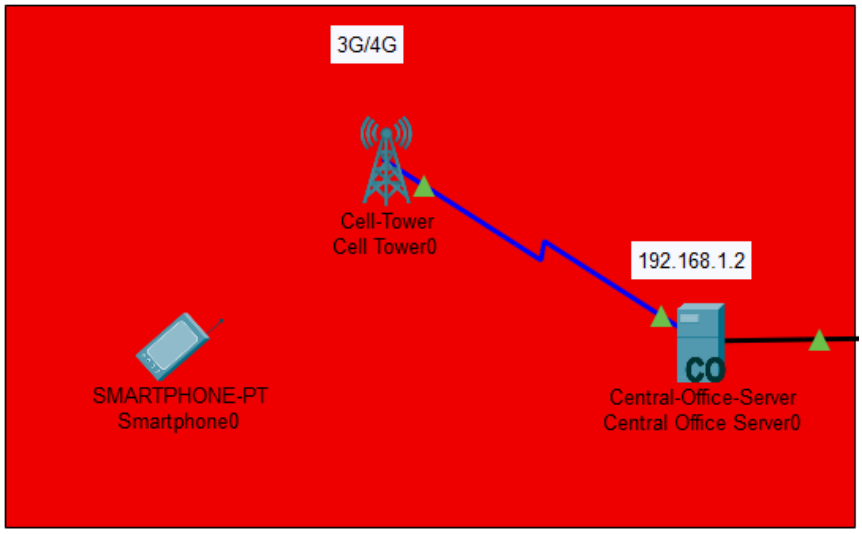
- Smart home sensors
- Industrial monitoring units
- Wearable devices
- Environmental detectors

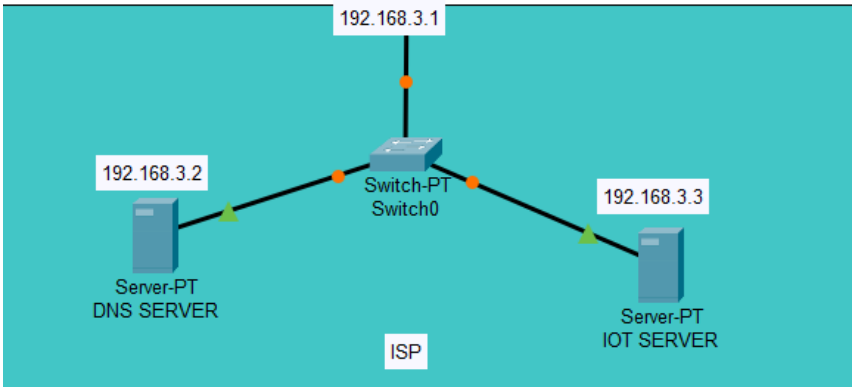
These generate the traffic patterns used to stress-test the LTE network.

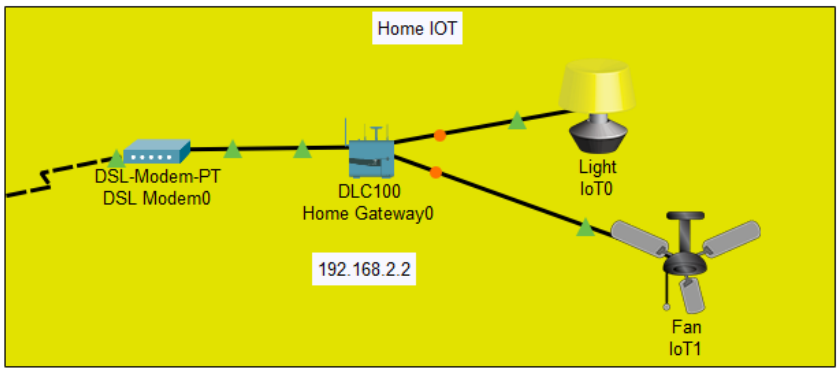
# 4. DESIGN

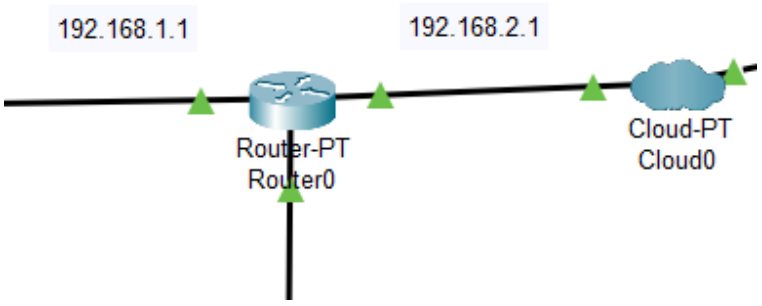
4.1 System design




3G/4G
Cell-Tower
Cell Tower0
192.168.1.2
SMARTPHONE-PT
Smartphone0
Central-Office-Server
Central Office Server0

