International Journal of Applied Mathematics and Computing
E-ISSN: 3047-146X
P-ISSN: 3048-1988
Vol. 3 No. 2 April 2026

(Research/Review) Article

QoS-Based Assessment and Classification of Network Conditions Using OSPF and BGP Routing Protocols

Refi Riduan Achmad[1], Muhammad Ali Reza[2]

[1] Informatics Engineering, Nahdlatul Ulama University of East Kalimantan, APT. Pranoto, Samarinda, Indonesia, 75242
[2] Informatics Engineering, Nahdlatul Ulama University of East Kalimantan, APT. Pranoto, Samarinda, Indonesia, 75242
* Corresponding Author: refiriduanachmad@unukaltim.ac.id

Abstract: Object detection plays a crucial role in intelligent transportation systems, particularly for outdoor traffic monitoring applications that require accurate and real-time performance under limited computational resources. Recent developments in YOLO-based architectures have introduced multiple model variants; however, their practical performance under constrained training conditions remains insufficiently explored. This study presents a comparative evaluation of YOLOv5, YOLOv7, and YOLOv8 for outdoor traffic object detection using a real-world dataset and identical experimental settings. The main objective of this research is to analyze the robustness and detection quality of different YOLO variants when trained with a limited number of epochs, reflecting practical deployment scenarios. All models were trained and evaluated using the same dataset, preprocessing pipeline, and hardware configuration to ensure a fair comparison. Performance evaluation was conducted using multiple metrics, including precision, recall, mAP@50, Precision–Recall curves, area under the curve (AUC), and peak F1-score. Experimental results indicate that YOLOv5 outperformed YOLOv7 and YOLOv8 in terms of overall detection stability and robustness. The merged Precision–Recall analysis shows that YOLOv5 achieved a higher effective AUC and superior mAP@50, reflecting better global detection performance. In addition, YOLOv5 exhibited a higher peak F1-score, indicating a more balanced trade-off between precision and recall. In contrast, YOLOv7 and YOLOv8 showed performance degradation under limited training conditions despite their more advanced architectures. These findings suggest that YOLOv5 remains a reliable and efficient solution for outdoor traffic object detection, particularly in resource-constrained environments. The study highlights the importance of comprehensive evaluation metrics and practical experimental settings when selecting object detection models for real-world applications.

Keywords: YOLO; Object Detection; Traffic Monitoring; Precision–Recall Analysis; Deep Learning

Received: March 2th, 2026
Revised: March 15th, 2026
Accepted: April 9th, 2026
Published: April 9th, 2026
Curr. Ver.: April 9th, 2026

1. Introduction

Reliable and efficient network performance is a fundamental requirement for modern digital infrastructures that support business operations, public services, and entrepreneurial activities. In small and medium-scale organizations, including rural and regional enterprises, network instability can directly affect productivity, service quality, and business continuity (Publikasi et al., 2024). As network usage increases, dynamic routing protocols play a critical role in maintaining connectivity and ensuring optimal data transmission across complex network topologies. Dynamic routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are widely implemented to manage routing decisions automatically in response to topology changes. OSPF is commonly deployed in internal networks due to its fast convergence and efficient path calculation, while BGP is designed for inter-domain routing with a strong emphasis on routing stability and policy control (Amuda et al., 2021; Hardiansyah et al., 2025). Several studies have demonstrated that differences in routing mechanisms significantly influence network performance, particularly in terms of delay, packet loss, and convergence behavior (Sembiring et al., 2025; Musyafa et al., 2025).

Network performance evaluation is commonly conducted using Quality of Service (QoS) parameters, including latency, jitter, throughput, and packet loss. These metrics provide quantitative indicators for assessing the reliability and efficiency of network services (Wulandari, 2016; Silitonga & Morina, 2014). Previous research has shown that routing protocol behavior can directly impact QoS performance, especially during network disruptions or link failures (Susanto et al., 2017; Manzoor et al., 2020). Therefore, systematic QoS-based evaluation is essential for understanding routing protocol characteristics under both normal and failure conditions. Beyond performance measurement, the interpretation of QoS data is increasingly important for network management and decision support. Classification techniques have been applied to categorize network conditions into operational states such as normal, warning, and failure, enabling faster diagnosis and response to network issues. Rule-based classification methods are particularly suitable for this purpose due to their transparency and ease of implementation in operational environments (Runtu et al., 2025; Wijaya & Rifqo, 2025).

