Quality of Service (QoS) Implementation: Final Project Report

Team Name: QOS COMMONDOS

Group Number: WINP5

Team Members:

Member Name	Student Number	Role Designation
Kamaljeet Kaur	500219463	QoS Policy Specialist
Mandeep Kaur	500230901	Tester and Troubleshooter
Sagnam	500219291	Documentation and Presentation Specialist
Sushant	500232309	Research Analyst
Tejas Narendrabhai Patel	500219954	Network Designer
Varun Sharma	500232404	Project Manager

Project Advisor: Bhavinkumar Kalathiya

Course Code: 2025W-T4 AIP

Date: APR/02/2025

Abstract

This report presents the comprehensive implementation of a Quality of Service (QoS) solution designed to enhance network performance by prioritizing critical traffic such as voice and video while managing bandwidth efficiently. The report details our project's objectives, methodologies, configuration processes, testing and validation procedures, project management, challenges encountered, and recommendations for future enhancements. Our QoS implementation has led to improved network reliability, efficient traffic management, and strengthened security through integrated authentication and monitoring systems.

Table of Contents

1. Introduction

In today's digital era, the reliability and efficiency of network communications are more critical than ever, especially as organizations rely heavily on real-time applications like VoIP, video conferencing, and cloud-based services. Our Quality of Service (QoS) project was initiated to address the growing challenges of network congestion, latency, jitter, and packet loss that can severely degrade performance. In modern networks, even minor delays or disruptions can lead to significant productivity losses and negatively impact user experience. This project aims to ensure that critical applications receive the necessary priority and bandwidth while maintaining overall network stability.

Our approach was to design and implement a comprehensive QoS solution that classifies, prioritizes, and manages data traffic across our network infrastructure. By integrating robust authentication mechanisms, effective traffic shaping policies, and a comprehensive monitoring system, we ensured that our network can adapt dynamically to varying traffic loads and potential security threats. We utilized a simulated environment with tools like Cisco Packet Tracer to model and test our configurations rigorously before any real-world deployment.

This report outlines the entire lifecycle of our project, detailing the design, implementation, and validation phases. It highlights how our team addressed common issues such as misconfigurations and hardware limitations, and discusses the measures taken to secure the network against unauthorized access. Moreover, the report reflects our collaborative efforts, challenges encountered, and the lessons learned throughout the project. Ultimately, our QoS implementation not only enhances network performance but also provides a scalable foundation

for future technological integrations and upgrades, ensuring that our network infrastructure remains resilient and efficient in a rapidly evolving digital landscape.

2. Project Background and Objectives

In modern network environments, issues like congestion, latency, jitter, and packet loss have become increasingly prevalent, especially as businesses expand their reliance on real-time communications and cloud-based services. With the exponential growth in data traffic and the diversification of network applications, ensuring a seamless user experience has become a significant challenge. Our project was initiated in response to these challenges, aiming to develop a robust Quality of Service (QoS) solution that not only improves network performance but also guarantees that critical applications receive the necessary resources for optimal functionality.

The project's background is rooted in the need to address the following core issues:

- **Increased Network Demand:** As organizations transition to digital operations, the volume of data transmitted across networks has surged. This growth often leads to congestion, where essential services such as VoIP and video conferencing can suffer from delays or interruptions.
- **Real-Time Communication Requirements:** Applications that require real-time data transmission are particularly sensitive to network delays and variability. Even minor disruptions can result in degraded audio quality, video lag, or loss of important data packets, negatively impacting user experience.
- **Security Vulnerabilities:** With the increase in network traffic, the potential for unauthorized access and misconfigurations also rises. Securing network configurations against malicious activities while ensuring seamless data flow is a critical concern.

- **Resource Allocation:** Efficiently managing and allocating bandwidth is essential to prevent performance degradation during peak usage periods. This includes ensuring that high-priority traffic receives preferential treatment without starving other services of necessary resources.

Based on these challenges, our key objectives for the QoS project were clearly defined:

1. **Traffic Prioritization:**

   Develop and implement mechanisms to classify network traffic based on application type, importance, and sensitivity. This involves using advanced techniques such as DSCP (Differentiated Services Code Point) markings and Class-Based QoS (CBQoS) to ensure that critical services, including voice and video communications, are prioritized over less sensitive data transfers.