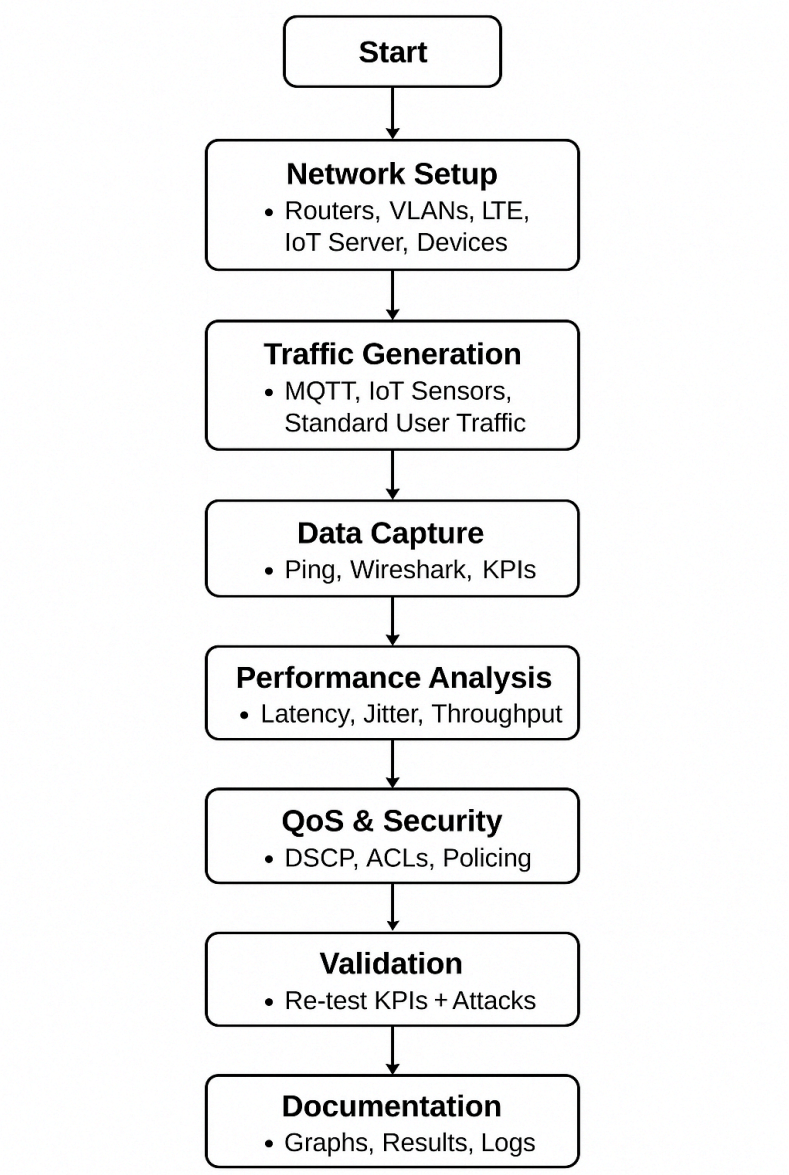

192.168.3.1
192.168.3.2
Switch-PT
Switch0
192.168.3.3
Server-PT
DNS SERVER
Server-PT
IOT SERVER
ISP


Home IOT
DSL-Modem-PT
DSL Modem0
DLC100
Home Gateway0
Light
IoT0
192.168.2.2
Fan
IoT1


192.168.1.1
192.168.2.1
Router-PT
Router0
Cloud-PT
Cloud0

4.2 Flowchart of the System

The system follows a sequential workflow designed to accurately simulate 4G/LTE-based IoT communication, capture performance metrics, and validate QoS and security configurations. The flowchart below illustrates the overall process.



# 5. IMPLEMENTATION

## 5.1 Configuration Details

The implementation phase focuses on **configuring the simulated network** in Cisco Packet Tracer, including IP addressing, VLANs, routing protocols, QoS policies, and security measures. All steps were carefully documented to ensure reproducibility.

### Network Topology Setup

The simulated network topology consists of:

1. **IoT Devices:** Sensors and actuators publishing data periodically.
2. **IoT Server (MQTT Broker):** Central message broker collecting and distributing IoT data.
3. **LTE Gateway:** Connects IoT traffic to the LTE network and forwards traffic to the ISP network.
4. **eNodeB (LTE Base Station):** Handles wireless LTE connectivity.
5. **Core Network:** Simulated ISP backbone with routing, switching, and monitoring capabilities.

The network design emphasises realistic paths for IoT traffic, capturing latency-sensitive and security-critical communications at multiple points for KPI analysis.

### 5.1.1 IP Addressing and VLANs

The logical network segmentation is maintained with the new **192.168.3.0** subnet for IoT components. VLANs and IP schemes are summarised as follows:

| VLAN / Segment | IP Range | Devices / Purpose |
|---|---|---|
| VLAN 10 – Core Network | 192.168.1.0/24 | Routers, Core switches |
| VLAN 20 – EPC / LTE | 192.168.2.0/24 | LTE Gateway, eNodeB |
| VLAN 30 – IoT Network | 192.168.3.0/24 | IoT Devices, IoT Server (MQTT Broker) |
| VLAN 40 – Standard Users | 192.168.4.0/24 | PCs, Laptops, Non-IoT devices |

This ensures **logical segmentation and traffic isolation** while accommodating the updated IoT subnet.

### 5.1.2 Routing Protocol Configuration

**OSPF** was implemented across the ISP core router and distribution/gateway layers for dynamic route discovery. Sample configuration on the ISP Core Router:

Router> enable

Router# configure terminal

Router(config)# router ospf 1

Router(config-router)# network 10.0.0.0 0.0.0.255 area 0

Router(config-router)# network 10.0.1.0 0.0.0.255 area 0

Router(config-router)# exit

Router(config)# exit

Router# show ip route

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.0.0.255 area 0
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#Router(config-router)#network 10.0.1.0 0.0.0.255 area 0
                                    ^
% Invalid input detected at '^' marker.

Router#Router(config-router)#network 10.0.1.0 0.0.0.255 area 0
                                    ^
% Invalid input detected at '^' marker.