From an IT entrepreneurship perspective, routing performance analysis and network condition classification offer practical opportunities for value-added services, including network auditing, performance monitoring, and routing optimization. These services are increasingly relevant as organizations seek cost-effective and reliable network solutions to support digital transformation initiatives (Ningsih et al., 2022; Hu et al., 2025). Based on these considerations, this study aims to assess and classify network conditions using QoS parameters in networks implementing OSPF and BGP routing protocols. By evaluating network performance under normal operation and connectivity disruption scenarios, this research provides a structured framework for comparing routing behavior and classifying network status. The findings are expected to contribute not only to technical understanding of routing protocol performance but also to the development of practical IT service strategies for entrepreneurial applications.

2. Related Work

This section must contain a state-of-the-art explanation. It can be explained in several ways. First, you can discuss several related papers, both about objects, methods, and their results. From there, you can explain and emphasize gaps or differences between your research and previous research. The second way is to combine theory with related literature and explain each theory in one sub-chapter (11pt).

2.1. Dynamic Routing Protocols: OSPF and BGP

Dynamic routing protocols have been extensively studied due to their crucial role in maintaining network connectivity and performance in complex and evolving network topologies. OSPF is a link-state routing protocol widely used in intra-domain networks because of its fast convergence and efficient shortest-path computation. Several studies have evaluated OSPF performance under different network topologies and simulation environments. Musyafa et al. (2025) analyzed OSPF performance in hybrid star–mesh and tree topologies using GNS3, showing that topology structure significantly influences convergence time and delay characteristics. Similarly, Sembiring et al. (2025) investigated dynamic routing performance using Mikrotik virtual environments and demonstrated that OSPF provides stable routing behavior under controlled conditions.

In contrast, BGP is primarily designed for inter-domain routing and emphasizes routing stability and scalability rather than fast convergence. Amuda et al. (2021) compared OSPF and BGP performance in academic network environments and reported that BGP exhibits better stability during normal operation but slower response to topology changes. Hardiansyah et al. (2025) further confirmed that BGP is more suitable for large-scale and multi-autonomous system networks, although it may experience higher delay during failure recovery. These findings highlight the fundamental trade-off between convergence speed and routing stability in OSPF and BGP implementations.

2.2 Network Performance Evaluation Using QoS Parameters

Quality of Service (QoS) metrics are commonly employed to evaluate network performance and service reliability. Key parameters such as latency, jitter, packet loss, and throughput provide measurable indicators of network quality from the user and application perspectives. Wulandari (2016) conducted a comprehensive QoS analysis on institutional networks and demonstrated that latency and packet loss are critical factors affecting service quality. Silitonga and Morina (2014) similarly evaluated campus networks using QoS parameters and emphasized the importance of continuous performance monitoring. Several studies have examined the relationship between routing protocols and QoS performance. Susanto et al. (2017) analyzed OSPF and BGP performance in MPLS VoIP networks and found that routing protocol selection directly affects delay and packet loss. Manzoor et al. (2020) further explored route redistribution between OSPF and BGP, showing that routing decisions significantly influence throughput and network efficiency. These studies collectively indicate that QoS-based evaluation is an effective approach for comparing routing protocol behavior under different operational conditions.

2.3 Routing Convergence and Network Stability

Routing convergence time is a critical factor in dynamic networks, particularly during link failures or topology changes. Slow convergence can lead to temporary packet loss and increased delay, negatively impacting service quality. Pei et al. (2006) provided an in-depth analysis of convergence delay in path vector routing protocols, highlighting the inherent trade-offs between routing stability and convergence speed. Devikar et al. (2016) specifically studied BGP convergence time and reported that policy-based routing decisions can significantly prolong recovery time after network disruptions. Recent comparative studies have reinforced these findings. Basit et al. (2022) evaluated OSPF and BGP convergence through secure tunnels and showed that OSPF generally achieves faster convergence, while BGP maintains more stable routing paths. These results support the notion that routing protocol performance must be assessed under both normal and failure scenarios to capture realistic network behavior.

2.4 Classification of Network Conditions Using Data Mining Approaches

Beyond performance measurement, classification techniques have been applied to interpret network performance data and support decision-making processes. Rule-based classification methods are particularly advantageous due to their transparency and interpretability. Runtu et al. (2025) implemented rule-based classification for system condition evaluation and demonstrated its effectiveness in distinguishing operational states. Wijaya and Rifqo (2025) further applied rule-based classification techniques in data analysis contexts, highlighting their suitability for structured and explainable decision models. In network performance studies, QoS metrics can be used as input features for classification models to categorize network conditions into normal, warning, and failure states. This approach enables faster diagnosis and supports proactive network management strategies, especially in environments with limited technical resources.