2. **Bandwidth Management:**

   Implement strategies for effective bandwidth allocation to prevent congestion and ensure fair distribution of network resources. By dynamically adjusting bandwidth allocation based on current traffic loads, we aim to maintain a balance between high-priority and best-effort traffic, ensuring consistent performance even during peak times.

3. **Security Enhancement:**

   Integrate robust authentication and authorization measures across all network devices to protect QoS configurations from unauthorized access or alterations. This involves deploying solutions such as AAA (Authentication, Authorization, and Accounting) and 802.1X port-based authentication to secure the network's critical infrastructure.

4. **Real-Time Monitoring and Proactive Maintenance:**

   Establish a comprehensive monitoring system that provides real-time insights into network performance. This system will track key metrics such as latency, jitter, and packet loss, and will include automated alert mechanisms to notify administrators of potential issues before they escalate. The goal is to enable proactive maintenance and rapid troubleshooting.

5. **Scalability and Future Integration:**

   Design the network architecture to be scalable, ensuring that the QoS solution can adapt to increasing traffic volumes and evolving technological demands. The project also aims to facilitate future integrations with advanced network management solutions, such as AI-driven traffic optimization, to continually enhance network performance.

Through this detailed focus on both immediate performance enhancements and long-term network stability, our project not only addresses current challenges but also sets a solid foundation for future network growth. The subsequent sections of this report will elaborate on the methodologies, configurations, testing procedures, and project management practices that were employed to meet these objectives.

3. Methodology and Implementation Process

Our methodology was structured into several key phases, each critical to the overall success of our QoS project. This section details the step-by-step approach we took, starting from network design to the final performance validation, ensuring that every aspect was rigorously planned, executed, and tested.

3.1 Network Architecture and QoS Design

We began by designing a scalable network architecture tailored to support both current and future traffic loads. This design involved:

- **Topology Planning:** We mapped out a network topology that included a Core Router, Core Switch, and Firewall. The design incorporated multiple VLANs to segregate critical traffic (like VoIP and video) from best-effort data, ensuring that high-priority traffic would have dedicated pathways.
- **Diagram Development:** Detailed diagrams and flow charts were created to visualize the network layout, illustrating the connections between devices, the distribution of traffic, and redundancy measures. These visuals helped us identify potential bottlenecks and plan for future scalability.
- **Redundancy and Failover:** Our design accounted for redundancy by planning backup routes and failover mechanisms, ensuring that if one device failed, the network could seamlessly switch to an alternate path, maintaining continuous service.

3.2 Authentication Mechanisms and Security Measures

Securing our network was a major priority. We implemented multiple layers of authentication and security measures across our devices:

- **AAA Implementation:** On the Core Router, we configured AAA (Authentication, Authorization, and Accounting) to ensure that only authorized users could access and modify critical settings. This involved setting up local databases and, where applicable, integrating with centralized systems.
- **SSH and Secure Access:** To protect remote management sessions, SSH was enabled on all devices, replacing less secure protocols such as Telnet.
- **802.1X Port-Based Authentication:** On the Core Switch, we deployed 802.1X to control access at the port level, ensuring that only authenticated devices could connect. This was crucial in preventing rogue devices from disrupting network traffic.
- **Role-Based Access Control on the Firewall:** We established clear role-based access controls by assigning different privilege levels. For instance, the Security Architect and Authentication Lead had full access, while other roles were given view-only or limited modification rights. This approach minimized the risk of unauthorized changes.

3.3 QoS Policy Implementation

The core of our project was to ensure that critical traffic was prioritized and managed efficiently through robust QoS policies:

- **Traffic Classification and Marking:** On the Core Router, we used Class-Based QoS (CBQoS) to classify traffic. This involved setting up DSCP (Differentiated Services Code Point) markings, such as EF (Expedited Forwarding) for VoIP traffic and AF (Assured

Forwarding) for video streams, ensuring that high-priority packets were easily identifiable.