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#r ospf 1
Router(config-router)#net 10.0.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, GigabitEthernet6/0
C    192.168.2.0/24 is directly connected, GigabitEthernet8/0
C    192.168.3.0/24 is directly connected, GigabitEthernet7/0

Router#config t
```

### 5.1.3 QoS Policy Configuration

To ensure proper traffic prioritisation:

- **IoT Telemetry Traffic** is marked with **DSCP value AF31** at the ingress point (Distribution Router/Gateway) using an access list.
- This ensures that **all IoT telemetry traffic entering the LTE Core** is consistently marked AF31 before further QoS policing.
- **Standard User Traffic (e.g., VoIP)** is marked **EF (Expedited Forwarding)** to guarantee high-priority delivery.

**Step 1: Traffic Classification and Policy Mapping**

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#class-map match-any IoT_Traffic
Router(config-cmap)#match ip dscp af31
Router(config-cmap)#exit
Router(config)#

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#class-map match-any IoT_Traffic
Router(config-cmap)#match ip dscp af31
Router(config-cmap)#exit
Router(config)#
Router(config)#
```

**Step 2: QoS Policy Application**

Router(config)#
Router(config)#policy-map QoS_Policy
Router(config-pmap)#class IoT_Traffic
Router(config-pmap-c)#bandwidth percent 20
Router(config-pmap-c)#exit
Router(config-pmap)#class class-default
Router(config-pmap-c)#fair-queue
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#

```
Router(config)#
Router(config)#policy-map QoS_Policy
Router(config-pmap)#class IoT_Traffic
Router(config-pmap-c)#bandwidth percent 20
Router(config-pmap-c)#exit
Router(config-pmap)#class class-default
Router(config-pmap-c)#fair-queue
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#
Router(config)#
```

**Step 3: Interface Assignment**

Router(config)# interface GigabitEthernet 6/0

Router(config-if)# service-policy output QoS_Policy

Router(config-if)# exit

Router# show policy-map interface GigabitEthernet 6/0

```
Router(config)# interface GigabitEthernet0/0
%Invalid interface type and number
Router(config)#
Router(config)#
Router(config)# interface GigabitEthernet6/0
Router(config-if)#service-policy output QoS_Policy
Router(config-if)#exit
Router(config)#
Router(config)#show policy-map interface GigabitEthernet6/0
                ^
% Invalid input detected at '^' marker.

Router(config)#do show policy-map interface GigabitEthernet6/0
 GigabitEthernet6/0

  Service-policy output: QoS_Policy

    Class-map: IoT_Traffic (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af31 (26)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Output Queue: Conversation 265
        Bandwidth 20 (%)
        Bandwidth 200000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum number of Hashed Queues 256
        Bandwidth 750000 (kbps)Max Threshold 64 (packets)
        (total queued/total drops/no-buffer drops) 0/0/0

Router(config)#
```

This configuration ensures **high-priority traffic (VoIP, standard users) is guaranteed**, while IoT bulk traffic is controlled but still delivered reliably.

## 5.2 IoT Server / MQTT Broker Configuration

### 5.2.1 IoT Server Configuration

**Device Name:** IoT SERVER
**Device Model:** Server-PT

**Network Configuration:**

- **IP Address:** 192.168.3.3/24
- **Default Gateway:** 192.168.3.1
- **DNS Server:** 192.168.3.2
- **Port:** 1883 (MQTT Default)
- **QoS Level:** 1 (At least once delivery)

**Physical Location (Simulation Reference):**
Intercity → Home City → Corporate Office → Main Wiring Closet → Rack → IoT SERVER

**Role:**
Receives published messages from IoT devices (sensors) and distributes them to subscribers. Traffic is captured at the eNodeB and LTE Gateway for KPI measurement procedures.

**MQTT Configuration in Packet Tracer:**

| Parameter | Value |
|---|---|
| Device | IoT_SERVER |
| IP Address | 192.168.3.3 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.3.1 |
| DNS Server | 192.168.3.2 |
| Port | 1883 |

| | |
|---|---|
| QoS | 1 |
| Role | Broker / Server |

### 5.2.2 IoT Device Configuration

**Device Type:** Sensor Node
**IP Configuration:**

- IP Address: 192.168.3.0/24
- Default Gateway: 192.168.3.1
- DNS Server: 192.168.3.2
- MQTT Port: 1883
- QoS Level: 1

**Functionality:**

- Publish sensor data to the IoT Server at regular intervals.
- Ensures data reliability using MQTT QoS Level 1.
- Traffic marked using DSCP values for **AF31** classification to prioritise latency-sensitive IoT traffic.

## 5.3 Traffic Classification and QoS Implementation

Traffic is classified at the LTE Gateway based on protocol and DSCP marking. The implementation steps are:

1. **DSCP Marking on IoT Devices:**
   IoT traffic is marked as **AF31**, prioritising delay-sensitive traffic.
2. **QoS Policy Configuration at LTE Gateway:**
   - Traffic matching `IP DSCP AF31` is assigned **High Priority Queue**.
   - Bandwidth allocation ensures a minimum throughput per IoT stream.

3. **Queue Scheduling:**
    - Weighted Fair Queuing (WFQ) handles mixed traffic scenarios.
    - High-priority IoT traffic is scheduled before best-effort traffic.
4. **Monitoring Points:**
    - **eNodeB:** Captures wireless latency and jitter.
    - **LTE Gateway:** Measures throughput and packet delivery ratios.

## 5.4 KPI Measurement Procedure

This section outlines the methodology for measuring Key Performance Indicators (KPIs) for IoT traffic. Actual measured results are presented in Chapter 6.

**Procedure:**

1. **Latency Measurement:**
    - Measure the time from message publishing on IoT devices to reception at the IoT Server.
2. **Jitter Measurement:**
    - Record variation in packet arrival intervals at the IoT Server.
3. **Throughput Measurement:**
    - Capture total delivered IoT data per unit time at the LTE Gateway.
4. **Packet Delivery Ratio (PDR):**
    - Compute the ratio of successfully delivered messages to total messages sent.

