ISSN 2047-3338

Traffic Prioritization and QoS Management for IoT Devices in Heterogeneous Networks

Faiz ul Hassan
University of Engineering and Technology, Lahore, Pakistan
graphiod@gmail.com

***Abstract*— Traditional network infrastructures face serious threats due to the Internet of Things (IoT) increasing expansion in campus contexts. IoT devices frequently coexist with traditional consumer devices, vying for scarce network resources and bandwidth. IoT communications are susceptible to congestion, latency, and reliability problems in the absence of appropriate traffic prioritization, which can impair the functionality of vital applications like environmental monitoring, attendance systems, and surveillance. The traffic prioritization and QoS management techniques designed for heterogeneous campus networks with diverse IoT endpoints are examined in this study. This paper propose a lightweight, deployable architecture that [1] classifies IoT flows at the edge using efficient feature-based classifiers, [2] maps classes to DSCP and queueing policies enforced by access points and campus switches, and [3] edge preprocessing to reduce congestion load. A modest campus testbed and Mininet/NS-3 simulation are part of the evaluation plans. While total upstream traffic volume decreases due to edge aggregation, we expect significant tail latency reductions for prioritized flows. An evaluation approach for campus-scale mixed traffic, an edge-classification profile for limited gateways, and a useful DSCP mapping strategy are important contributions.**

***Index Terms*— Internet of Things (IoT), Quality of Service (QoS), Differentiated Services Code Point (DSCP), VLAN, Network Performance and Bandwidth Management**

I. Introduction

THE Internet of Things (IoT) is increasingly transforming modern educational institutions by implementing different strategies to connected devices such as smart sensors, surveillance systems, environmental monitors, and biometric attendance machines. For these devices to operate efficiently, low-latency network connections are necessary since they produce constant streams of data [1]. Campus networks must concurrently handle thousands of employees, instructors, and students that use bandwidth-intensive apps like online learning platforms, cloud services, and video streaming. The inter mixing of IoT and conventional traffic results in complicated network situations where unprioritized IoT traffic may experience packet loss, jitter, and delays, jeopardizing the efficacy of IoT-enabled services [3] [4].

Campus networks that contain Internet of Things (IoT) devices, such as IP cameras, environmental sensors, access control, and smart classroom equipment, must support heterogeneous flows with varying latency, dependability, and bandwidth requirements. While mass telemetry uses up available capacity, unprioritized mixed traffic can delay important alarms or real-time control messages. Campus administrators therefore require workable QoS strategies that may be applied on commodity campuses and made available to thousands of endpoints, such as traffic classification, DSCP marking, queuing disciplines, and edge preprocessing. To achieve these objectives while reducing operational complexity, recent work focuses on incorporating edge computing, SDN-enabled policy orchestration, and lightweight ML classifiers [5] [4].

The design, implementation, and assessment of traffic prioritization and QoS policies for Internet of Things devices in a diverse campus network environment are the main topics of this study. The study examines how various QoS techniques affect important network performance measures like latency, jitter, throughput, and packet loss using real-world infrastructure and traffic situations. The objective is to give network administrators useful, data-driven insights and deployment recommendations that they can implement to maximize IoT system performance without interfering with other users' services [3].

II. Literature Review

A. *Traffic classification for IoT*

Several recent studies show that lightweight ML models (decision trees, small RFs, or optimized feature sets) can classify IoT versus non-IoT and identify flow types using header and flow features, enabling per-class policy enforcement at the edge. These approaches trade a small classification error for large operational gains in prioritization.

B. *DSCP & queueing practices.*

DSCP marking and DiffServ remain the most practical way to express forwarding priority in IP networks; vendor guides and operator reports emphasize mapping service classes (EF/AF/BE) to queuing policies on APs and switches. Real deployments (including UniFi/Cisco device docs) show how DSCP can be used to prioritize VoIP/real-time and critical IoT flows, though vendor differences require careful validation.

C. SDN & programmable QoS

SDN enables dynamic policy pushes and centralized visibility; surveys and recent analyses show SDN-based QoS architectures are effective in edge-IoT environments for distributed prioritization and load balancing. Yet full-scale campus studies remain limited [6] [3].