- **Congestion Management Techniques:** On the Core Switch, we implemented mechanisms like Priority Queuing (PQ) and Weighted Random Early Detection (WRED) to manage network congestion. PQ ensured that high-priority traffic was processed first, while WRED helped in preemptively dropping lower-priority packets before queues overflowed.
- **Bandwidth Shaping:** The Firewall was configured with traffic shaping policies to limit bandwidth for non-critical applications, ensuring that excessive usage did not compromise essential services. These shaping rules were fine-tuned through multiple iterations to achieve a balanced distribution of resources.
- **Iterative Testing and Refinement:** Throughout the implementation phase, we conducted several rounds of tests, adjusting configurations as necessary to optimize performance and minimize packet loss or latency issues.

3.4 Monitoring, Testing, and Performance Validation

To ensure that our configurations were effective, and the network was performing as expected, a comprehensive monitoring and testing strategy was put in place:

- **Real-Time Monitoring Tools:** We deployed SNMP, NetFlow, and Syslog across the network devices to continuously track key performance metrics such as bandwidth usage, latency, jitter, and packet loss. This real-time data allowed us to quickly identify any issues and adjust configurations accordingly.

- **Automated Alert System:** An alert system was configured to send notifications to administrators when critical thresholds were exceeded, such as sudden spikes in traffic or unexpected drops in performance. This proactive approach ensured that issues could be addressed before they escalated.
- **Performance Testing:** Rigorous performance tests were conducted under various simulated conditions. These tests included running multiple VoIP calls, video streams, and large file transfers concurrently to ensure that our QoS policies maintained their effectiveness even under heavy loads.
- **Security and Failover Validation:** Security tests, including intrusion detection simulations and VLAN isolation tests, were executed to validate that our authentication mechanisms and firewall configurations were robust. Additionally, failover simulations confirmed that our redundancy plans were effective, ensuring uninterrupted network service in the event of device failures.
- **Documentation and Reporting:** Every test was meticulously documented, and the results were analyzed to provide insights into network behavior. This documentation not only guided further adjustments during the project but also served as a critical reference for future maintenance.

Through this detailed methodology, we were able to create a network environment that is not only efficient and secure but also resilient and scalable for future growth. Each phase of the process was interconnected, ensuring that our QoS implementation met both the technical requirements and the operational goals of our project.

4. Project Management and Group Dynamics

The success of our Quality of Service (QoS) Implementation project was not only dependent on technical accuracy but also on how effectively our team managed the project and collaborated throughout the process. This section outlines the team structure, communication tools, coordination strategies, meeting organization, and approaches to resolving conflicts. It also includes a reflection on overall team performance and dynamics.

4.1 Team Roles and Responsibilities

Each member of the team was assigned a role based on their skills, interests, and prior experience. Role assignments were discussed and agreed upon during the planning phase to ensure a balanced workload. The roles were as follows:

- Kamaljeet Kaur: Security Specialist– Led the development of test cases, recorded test results, and helped consolidate weekly deliverables into a formal report.
- Mandeep Kaur: Deployment Engineer– Focused on verifying QoS policies and performance testing, preparing weekly test summaries and feedback reports.
- Sagnam: Documentation and Presentation Specialist– Configured and monitored tools like NetFlow and SNMP and validated the results using simulated traffic.
- Sushant: System Engineer– Assisted in real-time performance testing and helped optimize traffic flow and congestion management policies.
- Tejas Narendrabhai Patel: Network Architecture– Designed the network topology, Handled all AAA configurations, SSH setup, and role-based access controls.

- Varun Sharma: Project Manager –oversaw the implementation of QoS, and managed overall project coordination.

4.2 Project Planning and Coordination

Planning began in Week 3, with a focus on dividing the project into clear weekly goals and aligning those with individual responsibilities. A shared Google Sheet was used to create a project timeline and milestone tracker. Weekly deliverables were mapped against each week's goals, and responsibilities were color-coded per team member for clarity.

4.3 Tools for Collaboration and Communication

To coordinate efforts effectively, we used a mix of tools suited to different purposes:

- Google Docs & Sheets – Used for co-authoring weekly reports, checklists, and change logs.
- WhatsApp – Primary channel for quick updates, reminders, and daily check-ins.
- Zoom – Used for weekly team meetings and troubleshooting sessions.
- Trello – Used for task assignment and progress tracking via Kanban boards.
- Cisco Packet Tracer – Our main tool for simulating and testing network configurations.