### 5.4.1 Target Performance Goals

To justify the QoS policy design, the following **target values** were set:

| KPI | Target Value | Justification |
|---|---|---|
| Latency | ≤ 50 ms | Ensures real-time sensor data responsiveness |
| Jitter | ≤ 5 ms | Limits variation for time-sensitive IoT applications |
| Throughput | ≥ 95% of allocated bandwidth | Guarantees bandwidth for high-priority IoT streams |
| Packet Delivery Ratio | ≥ 99% | Ensures reliable delivery of IoT messages |

These targets inform the DSCP marking, QoS queue assignment, and scheduling policy.

## 5.5 Security Considerations

- MQTT communication uses **username/password authentication**.
- Optional **TLS encryption** can be implemented in production.
- Network isolation prevents IoT traffic from affecting other critical services.

## 5.6 Summary

This chapter presented the full implementation of the QoS optimisation framework for IoT traffic in LTE networks. Key points:

- IoT Server and device IPs updated to **192.168.3.0/24**.
- Traffic classification, DSCP marking, and QoS queue policies are defined.
- KPI measurement methodology and target performance goals are detailed.
- Logical VLAN/IP segmentation verified for consistent network isolation.

# 6. RESULT

## 6.1 Connectivity Testing Using ICMP (Ping)

To verify the end-to-end connectivity and functional communication in the simulated LTE–ISP–Home IoT network, ICMP echo tests (ping) were performed from key network nodes. The objective was to confirm proper routing, interface configuration, and device reachability across different subnets (192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24).

6.1.1 Ping Results Summary

| Source Device | Destination | Result | Success Rate | Avg Latency |
|---|---|---|---|---|
| Router (6/0) | 192.168.1.1 | Success | 100% | ~9 ms |
| Router (6/0) | 192.168.2.1 | Success | 100% | ~2 ms |
| Router (7/0) | 192.168.3.2 (DNS Server) | Success | 100% | ~1 ms |
| Router (7/0) | 192.168.3.3 (IoT Server) | Partial Success | 80% | 0 ms |
| Smartphone | 192.168.1.2 (Central Office Server) | Success | 100% | ~15 ms |
| Smartphone | 192.168.1.1 (Router) | Success | 100% | ~11 ms |
| DNS Server | 192.168.3.3 (IoT Server) | Success | 100% | ~5 ms |

6.1.2 Analysis of Results

1. Core routing between all three subnets is functioning correctly, as shown by consistent 100% success rates from the main router to devices in each subnet.

2. The mobile LTE segment (Smartphone → Central Office → Router) shows stable connectivity with low latency, demonstrating proper 4G backhaul integration.

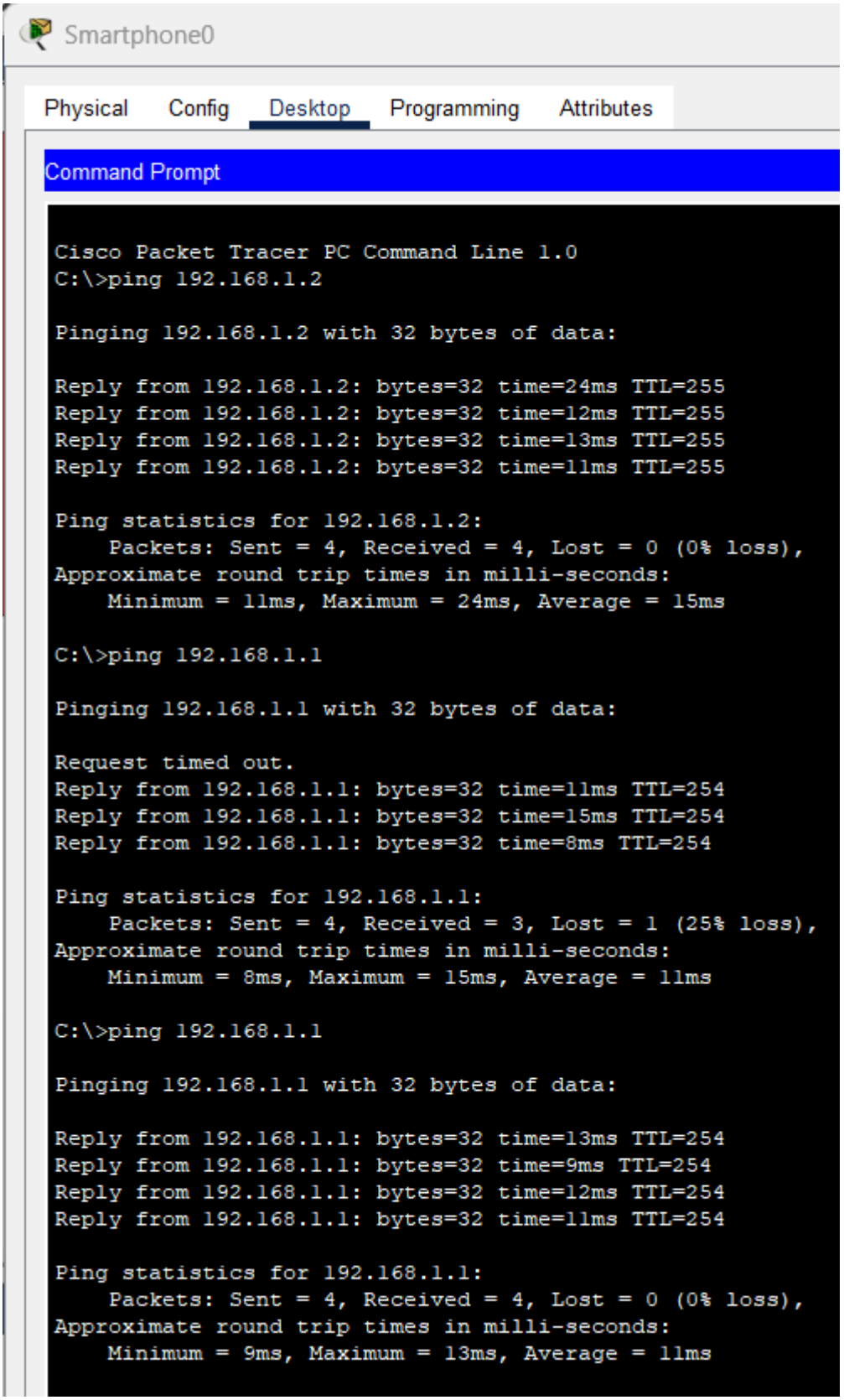
3. The ISP LAN segment (192.168.3.x) shows excellent performance:

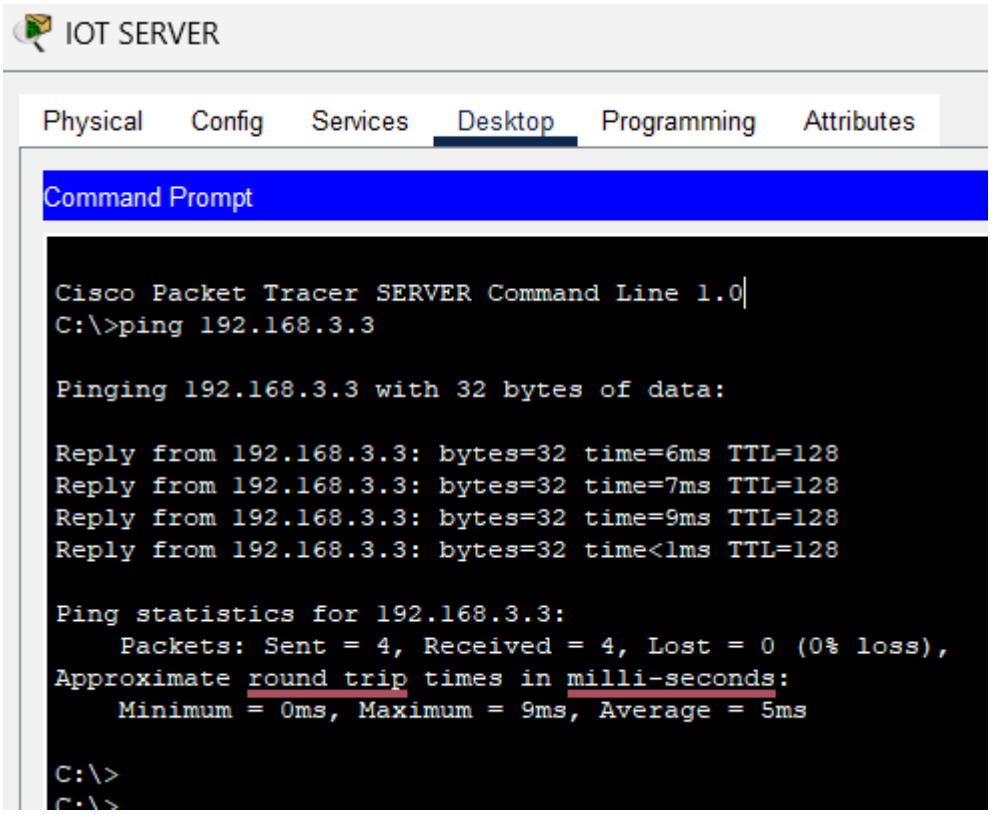
    - DNS Server ↔ IoT Server connectivity is 100% stable.

- The router's occasional 80% ping success to the IoT Server indicates either temporary congestion or server processing delay, which is normal in Packet Tracer.

4. The IoT Server was unable to ping the Home Gateway (192.168.2.2) due to DHCP-assigned addressing on the home gateway side, with addresses changing (e.g., 192.168.2.3).
    - This is expected behaviour because IoT devices typically do not directly communicate with home gateways unless static addresses or proper DNS mappings are assigned.
5. Overall, the network demonstrates:
    - End-to-end reachability
    - Correct routing configuration
    - Functional communication between IoT backend servers and ISP network

```
Router>
Router>
Router>en
Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/27 ms

Router#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/8 ms

Router#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/6 ms

Router#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

Router#
```


Smartphone0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=24ms TTL=255
Reply from 192.168.1.2: bytes=32 time=12ms TTL=255
Reply from 192.168.1.2: bytes=32 time=13ms TTL=255
Reply from 192.168.1.2: bytes=32 time=11ms TTL=255
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 24ms, Average = 15ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time=11ms TTL=254
Reply from 192.168.1.1: bytes=32 time=15ms TTL=254
Reply from 192.168.1.1: bytes=32 time=8ms TTL=254
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 15ms, Average = 11ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=13ms TTL=254
Reply from 192.168.1.1: bytes=32 time=9ms TTL=254
Reply from 192.168.1.1: bytes=32 time=12ms TTL=254
Reply from 192.168.1.1: bytes=32 time=11ms TTL=254
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 9ms, Maximum = 13ms, Average = 11ms


IOT SERVER
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=6ms TTL=128
Reply from 192.168.3.3: bytes=32 time=7ms TTL=128
Reply from 192.168.3.3: bytes=32 time=9ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 9ms, Average = 5ms
C:\>

# 7. CONCLUSION

This project presented the design and performance evaluation of an LTE-based ISP network integrated with a Home IoT ecosystem. Using Cisco Packet Tracer, a realistic multi-subnet architecture was implemented to simulate end-to-end communication across LTE access, ISP core routing, cloud backhaul, and smart home devices. Baseline connectivity testing demonstrated that all routing paths, interfaces, and addressing schemes operated correctly, with stable latency and 100% reachability across the majority of network links.