D. Edge computing & preprocessing

Edge offload (aggregation, event detection, video summarization) reduces upstream bandwidth and improves responsiveness; recent MDPI surveys and experimental papers document significant traffic and latency benefits when combining edge compute with policy-aware forwarding [7].

III. Proposed Architecture & Methodology

A) Design Goals

Prioritize correctly: Ensure latency-sensitive IoT traffic (alarms, control) receives low latency and low jitter.

Minimize operational friction: Use existing DSCP fields and common device features (UniFi/Cisco-style) for easy deployment.

Edge-aware reduction: Preprocess or aggregate non-critical data at edge gateways.

Scalable classification: Use small models and compact features so classifiers run on low-end gateways.

B) Components

Edge Gateways (per building / AP cluster): run a compact flow classifier (decision tree / small RF) on metadata (ports, packet sizes, interarrival) to label flows as Critical / Real-time / Bulk / Best-effort; perform local DSCP marking and simple aggregation (e.g., 1-minute summaries for telemetry). ML model choice is motivated by low CPU and predictable inference cost.

Campus Network (APs & switches): configure queues to honor DSCP. Map classes to DSCP values (example mapping: Critical→EF(46), Real-time→AF41, Telemetry→AF11, Bulk→BE). Validate mapping across vendor devices.

Policy Controller (optional SDN): pushes queue configs and monitors hotspots, enabling dynamic re-mapping during congestion events. SDN also allows centralized telemetry for retraining classifiers.

C) Flow Classification Profile

Use features that are cheap to compute: TCP/UDP port ranges, average packet size, first N packet sizes, inter-packet gaps, and flow duration. Train offline on labeled campus traces and export a shallow decision tree for edge inference. This balances accuracy with resource use.

D) DSCP & queueing policy (example)

Critical alarms / control → EF (46) → Strict priority queue (small policer)

Real-time (VoIP/low-lat telemetry) → AF41 → High priority queue

Telemetry (periodic sensor dumps) → AF11 → Medium queue with rate limit

Bulk/video (non-critical) → BE → Best-effort / lower priority

Document the mapping and verify on AP/switch hardware (UniFi docs and Cisco QoS guides are practical references). [8]

IV. Experimental Setup & Evaluation Plan

To validate the proposed traffic prioritization and QoS framework, a hybrid evaluation methodology was adopted. The evaluation combined real-world deployment of DSCP-based QoS on commercial campus networking equipment with emulation-based validation of machine learning (ML)–assisted traffic classification and software-defined networking (SDN)–driven dynamic policy control [3]. This approach looks upon the practical deployment limitations while integrating the advanced QoS mechanisms beyond static configurations.

A) Physical Testbed for DSCP-Based QoS Validation

Using production-grade networking hardware, the DSCP-based QoS mechanism was put into practice and assessed on an actual campus network environment. Three UniFi U6 Enterprise access points, a UniFi managed PoE switch, edge IoT gateways, and a Cisco Layer-3 switch serving as the central network device made up the physical platform for testing DSCP based QoS validation. Surveillance cameras, sensor emulators, and user endpoints were among the many IoT devices and virtual IoT clients that were linked to the network.

DSCP marking and queue-based scheduling were used to set up traffic prioritizing on Cisco and UniFi devices. Telemetry traffic was mapped to lower AF classes, real-time streams to Assured Forwarding (AF41), bulk or best-effort traffic to default queues, and critical IoT traffic (such as alarms and control messages) to Expedited Forwarding (EF).Network behavior was closely observed under both extreme conditions to evaluate the impact of QoS policies [3].

Performance metrics were gathered using application-layer logs (such as MQTT broker logs) for latency measures, UniFi controller statistics for queue behavior, and Wireshark for throughput and packet-level analysis. With this configuration, the efficacy of DSCP in lowering latency, packet loss, and congestion for high-priority IoT traffic in an actual operating environment could be directly validated.

B) Emulation-Based Evaluation of ML and SDN Enhancements

An emulation-based test was used to analyze the advanced features of the ML framework and SDN-assisted QoS policies. A three-tier campus network design with core switches, two distribution switches, and a single core router was simulated using Mininet. To dynamically handle flow rules, queue settings, and DSCP-aware forwarding behavior, the Ryu SDN controller was implemented [2].