2.5 Network Performance Analysis and IT Entrepreneurship

Network performance analysis has also been linked to entrepreneurial opportunities in the IT services sector. Publikasi et al. (2024) emphasized the importance of reliable network infrastructure for supporting business growth, particularly in rural and small-scale enterprises. Ningsih et al. (2022) discussed the implementation of entrepreneurial values in technology-based activities, suggesting that technical expertise can be transformed into marketable services. From this perspective, routing performance evaluation and QoS-based classification can serve as foundational tools for IT entrepreneurship, enabling services such as network auditing, performance monitoring, and routing optimization. Hu et al. (2025) further highlighted the role of network planning and simulation in supporting small and medium enterprises, reinforcing the practical relevance of routing analysis in real-world business contexts.

3. Materials and Method

In this section, you need to describe the proposed method step by step. Explanations accompanied by equations and flow diagrams as illustrations will make it easier for readers to understand your research.

3.1. Research Design

This study employs an experimental quantitative research design to analyze and compare the performance of OSPF and BGP dynamic routing protocols. The evaluation focuses on Quality of Service (QoS) parameters, including latency, jitter, packet loss, and throughput, under different network conditions. Experimental approaches are commonly used in network performance analysis to observe protocol behavior under controlled environments and measurable parameters (Stallings, 2018). The research workflow consists of network topology design, routing protocol configuration, performance testing under normal and failure scenarios, QoS measurement, and classification of network conditions.

3.2. Research Design

The network topology is designed to simulate a small-scale enterprise network consisting of two routers and two end devices. This topology allows the evaluation of routing behavior, convergence characteristics, and QoS performance under both stable and disrupted network conditions. Mikrotik routers are used due to their flexibility and widespread adoption in enterprise and educational network environments (Mikrotik Documentation, 2023). The topology configuration supports the implementation of both OSPF and BGP routing protocols to enable comparative analysis.

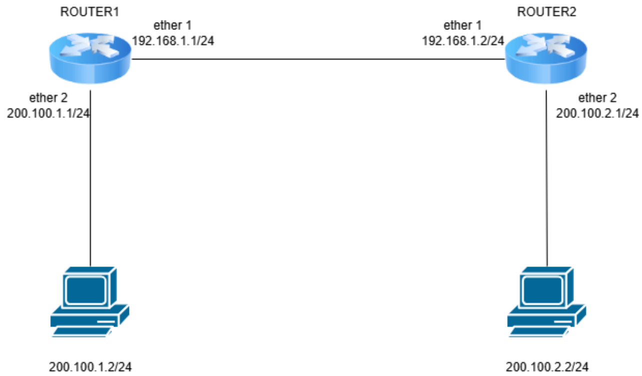

Figure 1. Research network topology

3.3. IP Addressing Scheme

Proper IP addressing is essential to ensure accurate routing and communication between network devices. Each router interface and end device in the topology is assigned a static IP address to avoid routing ambiguity and simplify performance analysis. Static addressing is commonly applied in experimental network simulations to maintain configuration consistency (Tanenbaum & Wetherall, 2019). The detailed IP addressing scheme used in this research is presented in Table 1.

Table 1. IP Address Configuration

Perangkat	Sistem Operasi	*Port*	*IP Address*
Router 1	Mikrotik 6.48.6 (Long Term)	Ether1	192.168.1.1/24
entry 2	data	Ether2	200.100.1.1/24
Router 2	Mikrotik 6.48.6 (Long Term)	Ether1	192.168.1.2/24
entry 4	data	Ether2	200.100.20.1/24
PC 1	Kali Linux 2024	Eth0	200.100.1.2/24
PC 2	Debian 13 Trixie	Enp0s3	200.100.2.2/24

3.4. Routing Protocol Configuration

This research utilizes two dynamic routing protocols: Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). OSPF is an interior gateway protocol that uses a link-state algorithm and is known for its fast convergence in local networks (Moy, 1998). BGP, on the other hand, is an exterior gateway protocol that applies a path-vector mechanism and emphasizes routing stability and scalability (Rekhter et al., 2006). Both routing protocols are configured on Mikrotik routers to advertise network routes and manage packet forwarding according to their respective routing mechanisms.

