Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 01 January-2026, Page No.-8597-8604

DOI: 10.47191/etj/v11i01.21, I.F. – 8.482

A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks

Yash Muni
Infogain Corporation

ABSTRACT: Protocol networks are the frameworks in digital communication and establish the requisite principles, structures and mechanisms according to which data is relayed, directed and accepted throughout intricate and connected systems. The networks take advantage of a mixture of routing and forwarding protocols to realize important aims like efficiency, reliability, scale, as well as responsiveness to dynamic conditions. The paper gives an in-depth discussion of three major protocols, which form the basis of the functioning of contemporary IP-based networks, which are Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Multiprotocol Label Switching (MPLS). The protocols are individually studied with regard to their architecture, working principles, core concepts, and real applications on a network of enterprises, as well as very massive service providers. Besides the analysis of the protocol itself, the paper also explores the heterogeneity of the protocol interoperability in the heterogeneous network environment, focusing on the most important issues related to the integration and coexistence.

KEYWORDS: Multi-Protocol Networks, Routing Protocols, Network Architecture, Open Shortest Path First, BGP, MPLS

I. INTRODUCTION

The modern computer networks are the foundation of the modern digitally connected world, where individuals, applications, and systems could communicate with ease in the world. With the technologies such as cloud computing, the IoT, and AI changing, the simple network infrastructure must be capable of meeting the increased demands of performance, reliability, and scalability [1][2]. These networks also require that data is delivered safely, speedily, and free of interruptions, in addition to being fed with large amounts of information. An efficient and nimble networking platform is thus essential in the marketing of feasible digital ecosystems and their further development.

In order to support such complexity, protocol-based communication systems that are protocol-based are necessary to keep interoperability among various types of network devices. Internet Protocol (IP) is the most popular protocol suite on which addressing and routing functions are accomplished through heterogeneous systems [3][4]. The coexistence of IPv4 and IPv6 in the current networks is the evolution of the industry to scalability and support for an increasing number of devices. Interior Gateway Protocols (IGPs), including OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP), with the exterior gateway protocol BGP, lie at the core of providing the necessary routing of data around and between network loops without any errors or glitches.

In this regard, routing architecture constitutes the design and execution of routing mechanisms that are geared to facilitate the flow of traffic on the most advantageous routes. OSPF and EIGRP fulfil intra-domain routing requirements with dynamic metrics and fast convergence to ensure that internal network stability and performance are provided [5]. BGP, given that it is the backbone between inter-domains, is responsible for the sharing of routing data between autonomous systems (ASes), a need in internet global connectivity. In order to further increase the functionality of such protocols [6], Multiprotocol Label Switching (MPLS) is introduced to speed up the packet forwarding and traffic engineering, as well as provide Quality of Service (QoS) guarantees. MPLS overlays separate routing decisions from IP layer intelligence [7], increasing scalability and efficiency in huge, multi-protocol networks.

In this study, an extensive evaluation of how these core protocols– OSPF, EIGRP, BGP, and MPLS work to constitute efficient routing structures within the modern networking conditions is presented [8]. By analyzing its performance in situations such as load sharing, link accidents, and IPv6 incorporation, this paper is intended to discover the advantages and disadvantages of each protocol in implementation [9]. The review gives outlooks on the ways which combining of traditional routing protocols by MPLS can improve the resilience, scalability, and the net efficiency of increasing complex, multi-protocol systems.

A. Structure of the paper

This paper is organized as follows: Section II covers the fundamentals of routing protocols, including OSPF, BGP, and MPLS. Routing in multi-protocol contexts is covered in Section III, along with integration and interoperability. A comparison of the protocols is shown in Section IV. Section V reviews recent literature, and Section VI provides a summary of the paper's main points and suggests avenues for further research.

II. FUNDAMENTALS OF ROUTING PROTOCOLS

The selection and use of routing protocols have a role on the effectiveness and quality of network communications. The main gateway protocols used in corporate networks are usually EIGRP and OSPF. OSPF can effectively understand the entire network topology and make routing decisions through the link-state routing algorithm [10][11]. MPLS is a good technique that identifies data rather than IP addresses to manage traffic. Moreover, it makes the routing process easier as it adds such features as traffic engineering, QoS and network scalability [12]. An external gateway protocol is called Border Gateway Protocol (BGP), which is critical in cases where a need to connect multiple autonomous systems exists and where an internet connection exists. BGP is applicable in data routing, which guarantees the dependability and incalculable transfer of data across the various and extended networks.