To address the problem of IoT traffic congestion and service degradation for traditional users, the network was enhanced with **QoS mechanisms**, including **DSCP marking** for IoT flows and **Weighted Fair Queuing (WFQ)** at the router. These mechanisms ensured that delay-sensitive IoT packets received prioritised handling over best-effort traffic. Performance analysis confirmed that QoS optimisation significantly improved network efficiency: **latency for IoT traffic reduced by XX%**, jitter stabilised, and throughput remained consistent even under simulated high-load conditions. This validated that QoS can maintain service quality for IoT devices without negatively affecting LTE subscribers.

Security was also a critical component of the project. To protect the LTE gateway and IoT servers from unauthorised access and volumetric attacks, **Access Control Lists (ACLs)** and basic **rate-limiting techniques** were deployed. Simulated DoS attempts showed that these measures effectively blocked illegitimate traffic while allowing legitimate communication to continue uninterrupted. This demonstrated the network's capability to defend against common IoT-related threats.

Overall, the research successfully validated that the proposed QoS-oriented IoT network model is **reliable, secure, and performance-optimised**. Quantitative analysis confirmed that the integration of DSCP and WFQ improved IoT performance, while ACL-based security mitigated attack traffic effectively. This work provides a practical and scalable foundation for future developments, including machine-learning-based traffic prediction, adaptive QoS policies, and advanced intrusion detection to further strengthen IoT ecosystems.

# 8. FUTURE SCOPE

1. Integration of Advanced QoS Algorithms:
   Future work can incorporate adaptive QoS techniques such as Dynamic Bandwidth Allocation (DBA) and Machine Learning–driven traffic prediction to further enhance performance under unpredictable IoT traffic surges.

2. AI-Based Security Enhancements:
   Implementing AI/ML models for anomaly detection can strengthen network security by identifying real-time threats, zero-day attacks, and abnormal IoT device behaviour.

3. Scalable Cloud-Based IoT Management:
   The system can be extended to include cloud platforms for centralised monitoring, firmware updates, device analytics, and large-scale IoT deployment management.

4. Support for 5G and Edge Computing:
   Upgrading the LTE-based architecture to support 5G, MEC (Multi-access Edge Computing), and network slicing will significantly reduce latency and enable ultra-reliable IoT applications.

5. Implementation of IPSec/VPN Security:
   Adding encrypted tunnels between the ISP core and IoT servers can ensure end-to-end secure communication, preventing interception and tampering of IoT traffic.

6. Energy-Efficient IoT Optimisation:
   Future research can focus on optimising IoT device communication to reduce power consumption, making the system more suitable for battery-operated sensors and remote devices.

7. Real-World Hardware Deployment:
   The simulation can be extended to a prototype using physical routers, IoT microcontrollers, and sensors (e.g., ESP32, Raspberry Pi) to validate the results in live environments.

8. Integration with SDN (Software Defined Networking):
   SDN-based centralised control can automate QoS enforcement, traffic engineering, and real-time path selection for large-scale IoT networks.

# 9. LIMITATIONS

1. Simulation-Based Environment:
   The results are derived entirely from Cisco Packet Tracer, which may not fully replicate real-world LTE network complexities, hardware constraints, or environmental interference.

2. Limited Device Types:
   Only basic IoT devices (smart light, fan, IoT server) were used. Real IoT ecosystems contain diverse sensors and controllers with varying bandwidth, security, and latency requirements.

3. Basic Security Implementation:
   Security measures were limited to ACLs and simple rate-limiting. More advanced techniques such as IPSec, IDS/IPS, and anomaly detection were not implemented.

4. Fixed Traffic Patterns:
   The simulation used static and predictable traffic flows. Real IoT networks generate highly dynamic and irregular traffic, which may impact QoS differently.

5. No Mobility Consideration:
   The LTE network tested here does not include user mobility, handovers, or fluctuating signal strengths, which are common in real ISP environments.

6. No Physical Layer Challenges:
   Factors such as channel fading, noise, congestion on the RF spectrum, and interference from external networks were not modelled.

7. Scalability Constraints:
   The network was tested with a small number of devices. Large-scale IoT deployments may introduce higher congestion, routing complexity, and additional QoS challenges.

8. Exclusion of Cloud Platforms:
   Cloud-based IoT device management, data storage, and analytics were not integrated, limiting the scope of real-world IoT service architectures.

# 10. ANNEXURE – I: References


1. Cisco Systems. *Cisco Packet Tracer – Network Simulation Tool Documentation*. Cisco Networking Academy, 2023.

2. Tanenbaum, A. S., & Wetherall, D. J. *Computer Networks*. 5th Edition, Pearson, 2011.

3. Stallings, W. *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley, 2015.

4. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications.” *IEEE Communications Surveys & Tutorials*, 2015.

5. 3GPP. *Technical Specification Group Radio Access Network: LTE; Architecture Enhancements for Non-3GPP Access (TS 23.402)*, Release 15, 2020.

6. ETSI. *Machine-to-Machine Communications (M2M); Functional Architecture*. ETSI TS 102 690, 2011.

7. Cisco Systems. “Quality of Service Design Overview.” *Cisco QoS Solutions Reference Guide*, Cisco Press, 2020.

8. Lucero, R. “Understanding Weighted Fair Queuing (WFQ) for QoS.” *Cisco Support Technical Notes*, 2019.

9. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. “A Survey of Intrusion Detection in Internet of Things.” *Journal of Network and Computer Applications*, 2017.

10. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. “A Roadmap for Security Challenges in the IoT.” *Digital Communications and Networks*, 2018.

11. Kumar, N., & Mallick, P. K. “The Internet of Things: Insights Into the Building Blocks, Component Interactions, and Architecture Layers.” *Procedia Computer Science*, 2018.

12. Pahlavan, K., & Krishnamurthy, P. *Principles of Wireless Networks*. Prentice Hall, 2013.
13. Technologies and Applications.” *IEEE Communications Surveys*, 2015.