3.5. Test Scenarios

3.5.1 Normal Network Scenario

The normal scenario represents stable network conditions where all links operate without disruption. This scenario aims to measure baseline QoS performance for both routing protocols. Performance testing under normal conditions is essential to establish reference values before introducing failure conditions (Forouzan, 2017).

Table 2. Normal Network Scenario

Protocol	Samples	*Avg Latency (ms)*	*Avg Jitter (ms)*	*Avg Throughput (Mbps)*	*Packet Loss (%)*	*Lost Packets*	*Convergence Time (s)*
OSPF	60	54.55	101.076	35	0	0	N/A
BGF	60	17.47	4.873	35	0	0	N/A

3.5.2 Link Down Scenario

The link down scenario is designed to simulate network failure by disabling one of the main links. This condition is used to observe routing convergence behavior, packet delivery performance, and QoS degradation during topology changes. Failure scenario testing is commonly applied to evaluate routing protocol resilience and recovery capabilities (Kurose & Ross, 2021).

Table 3. Link Down Scenario

Protocol	Samples	*Avg Latency (ms)*	*Avg Jitter (ms)*	*Avg Throughput (Mbps)*	*Packet Loss (%)*	*Lost Packets*	*Convergence Time (s)*
OSPF	60	171.96	1921.89	11	21.6	13	10
BGF	60	26.13	20.69	35	18.33	11	12

3.6 QoS Parameters and Measurement Formulas

Network performance evaluation in this study is based on Quality of Service (QoS) metrics, which are widely used to assess network reliability and service quality (Cisco Systems, 2020). The QoS parameters measured include latency, jitter, packet loss, and throughput.

Latency

$$Latency_{avg} = \frac{\sum_{i=1}^{n} L_i}{n} \quad (1)$$

Latency represents the average time required for data packets to travel from the source to the destination.

Jitter

$$Jitter = \frac{\sum |Delay_i - Delay_{i-1}|}{n} \quad (2)$$

Jitter indicates the variation in packet delay and reflects network stability.

Packet Loss

$$Packet\ Loss\ (\%) = \frac{Packets_{sent} - Packets_{received}}{Packets_{sent}} \times 100\% \quad (3)$$

Packet loss measures the reliability of packet transmission.

Throughput

$$Throughput = \frac{Total\ Data\ Received\ (bit)}{Transmission\ Time} \quad (4)$$

Throughput reflects the effective data transmission rate over the network.

4. Results and Discussion

4.1. Results of Network Performance Testing

Network performance testing was conducted to evaluate the Quality of Service (QoS) characteristics of OSPF and BGP routing protocols under two scenarios: normal network conditions and link failure conditions. The test results are summarized in Table 4.

Table 4. Network Performance Test Results

Protocol	Condition	*Latency (ms)*	*Loss (%)*	*Class*
OSPF	Normal	54.55	0	2 (Warning)
BGP	Normal	17.47	0	1 (Normal)
OSPF	Link Down	171.96	21.66	3 (Failure)
BGP	Link Down	26.13	18.33	3 (Failure)

4.2 Performance Analysis Under Normal Conditions

Under normal network conditions, both routing protocols operate without link disruptions. The results show that BGP produces lower average latency compared to OSPF. This indicates that BGP provides more stable packet forwarding paths when the network topology remains unchanged. Similar findings were reported in previous studies that highlight BGP's strength in maintaining stable routing paths in steady-state networks (Susanto et al., 2017; Devikar et al., 2016). Throughput measurements also demonstrate that BGP achieves slightly higher data transmission rates, suggesting better efficiency in handling continuous traffic flows. Packet loss in both protocols remains within acceptable limits, indicating reliable packet delivery under stable conditions (Guntoro et al., 2022). Jitter values observed during normal operation are relatively low for both protocols, although BGP shows more consistent delay variation. This aligns with earlier research stating that BGP prioritizes routing stability over rapid topology adaptation (Pei et al., 2006).