These tools helped improve team coordination, especially since we had different availability schedules. Being able to update documents asynchronously and get immediate feedback was key to staying on track.

4.4 Meeting Structure and Progress Tracking

We scheduled two team meetings per week—one on Monday to set goals and distribute tasks, and one on Friday to review progress and address issues. Meetings were held over Zoom and typically lasted between 30–45 minutes. Meeting minutes were recorded in a shared document, and action items were clearly assigned at the end of each call.

Daily progress was discussed informally on WhatsApp, and team members updated their Trello cards as tasks moved from “In Progress” to “Complete.” This real-time visibility helped the Project Manager identify any potential delays early.

4.5 Conflict Resolution and Adaptability

As with any group project, differences in opinion and occasional misunderstandings did occur. One such instance involved conflicting interpretations of how QoS classification should be handled on the switch vs. the router. Rather than escalating, the team held a Zoom call to walk through each configuration step and consulted Cisco documentation together to reach a consensus.

Another issue involved a delay in configuring NetFlow correctly. The team members involved reassessed workload distribution to support the Monitoring Specialist, and the task was completed collaboratively without impacting overall progress.

4.6 Team Dynamics and Leadership

Overall, the team worked effectively and respectfully. Varun Sharma, as the Project Manager, provided clear direction and ensured deliverables stayed aligned with deadlines. However, leadership was shared depending on the task—for example, Tejas took the lead during security configuration and Kamaljeet during documentation consolidation.

The team was characterized by open communication, a willingness to help one another, and flexibility. Members volunteered to support each other whenever someone was overloaded or facing technical difficulties. Weekly retrospectives also allowed us to reflect on what went well and what needed adjustment.

4.7 Adjustments and Reassignments

During Week 6, one member faced unexpected personal commitments that affected their availability. To accommodate this, other members temporarily redistributed parts of their responsibilities. This adaptive response helped avoid any major disruption to the project schedule.

5. Drawbacks and Setbacks

While our team was able to complete the QoS implementation project successfully, the process was not without its challenges. This section outlines the specific technical and organizational issues we encountered, the impact of those setbacks, and the steps we took to overcome them. It also highlights our proactive approach to risk mitigation throughout the duration of the project.

5.1 Challenges Encountered and Solutions

1. Misconfiguration of QoS Policies

   One of the most significant early challenges we faced was in the classification and marking of traffic using CBQoS on the router. Initial attempts to prioritize voice and video traffic resulted in unintended behavior where some best-effort traffic was dropped prematurely. The issue was traced to an incorrect mapping of DSCP values and misconfigured class maps.

- Resolution: We reviewed Cisco's QoS best practices and restructured our policy-map configurations. A round of test traffic using simulated VoIP and FTP flows helped us verify that the updated settings functioned as expected.

2. VLAN Tagging Conflicts

   When setting up VLANs on the switch, we encountered inconsistencies in traffic forwarding between VLAN 1 and VLAN 2. Some devices were unable to communicate due to incorrect trunk port configurations and overlapping subnet assignments.

- Resolution: We re-examined the interface configurations and corrected both the trunking mode and IP address assignments. Ping tests and connectivity checks confirmed that inter-VLAN routing was restored successfully.

3. Limited Simulation Environment

   Using Cisco Packet Tracer posed some constraints. Not all commands supported on physical Cisco IOS devices were available in the simulation. This particularly affected our ability to test SNMP traps and advanced monitoring features fully.

- Resolution: We documented these limitations and proposed that future phases of the project be carried out on real hardware or in GNS3 for more advanced testing. In the meantime, we focused on testing the features that were supported.

4. Authentication Timeouts and Access Denials

   After implementing AAA and 802.1X, some authenticated devices experienced timeouts or were denied access during initial configuration. The issue was due to a mismatch between local user credentials and incorrect privilege assignments.

- Resolution: The Security Architect cross-checked the AAA configuration and synchronized usernames, privilege levels, and login settings across all devices. Once resolved, the system allowed appropriate access based on user roles.