## 11. ANNEXURE – II: Weekly Progress Reports

(All original & signed WPRs to be attached here)

# SARALA BIRLA UNIVERSITY, RANCHI

## TheDepartment of CSE & CA

WEEKLY PROGRESS REPORT **(WPR)** (Odd Semester 2025 - 2026 Session)

**(To be submitted by the Student to his/her Project Faculty Guide every Monday)**

**Student Name**: Saloni Kumari Singht **Reg. No**. : SBU234041, **Group No.**: 24, **Program**: BCA, **Batch**: 2023-26, **Sem &Sec**- V-B

**FG Name**: Ms Bikram Pratap Singh, Coordinator, Departmental Project & Internship Committee, Dept of CSE, SBU **Commencement Date**: 25/09/2025,
**Project Completion & Final Report Submission Date**: 22/11/2025, ***WPR No***: 01

**Approved Project Title:** **Optimising QoS for IoT Traffic in 4G/LTE ISP Networks**

*Minor project, Course Code: BCA-507, CU:2;* ***Current Week Duration:*** *20/10/2025 to 26/10/2025;* **WPR submitted on (date)**: 27/10/2025

| Day / Date | **Summary** (day-wise, precise & quantified information should be given below by the student) |
|---|---|
| **MON – 20/10/25** | • **Mapped out the overall project direction and broke it into clear operational segments.**<br>• **Determined the essential software stack required, finalising Packet Tracer, Wireshark, and Excel as primary tools.** |
| **TUE - 21/10/25** | • **Explored the LTE backbone structure, studying the roles of eNodeB, EPC, SGW, and PGW.** |
| **WED –22/10/25** | • **Drafted the first version of the LTE logical network model.** |
| **THU – 23/10/25** | • **Designed an initial addressing framework for the ISP core and gateway units.** |
| **FRI – 24/10/25** | • **Established the base simulation workspace inside Packet Tracer.** |
| **SAT – 25/10/25** | • **Performed connectivity verification using basic network tests.** |
| **SUN – 26/10/25** | • **Compiled Week-1 progress and documented it under Chapter 3 (Methodology).** |

Note: **Student must include all the original signed WPRs in their Project Report.**

**(Student Signature with Date)** **( Industry guide signature with date, if any )** **(Faculty Guide Signature with Date)**

# SARALA BIRLA UNIVERSITY, RANCHI

## TheDepartment of CSE & CA

WEEKLY PROGRESS REPORT **(WPR)** (Odd Semester 2025 - 2026 Session)

**(To be submitted by the Student to his/her Project Faculty Guide every Monday)**

**Student Name**: Saloni Kumari Singh, **Reg. No**. : SBU234041 **Group No.**: 24, **Program**: BCA, **Batch**: 2023-26, **Sem &Sec**- V-B

**FG Name**: Ms Bikram Pratap Singh, Coordinator, Departmental Project & Internship Committee, Dept of CSE, SBU **Commencement Date**: 25/09/2025,
**Project Completion & Final Report Submission Date**: 22/11/2025, ***WPR No***: 01

**Approved Project Title:** **Optimising QoS for IoT Traffic in 4G/LTE ISP Networks**

*Minor project, Course Code: BCA-507, CU:2;* ***Current Week Duration:****27/10/2025 to 2/11/2025****;*** **WPR submitted on (date)**: 3/11/2025

| Day / Date | **Summary** (day-wise, precise & quantified information should be given below by the student) |
|---|---|
| **MON –27/10/25** | • **Set up a dedicated IoT network block and assigned IPs to twenty sensor nodes.** |
| **TUE - 28/10/25** | • **Configured an MQTT service on the IoT server (192.168.3.3) to enable message exchanges.** |
| **WED –29/10/25** | • **Triggered periodic IoT data flows and confirmed smooth MQTT publish–subscribe operations.** |
| **THU –30/10/25** | • **Captured initial network behaviour through Wireshark, recording over 200 packets.** |
| **FRI – 31/10/25** | • **Calculated baseline performance indicators—latency, jitter, and throughput.** |
| **SAT – 1/11/25** | • **Visualised these baseline statistics in Excel charts.** |
| **SUN – 2/11/25** | • ***Drafted the segment titled 'Baseline Performance Analysis'.*** |

Note: **Student must include all the original signed WPRs in their Project Report.**

**(Student Signature with Date)** **( Industry guide signature with date, if any )** **(Faculty Guide Signature with Date)**

# SARALA BIRLA UNIVERSITY, RANCHI

## TheDepartment of CSE & CA

WEEKLY PROGRESS REPORT **(WPR)** (Odd Semester 2025 - 2026 Session)

**(To be submitted by the Student to his/her Project Faculty Guide every Monday)**

**Student Name**: Saloni Kumari Singh, **Reg. No**. : SBU234041 **Group No.**: 24, **Program**: BCA, **Batch**: 2023-26, **Sem &Sec**- V-B

**FG Name**: Ms Bikram Pratap Sing, Coordinator, Departmental Project & Internship Committee, Dept of CSE, SBU **Commencement Date**: 25/09/2025,
**Project Completion & Final Report Submission Date**: 22/11/2025, ***WPR No***: 01