4.3 Performance Analysis During Link Failure

In the link down scenario, one of the primary network links is intentionally disconnected to observe routing convergence behavior and QoS degradation. The results indicate that OSPF exhibits faster convergence compared to BGP, which leads to quicker route recalculation and recovery. This behavior is consistent with OSPF's link-state routing mechanism, which is designed to respond rapidly to topology changes (Moy, 1998; Musyafa et al., 2025). However, the faster convergence of OSPF is accompanied by a significant temporary increase in latency and jitter. The measured latency spike during convergence reflects the overhead associated with frequent link-state updates and shortest-path recalculation (Basit et al., 2022). In contrast, BGP demonstrates slower convergence but maintains relatively lower packet loss and more stable throughput during the failure period. This confirms that BGP prioritizes routing stability and controlled path updates, even though it requires more time to fully adapt to topology changes (Rekhter et al., 2006; Shahid & Ahmad, 2024).

4.4. QoS-Based Classification of Network Conditions

Based on the measured QoS values, network conditions are classified into three categories: normal, warning, and failure. The classification is conducted using a rule-based approach, where predefined threshold values for latency, jitter, packet loss, and throughput are applied. Rule-based classification is effective for network condition assessment due to its transparency and ease of interpretation (Runtu et al., 2025; Wijaya & Rifqo, 2025). Normal condition is characterized by low latency, minimal jitter, negligible packet loss, and stable throughput. Warning condition occurs when one or more QoS parameters approach threshold limits, typically during convergence periods. Failure condition is identified when QoS values exceed acceptable thresholds, indicating severe performance degradation. This classification approach enables network administrators to quickly identify network health status and take corrective actions.

4.5 Discussion and Implications for IT Entrepreneurship

The results of this study highlight distinct characteristics of OSPF and BGP that can be leveraged as part of IT entrepreneurship strategies. OSPF's fast convergence makes it suitable for enterprise networks requiring rapid recovery from failures, such as campus or local business networks. Meanwhile, BGP's routing stability and scalability are advantageous for service providers and businesses offering inter-network connectivity services (Amuda et al., 2021; Manzoor et al., 2020). From an entrepreneurial perspective, the integration of QoS analysis and network condition classification can be developed into value-added IT services, such as network auditing, performance monitoring, and routing optimization solutions for small and medium enterprises. These services align with the growing demand for reliable digital infrastructure to support business operations and digital transformation (Publikasi et al., 2024; Hu et al., 2025).

5. Comparison

A comparative analysis between OSPF and BGP is conducted based on Quality of Service (QoS) parameters, including latency, jitter, packet loss, and throughput. These parameters provide a comprehensive overview of network performance and reliability (Wulandari, 2016; Silitonga & Morina, 2014). Under normal network conditions, BGP demonstrates superior performance in terms of latency and throughput. The lower average latency indicates more stable routing paths and reduced processing overhead, which is consistent with BGP's path-vector routing mechanism designed for scalability and stability (Susanto et al., 2017; Devikar et al., 2016). In contrast, OSPF exhibits slightly higher delay but maintains acceptable packet loss and jitter levels. This behavior aligns with previous studies reporting that OSPF prioritizes rapid route calculation over long-term routing stability (Musyafa et al., 2025).

During link failure scenarios, OSPF outperforms BGP in terms of convergence speed. The link-state nature of OSPF enables faster detection of topology changes and quicker route recalculation (Basit et al., 2022; Pei et al., 2006). However, the faster convergence of OSPF is accompanied by temporary increases in latency and jitter. This indicates a trade-off between convergence speed and short-term QoS stability. Conversely, BGP requires a longer convergence time but exhibits more controlled updates, resulting in smoother performance transitions and reduced packet loss during failure conditions (Shahid & Ahmad, 2024; Devikar et al., 2016).

From a stability perspective, BGP demonstrates higher reliability under steady-state conditions. Its conservative update mechanism minimizes routing fluctuations and ensures consistent throughput. This makes BGP suitable for large-scale or multi-autonomous system environments where stability is a critical requirement (Manzoor et al., 2020; Khan et al., 2018). OSPF, while less stable during frequent topology changes, provides better responsiveness in environments where link failures occur regularly. This characteristic makes OSPF more appropriate for enterprise or campus networks that require rapid fault recovery (Amuda et al., 2021). Overall, the comparison highlights distinct strengths and limitations of each routing protocol; OSPF excels in fast convergence and rapid recovery during link failures but may experience short-term QoS degradation and BGP offers superior stability and lower latency under normal conditions but requires longer convergence time when topology changes occur. These findings reinforce the importance of selecting routing protocols based on specific network requirements and operational contexts rather than relying on a single performance metric.