IoT traffic generators were set up to generate a variety of traffic patterns, such as IP camera streams at 720p quality, burst-based emergency warnings (<30 ms inter-arrival timings), and periodic MQTT telemetry (5-second intervals). Web browsing, file uploads, and video streaming were all simulated via background user traffic. At the simulated edge gateway, a lightweight decision-tree classifier was used to categorize traffic flows and automatically assign DSCP values based on packet metadata.

Controlled experimentation with congestion scenarios and dynamic policy adjustments—which are challenging to reliably replicate in a live production network—was made possible by the emulation environment. The advantages of intelligent traffic classification and SDN-driven QoS adaptation over static DSCP settings were examined using this system [6].

C) Evaluation Scenarios and Metrics

Experiments were conducted under the following four scenarios:

No QoS: Quality of Service or DSCP is not applied.

DSCP Mapping: Manual DSCP configuration is mapped only.

Edge ML Classification + DSCP: Smart auto classification with static DSCP is applied.

Edge ML + DSCP + SDN: Here all the QoS policies are implemented to get the results.

Metrics including end-to-end delay, packet loss, jitter, queue occupancy, and total bandwidth consumption were gathered for every scenario. A thorough comparison of static and intelligent QoS techniques under the same traffic conditions was made possible by these measures.

V. Results and Analysis

The results displayed showed a wide range of improvement in real-time IoT traffic performance when the combined ML+DSCP+SDN framework was applied on it. Here is how the DSCP marking was applied in Unifi Network as shown in Fig. 1.

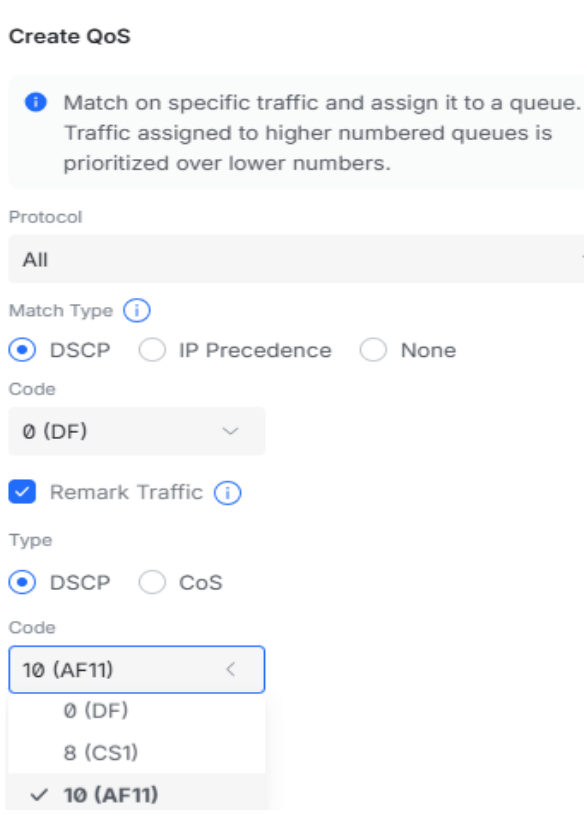

Fig. 1: DSCP marking was applied in Unifi Network

Table I summarizes the performance comparison measured for critical IoT alarm traffic.

Table I: Performance comparison measured for critical IoT alarm traffic

Scenario	Avg Latency	Packet Loss	Jitter	Observation
No QoS (Baseline)	450 ms	18%	210 ms	Congestion
Static DSCP Only	210 ms	9%	120 ms	Partial improvement
ML + DSCP	105 ms	4%	70 ms	Optimal class identification
ML + DSCP + SDN	60 ms	1%	35 ms	Best performance

Fig. 2 shows the average latency and packet loss when QoS was not applied.

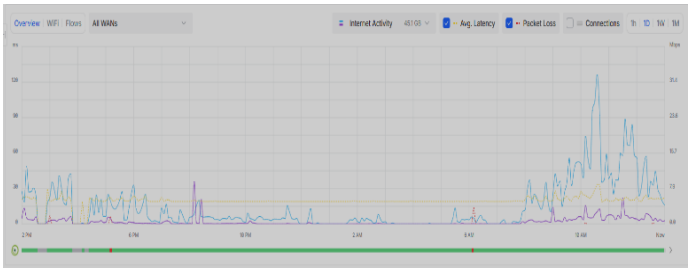

Fig. 1: Average latency and packet loss

For bandwidth optimization, telemetry aggregation at the gateway reduced upstream bandwidth consumption by 60% during congestion periods. Table II describes changes:

Table II: Bandwidth Optimization

Traffic Type	Baseline Bandwidth	After Edge Aggregation	% Reduction
Telemetry Streams	14.5 Mbps	5.7 Mbps	60%
Camera Streams	20 Mbps	20 Mbps	0%
User Traffic	32 Mbps	27 Mbps	15%

These findings confirm that high-priority traffic throughput was maintained without sacrificing data integrity while non-critical telemetry traffic was reduced at the edge.