5. Time Management During Testing Weeks

   While the team was diligent, during Weeks 10 and 11—when testing and validation were the focus—some delays occurred due to conflicting class schedules and heavy workloads in other courses.

- Resolution: We adapted our workflow by breaking down tasks into smaller units that could be completed asynchronously. Team members worked in shifts and communicated via Trello and WhatsApp to stay updated. Additional evening meetings were scheduled to catch up.

5.2 Risk Mitigation Strategies

Despite these challenges, the team maintained steady progress thanks to a combination of pre-planning, real-time problem-solving, and regular risk assessments. Our strategies included:

- Maintaining version-controlled configuration files in Google Docs to allow rollback if needed.
- Using a shared risk tracker document to log technical and organizational risks weekly.
- Assigning a backup team member for every critical role (especially for security and testing tasks).
- Holding regular “checkpoint” meetings to identify emerging issues early and respond before they escalated.
- Documenting every configuration step, error message, and fix to create a troubleshooting log that was useful for recurring issues and final reporting.

These strategies allowed us to maintain momentum and adapt to unforeseen difficulties, ultimately ensuring the project’s timely completion and high quality.

6. Resources and Labour Analysis

The success of our QoS implementation project depended heavily on thoughtful planning and effective use of available tools, human capital, and informational resources. This section outlines the tools, technologies, and reference materials we utilized, as well as a breakdown of how the team's time and effort were distributed across project phases.

6.1 Technical and Software Resources

To carry out our work efficiently in a virtual setting, we leveraged a variety of industry-standard and academic tools that enabled network simulation, testing, documentation, and communication.

Simulation and Configuration Tools

- Cisco Packet Tracer (Version 8.2.1): Used for simulating our network environment, including the configuration of routers, switches, VLANs, and firewalls. While limited in some advanced features, it was sufficient for demonstrating QoS policies, AAA setups, and VLAN behavior.
- Cisco IOS CLI: While accessed via Packet Tracer, we modeled our configurations based on real-world IOS syntax and command sequences.

Monitoring and Analysis Tools

- NetFlow & Syslog: Simulated via Packet Tracer for traffic visualization and behavior analysis.
- SNMP (Simple Network Management Protocol): Used to simulate performance monitoring and device status polling.

Documentation and Collaboration Tools

- Google Docs & Google Sheets: Used for co-authoring the weekly reports, role documentation, and timeline/milestone tracking.
- Trello: Helped organize weekly tasks and monitor progress through a shared Kanban board.
- Zoom & WhatsApp: Facilitated team communication through video calls and real-time chat updates, especially during testing weeks and milestone reviews.

Research and Academic References

- Cisco QoS Configuration Guides
- Online documentation for AAA, ACLs, and VLAN management
- IEEE articles and whitepapers related to network performance management
- Class lecture slides and textbooks provided by the course instructor

6.2 Labour Distribution

The project team consisted of six members, each contributing according to their roles and weekly focus areas. Labour hours were tracked individually and aggregated during weekly retrospectives. The following is an approximate breakdown:

- Network Design and Planning (Weeks 3–4): ~40 total hours
- Installation and Initial Configuration (Weeks 5–6): ~55 total hours
- Security and Authentication Setup (Week 7): ~30 total hours

- QoS Implementation (Week 8): ~45 total hours
- Monitoring System Setup (Week 10): ~35 total hours
- Testing and Validation (Week 11): ~50 total hours
- User Manual & Documentation (Week 12): ~25 total hours
- Final Report Compilation & Presentation Prep (Weeks 13–15): ~40 total hours

Estimated total: ~320–340 team hours

Note: Due to overlapping responsibilities and rotating leadership roles, some tasks—particularly documentation, testing, and troubleshooting—were shared across multiple team members, ensuring that workloads remained balanced.

6.3 Cost Analysis

As a student-based academic project, the direct monetary cost was minimal. All tools used were freely available (either open-source or provided by the institution), and no physical hardware purchases were required.

- Simulation: Cisco Packet Tracer (Free, provided by Cisco Networking Academy)
- Collaboration: Google Workspace, Trello (Free versions)
- Communication: Zoom (Free license), WhatsApp (Free mobile app)
- Research: Open-access academic databases, public documentation, and instructor-provided materials

Overall, the project was highly cost-effective, requiring zero financial expenditure while still delivering a rich, technically sound result.