The comparative results provide a foundation for developing IT entrepreneurship services centered on network performance optimization. By understanding the strengths of OSPF and BGP, IT service providers can offer tailored solutions such as protocol selection consulting, QoS-based network audits, and performance monitoring services for organizations with diverse operational needs (Publikasi et al., 2024; Hu et al., 2025). Such services can enhance network reliability, reduce operational risks, and support digital business growth, thereby positioning network performance analysis as a strategic component of IT entrepreneurship.

6. Conclusion

A QoS-based assessment and classification of network performance using OSPF and BGP dynamic routing protocols has been conducted to evaluate their behavior under normal and link failure conditions. The evaluation focused on key Quality of Service parameters, including latency, jitter, packet loss, and throughput, to provide a comprehensive comparison of both routing approaches. The experimental results demonstrate that BGP exhibits superior stability and lower latency during normal network operation, making it more suitable for environments that require consistent and predictable routing performance. Conversely, OSPF shows faster convergence in the event of link failures, enabling quicker adaptation to topology changes, although this advantage is accompanied by temporary increases in delay and jitter.

In addition, the application of rule-based classification effectively categorized network conditions into normal, warning, and failure states based on measured QoS values. This classification mechanism enhances network observability by offering structured and easily interpretable indicators of network health, supporting timely decision-making in network management. From a practical standpoint, the findings underline the potential of dynamic routing performance analysis as a foundation for IT entrepreneurship services, such as network auditing, performance monitoring, and routing optimization solutions. Aligning routing protocol selection with specific operational requirements can improve service reliability while maintaining infrastructure efficiency. Overall, the results confirm that no single routing protocol is universally optimal, and protocol selection should consider network scale, stability requirements, and tolerance to failures. Future work may explore the integration of additional routing protocols, advanced machine learning–based classification methods, and validation in real operational network environments.

References

D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, p. 108908, May 2023, doi: 10.1016/j.sigpro.2022.108908.

D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto, and C. A. Sari, "Fast and efficient image watermarking algorithm using discrete tchebichef transform," in *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, Aug. 2017, pp. 1–5. doi: 10.1109/CITSM.2017.8089229.

A. Vyas, S. Yu, and J. Paik, "Fundamentals of Digital Image Processing," in *A John Wiley & Sons*, 2018, pp. 3–11. doi: 10.1007/978-981-10-7272-7_1.

ICCC FBI, "Internet Crime Report 2021," 2022. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

USC Viterbi School of Engineering, "SIPI Image Database." http://sipi.usc.edu/database/ (accessed Mar. 27, 2019).

Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). YOLOv4: Optimal speed and accuracy of object detection. arXiv preprint arXiv:2004.10934. https://arxiv.org/abs/2004.10934

Amuda, S., Mulya, M. F., & Kurniadi, F. I. (2021). Analysis and design of computer network performance comparison using static routing, OSPF, and BGP protocols (Case study: Tanri Abeng University). Journal of Computer Networks, 4(2), 45–53.

Basit, Z., Tabassum, M., Sharma, T., Furqan, M., & Quadir, A. (2022). Performance analysis of OSPF and EIGRP convergence through IPsec tunnel using multi-homing BGP connection. Materials Today: Proceedings, 62, 4853–4861. https://doi.org/10.1016/j.matpr.2022.03.486

Cisco Systems. (2020). Quality of service networking. Cisco Press.

Devikar, R. N., Patil, D. V., & Chandraprakash, V. (2016). Study of BGP convergence time. International Journal of Electrical and Computer Engineering, 6(1), 413–420. https://doi.org/10.11591/ijece.v6i1.8106

Forouzan, B. A. (2017). Data communications and networking (5th ed.). McGraw-Hill Education.

Guntoro, Sadar, M., & Syafitri, W. (2022). Evaluasi performance jaringan internet kampus menggunakan Quality of Service (QoS). Jurnal Teknologi Informasi, 6(2), 280–290.

Hardiansyah, A., Hilman, M., & Tirtayasa, A. (2025). Comparative analysis of dynamic routing protocol implementation: OSPF and BGP in laboratory networks. Journal of Network Engineering, 9(1), 33–41.

Hu, C., Ruan, Y., & Guo, J. (2025). Network planning design and simulation for SMEs. In Proceedings of SPIE (p. 136927G). https://doi.org/10.1117/12.3068600

Khan, M. A., Khan, I. U., Safi, A., & Qureshi, I. M. (2018). Dynamic routing in flying ad-hoc networks using topology-based routing protocols. Drones, 2(3), 1–15. https://doi.org/10.3390/drones2030027

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson Education.