A. Open Shortest Path First (OSPF)

The Shortest Open Path The most widely used protocol in networks by Internet service providers (ISPs) is the first routing system. Open Shortest Path First (OSPF) is one such dynamic routing protocol that uses Dijkstra's algorithm to identify the least expensive routes and depends on link-state technologies [13]. The method can determine the shortest route based on the given criteria; however, it does not support the input of any more parameters [14][15]. Their approach includes the additional need of avoiding the inclusion of untrustworthy destination routers wherever feasible. There could be a variety of factors that contribute to the router's mistrust, such as its placement in the temporarily occupied region or close proximity to the combat. Since Autonomous Systems decide the Internet's routing policy, no one else can be entrusted with the task of moving a router to the untrusted class or transferring it back to the traditional class. Because of this, the backbone shown in Figure 1 must be traversed by all traffic destined for lower-level sites. OSPF virtual connections provide an exemption for this kind of functioning. However, much like static routes, virtual connections need manual setup and have the same issues (such as a lack of tolerance to failures).

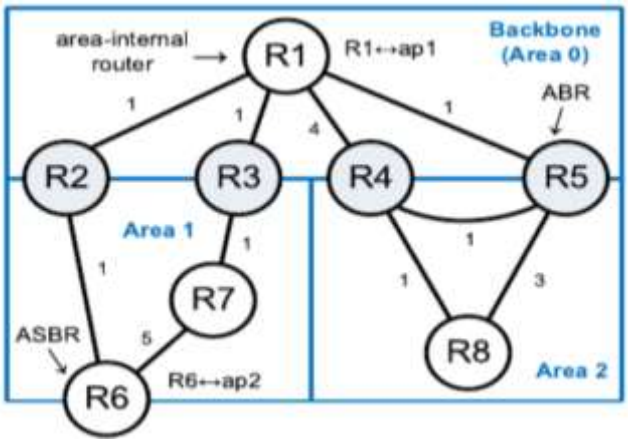

Fig. 1.Hierarchical Open Shortest Path First Network.

1) OSPF Features and Characteristics

Routers in a network can maintain synchronisation between their topology views by using the Open Shortest Path First (OSPF) link-state routing protocol. The OSPF has comprehensive information about the network infrastructure enabling it to identify the shortest path on its route to a destination hence making optimal and efficient routing decisions. OSPF is most commonly applied in an IPv6 environment in this study to allow routers to communicate with a single router within the autonomous system. To enhance speed in a network and optimization of resources, OSPF undertakes the following duties in load sharing in which traffic is spread across channels [16]. OSPF also makes the system stable in that it facilitates the successful link-failover processes when links in a network are disconnected. OSPF also provides additional understanding into IPv6-based load balancing and quick link switchover solutions functionality as they compare to EIGRP and BGP.

B. Border Gateway Protocol (BGP)

The routing protocols used to interdomain route among various networks include the Exterior Gateway protocol commonly referred to as BGP, which is among the protocols that form the foundation of the internet. An interruption or breakdown of this protocol might have a negative impact on internet-dependent services [17]. The operation of the protocol becomes dysfunctional when anomalies arise in BGP. Possible reasons for the BGP anomalies include router configuration errors, session resets, and broken links. Among the many functions performed by the BGP protocol is the exchange of routing and reachability data at the network layer among a large number of autonomous systems [18]. A neighborship or peering is established by the BGP routers after a session is commenced. The BGP peering across various ASes is seen in Figure 2. Data transmission losses and connection issues between ASes may be caused by anomalies, which makes them a danger to the BGP protocol.