7. Final Evaluation and Recommendations

As our QoS implementation project concludes, it is essential to assess the outcomes achieved, measure how well they align with our initial goals, and outline recommendations for future improvements. This section presents a critical evaluation of the technical and managerial aspects of the project, reflecting on its effectiveness and identifying areas where enhancements can be made, especially for real-world deployment.

7.1 Technical Evaluation

Overall, the network performed as expected across multiple test scenarios. After applying our QoS configurations, simulated voice and video traffic experienced reduced latency, lower jitter, and minimal packet loss—indicating that traffic prioritization policies were functioning correctly.

Key technical achievements included:

- Successful configuration of DSCP markings (EF for VoIP, AF41 for video) that aligned with industry standards.
- Reliable traffic prioritization using Class-Based QoS (CBQoS), Priority Queuing (PQ), and Weighted Random Early Detection (WRED).
- Functional bandwidth shaping at the firewall level, which ensured that bulk downloads or large file transfers didn’t degrade the quality of higher-priority traffic.
- A secure authentication system using AAA and SSH that restricted unauthorized access and protected QoS policy configurations.

- A real-time monitoring system using SNMP, NetFlow, and Syslog that enabled effective visibility into performance metrics and allowed for rapid identification of traffic anomalies.

These configurations were tested under both normal and stressed conditions. Our tests showed that high-priority services remained responsive, even when the network simulated congestion with mixed traffic types. Failover simulations confirmed that the redundancy measures worked as expected.

7.2 Project Management Evaluation

From a project management standpoint, the team maintained a consistent workflow with well-defined weekly milestones. Workload was distributed fairly, and responsibilities were clearly communicated. Issues were resolved efficiently due to transparent communication, regular check-ins, and the use of collaboration tools like Trello, WhatsApp, and Zoom.

The inclusion of retrospectives at the end of each week allowed us to reflect on what went well, identify bottlenecks early, and make real-time adjustments. One notable strength was the team's ability to rotate leadership based on technical areas—enhancing both the technical depth and team cohesion.

However, some challenges—such as scheduling conflicts and tool limitations (particularly in the simulation environment)—delayed certain testing phases. These were mitigated by adapting task timelines and sharing responsibilities across roles.

7.3 Alignment with Objectives

Our final deliverables demonstrate that we successfully achieved all key objectives defined in the early stages of the project:

✓ Traffic was classified and prioritized according to real-time service requirements.

✓ Bandwidth was managed effectively during simulated congestion periods.

✓ Authentication mechanisms prevented unauthorized configuration changes.

✓ Monitoring and alert systems provided real-time insights and visibility.

✓ The system was designed to be scalable and adaptable for future upgrades.

7.4 Recommendations for Future Improvement

Although the project met its intended goals, there are areas where improvements can be made, especially if this system were to be deployed in a live enterprise environment:

- Transition to Physical Hardware or GNS3

  Cisco Packet Tracer was helpful for demonstration purposes, but it lacks some enterprise-level capabilities. For more accurate QoS behavior and monitoring capabilities, we recommend transitioning to GNS3 or physical routers/switches in future iterations.

- Automate Monitoring and Alerts

  The current monitoring system is functional but manual in nature. Integration with cloud-based dashboards, AI traffic analyzers, or systems like SolarWinds or Zabbix could improve scalability and automation.

- Include VPN and Remote Access Considerations

  Future versions should explore secure remote access (VPNs) and how QoS policies apply to remote endpoints, especially in hybrid work scenarios.

- Periodic Security Reviews

  Although initial authentication policies were implemented, ongoing auditing and log reviews are essential to maintain long-term security. Future systems should incorporate routine IDS/IPS checks and regular policy reviews.

- Expand Testing Scenarios

  Due to time and simulation constraints, we were only able to test specific types of traffic. Broader testing with varied applications (e.g., real-time gaming, IoT data streams) could help evaluate the flexibility of QoS policies under more complex traffic patterns.