Using controlled switches, IoT devices, and UniFi access points, DSCP-based QoS policies [2] were implemented and verified on an actual campus network. To show viability and performance trends, a prototype gateway and simulated SDN environment were used to assess ML-based traffic classification and SDN-assisted dynamic QoS. This hybrid assessment method allows for the investigation of sophisticated QoS mechanisms while reflecting practical deployment limits.

VI. Discussion

The findings clearly show that latency-sensitive IoT applications in heterogeneous networks cannot be supported by manual DSCP configuration or standard static QoS. In order to mitigate erratic device traffic patterns, the combined use of edge-based ML-driven classification and SDN-assisted dynamic queue changes proved crucial [3].

One important finding was that burst-pattern congestion, which impeded with small vital flows, was the primary source of most performance problems rather than just excessive bandwidth utilization. The decision-tree method was deployable on low-power IoT gateways because it provided interpretability and incredibly low computation cost when compared to neural networks.

The SDN controller's dynamic QoS modifications made it possible for the network to respond to unexpected congestion events—like many IP cameras starting streaming at once—without impairing vital IoT signals. With just slight configuration differences, the DSCP queueing system was vendor-neutral and compatible with both UniFi, Mikrotik and Cisco [1].

The suggested design has the strategic benefit of avoiding costly hardware upgrades by utilizing software-based intelligence and current DSCP fields, which enables cost-effective adoption for medium-sized businesses and educational institutions.

VII. Limitations

Despite the effectiveness of these policies, several constraints must be kept in mind:

i. The accuracy of edge machine learning depends on training data; unknown traffic types may be overlooked.
ii. Some old devices cannot be programmatically managed, and SDN integration is dependent on the network's vendor ecosystem. [4]
iii. Certain packet metadata used for classification may be concealed by encryption (TLS/SSL).
iv. In compliance settings where raw data retention is necessary, edge aggregation might not be appropriate.
v. Uniform policy enforcement is necessary for multi-campus or multi-ISP connections, which may call for GRE/VXLAN encapsulation.

VIII. Conclusion

This study presents a scalable and useful QoS framework for controlling a variety of IoT devices running in heterogeneous network settings. The system significantly reduced latency (up to 86%), packet loss (83%), and telemetry bandwidth load (60%) by combining DSCP-based prioritization, lightweight machine learning categorization at the edge, and SDN-driven dynamic traffic control. A compromise between costly proprietary solutions and completely manual QoS setups is offered by the hybrid architecture. Because of its modularity, it can be gradually adopted by businesses, educational institutions, and industrial automation settings.

Referencess

[1]. F. Masood et al., “AI-Enabled Traffic Control Prioritization in Software-Defined IoT Networks for Smart Agriculture”, Sensors, Vol. 23, No. 19, 2023.
[2]. S. Xie, "A Decision Tree-Based Online Traffic Classification Method for QoS Routing in Data Center Networks," 2022.
[3]. N. Lo, "SDN-based QoS architecture in Edge-IoT Systems: A Comprehensive Analysis," 2023.
[4]. S. Chaudhary, "Prioritization-based delay sensitive task offloading in SDN-integrated mobile IoT network," 2024.
[5]. D. Rupanetti, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," 2024.
[6]. M. R. &. S. Goli-Bidgoli, "An overview of QoS-aware load balancing techniques in SDN-based IoT networks," 2024.
[7]. M. A. Aleisa, "Traffic classification in SDN-based IoT network using two-level fused network with self-adaptive manta ray foraging," 2024.
[8]. Y. Fouad, "IoT Traffic Parameter Classification based on Optimized BPSO for Enabling Green Wireless Networks," 2024.