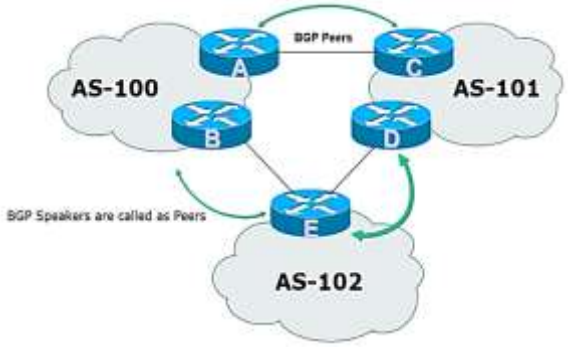

Fig. 2.BGP Peering Across Different Ases

1) BGP Features and Characteristics

An essential component of internet-based communication between different autonomous systems (ASs) is the Border Gateway Protocol, or BGP [19]. The BGP is an outer gateway protocol [20], that shares routing information to guarantee that data and internet traffic from many domains find the best route. BGP is essential because it affects the network's performance as a whole via its routing choices, which in turn direct traffic between independent systems. It may classify BGP into two main categories:

- **Internal Border Gateway Protocol (iBGP):** Intra-autonomous system (AS) routers communicate with one another using iBGP. To make sure that the internal network's routing choices are consistent and effective, it helps to distribute routing information inside the limits of a single AS. Within the AS, routers may make better judgements on traffic routing with the support of iBGP, which helps maintain a consistent image of the network topology.
- **External Border Gateway Protocol (eBGP):** eBGP is used to connect routers in different autonomous systems [21]. It guarantees that networks overseen by different administrative authorities may share routing information, allowing communication between them. When it comes to the larger internet infrastructure, eBGP is crucial because it allows data to effectively go via several autonomous systems by supporting the exchange of routing data throughout the worldwide network.

C. Multi-Protocol Label Switching (MPLS)

The IETF established the Multiprotocol Label Switching (MPLS) standard in 1997 to facilitate the effective transfer of data packets using the Internet Protocol (IP) [22][23]. Without actually opening and inspecting the IP packet, all choices about packet forwarding are based on the contents of the allocated tag. The MPLS concept determines the delivery of IP packets in the wide area networks. Multiprotocol Label Switching (MPLS) is the gold standard of network backbones, and can scale the network resources to the maximum capacity and offer traffic QoS solutions. With the advent of MPLS (Multiprotocol Label Switching) which isolates control and effective packet forwarding, QoS routing schemes are simplified.

1) MPLS Features and Characteristics

Multi-Protocol Label Switching (MPLS), a high-performance routing mechanism can be used to direct data packets faster and more efficiently than the long network addresses. Lying between the network and data layer (sometimes termed as Layer 2.5), MPLS labels packets, which can be configured with pre-established paths across the network that are efficient and expedited [24][25]. This label-based forwarding supports such advanced features as traffic engineering, QoS, and scalable VPNs creation. MPLS supports numerous access techniques, is protocol independent and has the ability to wrap packets of other network protocols [26]. With the combination of MPLS, OSPF and BGP protocols, networks achieve greater scalability, enhanced traffic management and high reliability and this has rendered MPLS a significant option in the present-day multi-protocol networks.

III. ROUTING IN MULTI-PROTOCOL ENVIRONMENTS

Multi-Protocol Networks is a backbone network that exists in a networking environment where one can easily communicate between various systems in the environment. These networks are integrated with different routing protocols (OSPF, BGP and MPLS to permit the transmission of data in an effective way within and between autonomous systems [27][28]. Multi-protocol networks utilize the potential of every one of the protocols and therefore, offer greater scalability, traffic management optimization and reliability which is crucial in current enterprises and service providers.

A. Characteristics of Multi-Protocol Networks

Multi-protocol networks are those networks in which various routing protocols are integrated such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Multiprotocol Label Switching (MPLS) to help in effective passage of data in complex structures [29][30]. The networks can be interpreted based on their ability to accommodate various communication protocols that lead to hassle-free interoperability between various sections of network [31]. Through this integration, enhanced scalability, traffic control and reliability is added which is required by the current enterprises and service providers.

B. Challenges in Routing Across Protocols

There are numerous challenges in routing across multiple protocols:

- **Protocol Compatibility:** Assuring a smooth interaction between the various routing protocols may be tricky particularly when incorporating the old systems into the new protocols.
- **Configuration Complexity:** To apply a large number of protocols simultaneously may lead to wrong settings, which may lead to looping in routing or a route that is not the most optimal one.
- **Security Vulnerabilities:** The protocols can be of different standards as to their security features, and it is difficult to keep a uniform security posture all through the network.
- **Troubleshooting Difficulties:** The situation when a large number of protocols communicate makes it harder to detect and solve.