8. Conclusion

The Quality of Service (QoS) Implementation project provided our team with an in-depth understanding of network performance management, real-time traffic optimization, and secure network design. From the initial planning phases to final testing and documentation, this project challenged us to apply both theoretical concepts and practical configurations in a simulated but realistic environment. Through a methodical approach, we successfully achieved our objectives and gained valuable insights into the complexities of enterprise-level network management.

At the core of the project was the objective to prioritize critical network traffic—namely, voice and video communication—without compromising overall network efficiency. By implementing advanced QoS techniques such as traffic classification, priority queuing, and bandwidth shaping, we were able to design a system that effectively handled multiple traffic types while maintaining optimal performance during congestion. Additionally, the integration of AAA security, 802.1X port authentication, and role-based access controls ensured that the QoS policies were protected from unauthorized access and misconfiguration.

The establishment of a real-time monitoring and alert system played a crucial role in validating our configurations and identifying performance issues early. While Cisco Packet Tracer had limitations, it proved adequate for demonstrating key principles and verifying the functionality of our QoS policies in various traffic scenarios. The testing results affirmed that high-priority applications-maintained stability and low latency, even under simulated load conditions.

From a project management perspective, our team demonstrated strong coordination, adaptability, and shared leadership. The use of collaboration tools and structured communication allowed us to work efficiently, resolve issues quickly, and stay aligned on our weekly milestones.

Challenges such as time constraints and simulation tool limitations were met with proactive planning and teamwork, ensuring that project objectives were not compromised.

In conclusion, the QoS implementation project equipped our team with valuable technical and collaborative skills essential for careers in network engineering and cybersecurity. The outcome reflects not only our technical capabilities but also our ability to manage real-world constraints, document procedures effectively, and deliver a solution that aligns with industry standards. This experience has laid the foundation for future projects involving advanced traffic management, secure infrastructure deployment, and network performance optimization at scale.

9. References

The following sources were instrumental in guiding the design, implementation, and validation of our Quality of Service (QoS) project:

1. Cisco Systems. (n.d.). *Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.6.x*. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html Cisco+4Cisco+4Cisco+4

2. Cisco Systems. (n.d.). *Understanding and Configuring 802.1X Port-Based Authentication*. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dot1x.pdfCisco+2Cisco+2Cisco+2

3. SecureW2. (2024). *AAA Server Best Practices: Secure and Optimize Your Authentication Framework*. Retrieved from https://www.securew2.com/blog/aaa-server-best-practices-secure-and-optimize-your-authentication-frameworkSecureW2+1SecureW2+1

4. ElastiFlow. (2023). *NetFlow, SNMP, and Network Monitoring: An Introduction*. Retrieved from https://www.elastiflow.com/blog/posts/an-introduction-to-netflow-flow-and-snmp-in-network-monitoringelastiflow.com

5. FS.com. (2025). *SFlow vs SNMP vs NetFlow: What Are the Differences?*. Retrieved from https://www.fs.com/blog/sflow-vs-snmp-vs-netflow-what-are-the-differences-387.html fs.com

6. Cisco Systems. (n.d.). *Configuring IEEE 802.1X Port-Based Authentication*. Retrieved from https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_8021x/configuration/15-2mt/config-ieee-802x-pba.htmlCisco

7. MDPI. (2023). *Quality of Service (QoS) Performance Analysis in a Traffic Engineering Model for Next-Generation Wireless Sensor Networks*. Retrieved from https://www.mdpi.com/2073-8994/15/2/513MDPI+1ResearchGate+1

8. Cisco Systems. (n.d.). *Quality of Service Configuration Guide, Cisco IOS XE 17.x*. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/qos/b-quality-of-service/m_qos-apply.htmlCisco+2Cisco+2Cisco+2

9. SecureW2. (2023). *802.1X Port Security Simplified*. Retrieved from https://www.securew2.com/blog/802-1x-port-security-simplified SecureW2+1SecureW2+1

10. StrongDM. (2024). *What is AAA Security? Authentication, Authorization, and Accounting*. Retrieved from https://www.strongdm.com/blog/aaa-securityStrongDM

11. Cisco Systems. (n.d.). *Configuring QoS on Cisco Routers*. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/QoS.htmlCisco