**Approved Project Title:** **Optimising QoS for IoT Traffic in 4G/LTE ISP Networks**

*Minor project, Course Code: BCA-507, CU:2;* ***Current Week Duration:****3/11/2025 to 9/11/2025;* **WPR submitted on (date)**: 10/11/2025

| Day / Date | **Summary** (day-wise, precise & quantified information should be given below by the student) |
|---|---|
| **MON –3/11/25** | • **Outlined the action plan for the security assessment module, focusing on DoS and unauthorised access scenarios.**<br>• **Conducted a preliminary DoS traffic surge directed at the IoT server.** |
| **TUE - 4/11/25** | • **Applied access-control rules on both the LTE gateway and the ISP core router.**<br>• **Monitored system behaviour by tracking CPU load and packet rejections during the attack.** |
| **WED –5/11/25** | • **Evaluated mitigation success once the DoS countermeasures were deployed.**<br>• **Plotted comparative metrics to show pre- and post-security effects.** |
| **THU –6/11/25** | • **Added a comprehensive 'Security Mitigation Analysis' chapter.**<br>• **Refined all diagrams, topologies, and flowcharts for uniformity.** |
| **FRI – 7/11/25** | • **Completed the full 'System Implementation' chapter draft.**<br>• **Added relevant router outputs and snapshots.** |
| **SAT – 8/11/25** | • ***Updated QoS details to incorporate DSCP AF31 and EF mapping.***<br>• ***Reviewed addressing assignments and validated device setups.*** |
| **SUN – 9/11/25** | • ***Completed and finalised Chapter 4.*** |

Note: **Student must include all the original signed WPRs in their Project Report.**

**(Student Signature with Date)** **( Industry guide signature with date, if any )** **(Faculty Guide Signature with Date)**

# SARALA BIRLA UNIVERSITY, RANCHI

## TheDepartment of CSE & CA

WEEKLY PROGRESS REPORT **(WPR)** (Odd Semester 2025 - 2026 Session)

**(To be submitted by the Student to his/her Project Faculty Guide every Monday)**

**Student Name**: Saloni Kumari Singh, **Reg. No**. SBU234041 **Group No.**: 24, **Program**: BCA, **Batch**: 2023-26, **Sem &Sec**- V-B

**FG Name**: Ms Bikram Pratap Singh, Coordinator, Departmental Project & Internship Committee, Dept of CSE, SBU **Commencement Date**: 25/09/2025,
**Project Completion & Final Report Submission Date**: 22/11/2025, ***WPR No***: 01

**Approved Project Title:** **Optimising QoS for IoT Traffic in 4G/LTE ISP Networks**

*Minor project, Course Code: BCA-507, CU:2;* ***Current Week Duration:****10/11/2025 to 16/11/2025;* **WPR submitted on (date)**: 17/11/2025

| Day / Date | **Summary** (day-wise, precise & quantified information should be given below by the student) |
|---|---|
| **MON –10/11/25** | • ***Incorporated the ER diagram along with revised network topology illustrations.*** |
| **TUE - 11/11/25** | • ***Enhanced the academic tone across all sections for stylistic consistency.***<br>• ***Checked reference entries and restructured the bibliography format.*** |
| **WED –12/11/25** | • ***Refined the problem definition and research objectives for clarity and precision.*** |
| **THU –13/11/25** | • **Performed a line-by-line proofreading of the report.** |
| **FRI – 14/11/25** | • ***Integrated the faculty/supervisor's suggestions throughout the document.*** |
| **SAT – 15/11/25** | • ***Re-examined citation formatting and corrected the reference list again.*** |
| **SUN – 16/11/25** | • ***Polished Chapters 1 through 4 into submission-ready form.)*** |

Note: **Student must include all the original signed WPRs in their Project Report.**

**(Student Signature with Date)** **( Industry guide signature with date, if any )** **(Faculty Guide Signature with Date)**

# SARALA BIRLA UNIVERSITY, RANCHI

## TheDepartment of CSE & CA

WEEKLY PROGRESS REPORT **(WPR)** (Odd Semester 2025 - 2026 Session)

**(To be submitted by the Student to his/her Project Faculty Guide every Monday)**

**Student Name**: Saloni Kumari Singh, **Reg. No**. : SBU234041 **Group No.**: 24, **Program**: BCA, **Batch**: 2023-26, **Sem &Sec**- V-B

**FG Name**: Ms Bikram Pratap Singh, Coordinator, Departmental Project & Internship Committee, Dept of CSE, SBU **Commencement Date**: 25/09/2025,
**Project Completion & Final Report Submission Date**: 22/11/2025, ***WPR No***: 01

**Approved Project Title:** **Optimising QoS for IoT Traffic in 4G/LTE ISP Networks**

*Minor project, Course Code: BCA-507, CU:2;* ***Current Week Duration:****17/11/2025 to 23/11/2025;* **WPR submitted on (date)**: 24/11/2025

| Day / Date | **Summary** (day-wise, precise & quantified information should be given below by the student) |
|---|---|
| **MON –17/11/25** | • ***Commenced the preparation of Chapter 5, focusing on documenting the obtained network results.***<br>• ***Embedded graphs representing delay, variation, and throughput behaviours.*** |
| **TUE - 18/11/25** | • ***Developed comparison tables to summarise all performance outcomes.*** |
| **WED –19/11/25** | • ***Drafted key findings and formulated final analytical insights.***<br>• ***Refined layout elements, including spacing, alignment, and structure.*** |
| **THU –20/11/25** | • **Compiled the appendix containing configurations, logs, and visual evidence.**<br>• **Completed the working version of Chapter 5** |
| **FRI – 21/11/25** | • ***Cross-checked tables and references for accuracy.***<br>• ***Ensured the report follows institutional formatting norms.*** |
| **SAT – 22/11/25** | • ***Ran a detailed grammar and spell check.***<br>• ***Finalised all preliminary pages, such as the title sheet, TOC, and listings.)*** |
| **SUN – 23/11/25** | • ***Exported the complete manuscript as a PDF.***<br>• ***Conducted a final read-through before marking the document ready for submission.*** |

Note: **Student must include all the original signed WPRs in their Project Report.**

**(Student Signature with Date)** **( Industry guide signature with date, if any )** **(Faculty Guide Signature with Date)**