12. LogicMonitor. (2025). *Essential Network Monitoring Metrics & Protocols*. Retrieved from https://www.logicmonitor.com/blog/network-monitoring-metrics-protocols LogicMonitor

13. Orhan Ergun. (2023). *Best Practices for Authorization, Authentication, and Accounting*. Retrieved from https://orhanergun.net/best-practices-for-aaaorhanergun.net

14. Portnox. (n.d.). *What is 802.1X Port Security?*. Retrieved from https://www.portnox.com/cybersecurity-101/8021x-port-security/Portnox

15. Kentik. (2024). *Network Monitoring Protocols: 6 Essential Network Technologies*. Retrieved from https://www.kentik.com/kentipedia/network-monitoring-protocols/Kentik

16. Cisco Systems. (n.d.). *Cisco Catalyst SD-WAN Forwarding and QoS Configuration Guide*. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/qos/ios-xe-17/qos-book-xe/forwarding-qos.htmlCisco+4Cisco+4Cisco+4

17. Noction. (2018). *The Difference between SNMP and NetFlow. Why should I use both?*. Retrieved from https://www.noction.com/blog/snmp-and-netflowNoction

18. TechTarget. (2024). *What is authentication, authorization and accounting (AAA)?*. Retrieved from https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accountingInforma TechTarget+1StrongDM+1

19. CrowdSec. (2024). *What Is the AAA Protocol?*. Retrieved from https://www.crowdsec.net/glossary/what-is-the-aaa-protocolCrowdSec

20. Cisco Systems. (n.d.). *Configuring Quality of Service (QoS) on Cisco Switches*. Retrieved from https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swqos.pdf Cisco

10. Appendices

The appendices provide supplementary materials that support and enhance the main content of our Quality of Service (QoS) Implementation project report. These materials include detailed configurations, testing data, and additional resources that offer deeper insights into our project's execution.

Appendix A: Network Device Configurations

This section contains the complete configuration files for all network devices used in our project, including routers, switches, and firewalls. Each configuration is annotated to explain the purpose of specific settings related to QoS policies, security measures, and network management protocols.

- **Router Configuration:** Detailed settings for traffic classification, policy maps, and interface configurations.
- **Switch Configuration:** VLAN setups, QoS trust boundaries, and port configurations.
- **Firewall Configuration:** Access control lists (ACLs), traffic shaping policies, and security rules.

Appendix B: Testing and Validation Results

This appendix presents the raw data and analysis from our testing phases, demonstrating the effectiveness of our QoS implementation.

- **Latency and Jitter Measurements:** Tables and graphs showing performance metrics under various traffic conditions.

- **Bandwidth Utilization Reports:** Data illustrating how bandwidth was allocated and utilized across different traffic classes.
- **Packet Loss Statistics:** Records of packet loss incidents and their correlation with network congestion levels.

Appendix C: Monitoring and Alerting Configurations

This section provides the configurations for our monitoring tools, including SNMP settings, NetFlow parameters, and Syslog configurations. Sample outputs and screenshots from these tools are included to illustrate how network performance was tracked and anomalies detected.

Appendix D: Project Management Artifacts

To offer insight into our project management approach and team collaboration, this appendix includes:

- **Project Timeline and Milestones:** A Gantt chart detailing the project's phases, tasks, assigned team members, and deadlines.
- **Meeting Minutes:** Summaries of key decisions, action items, and discussions from our regular team meetings.
- **Risk Assessment Logs:** Documentation of identified risks, their potential impacts, mitigation strategies, and status updates throughout the project lifecycle.

Appendix E: User Training Materials

Recognizing the importance of knowledge transfer, this section contains materials developed for training end-users on the implemented QoS system:

- **User Manuals:** Step-by-step guides on accessing and utilizing network resources post-implementation.
- **FAQs:** A compilation of anticipated user questions and comprehensive answers to facilitate smooth adoption.
- **Training Session Agendas and Materials:** Outlines and content used during user training sessions, including presentation slides and hands-on exercises.

These appendices serve to provide a comprehensive view of the project's execution, offering detailed insights into the technical configurations, validation processes, project management strategies, and user engagement efforts that contributed to the successful implementation of the QoS system.