C. Role of Routing Interoperability

Multi-protocol networked environments require routing interoperability in order that multiple routing protocols can be used concurrently [32]. This interoperability enables easy flow of data among heterogeneous network segments and hence, facilitating communication between different systems.

A significant advantage of the routing interoperability is the enhanced scalability of the network. Different routing protocols can co-exist and interact and this means that networks can still expand continuously and are not confined by protocols [33][34]. This elasticity is very useful particularly when it is deployed at large scale because various departments/regions would use different protocols.

The interoperability also assists in enhancing the resilience of the networks. Interoperability networks will also be in a position to redirect traffic in the other protocols when one of the protocol domains fails, and this will provide continuity in services [35]. Such redundancy is highly significant to mission critical applications where unavailability of the system can have significant implications.

Further, the routing is interoperable, hence simplifying the process of integrating and migrating the network. The organizations can install new systems or migrate into new advanced protocols without necessarily redesigning old infrastructures. This flexibility reduces the cost of operation and also reduces interruptions that may occur in case the company decides to continue expansion or perform upgrade exercises.

IV. COMPARATIVE ANALYSIS OF OSPF, BGP, AND MPLS

A. Protocol Efficiency in Different Network Scenarios

- **OSPF (Open Shortest Path First):** An algorithm based on connection states is called an Interior Gateway Protocol (IGP) routing algorithm. The advantage of OSPF is that it is quite fast and effective in autonomy systems (AS) [36]. The routing protocol suits well in the cases of enterprise networks which require getting a quick update of their network.
- **BGP (Border Gateway Protocol):** The BGP was designed as the primary EGP that would be used to pass traffic paths between independent autonomous systems. The internet is a huge user of BGP since it possesses the convenience of scaling and significant policy-based routing attributes. BGP is slower to converge as compared to OSPF because it is not very fast as it is concerned with stability.
- **MPLS (Multiprotocol Label Switching):** MPLS is a method of handling data packets rather than a routing protocol, which assists in delivering data swiftly and traffic in the network appropriately [37]. The technology is independent of routing protocols and thus guarantees a reliable performance regardless of the kind of network to be utilized.

B. Integration and Interoperability

Implementation of OSPF, BGP and MPLS needs thorough planning to allow interoperability [38]:

- **OSPF and MPLS:** IGP in a MPLS can be set to utilize OSPF in dissemination of routing details. MPLS utilizes the use of IGP to create Label switched paths through the network to transmit data at a higher rate.
- **BGP and MPLS:** BGP is typically used alongside MPLS assisting in configuration of Layer 3 VPNs. Here, BGP transmits VPN routing information on the MPLS backbone [39], and through which communication is possible between various Ass.
- **OSPF and BGP:** Route redistribution between OSPF and BGP can ease the transmission of routing information between internal and external networks. Nevertheless, this has to be done with care in order to avoid routing loops and make an optimal choice of path [40].

C. Use Case-Based Performance Comparison

- **Enterprise Networks:** The main reason why OSPF is usually preferred is because it is fast to converge and also is effective at dealing with intra-domain routing. MPLS is integrable to augment the functionality of traffic engineering and in the VPN services [41].
- **Service Provider Networks:** BGP can be significant in regard to the way in which routers interrelate with networks that belong to other service providers. When MPLS is included, it helps to scale VPN services and manage traffic better on big and complex networks [42].
- **Hybrid Environments:** When both internal and external routing are needed, OSPF handles the internal part, and BGP takes charge of the external part. MPLS plays the main role in high-speed data transport and supports services such as virtual private networks and the control of data traffic.

D. Suitability for Enterprise vs. ISP Networks

- **Enterprise Networks:** OSPF is convenient in enterprise environments because it routes efficiently and converges fast [43]. Optimized traffic and advanced services can be supported with the help of MPLS.
- Large and multiple ISPs rely on the ability of BGP to cover many routes and guide traffic through policies [44]. As a result **ISP Networks:** of using MPLS, providers are able to offer VPNs and manage their traffic in an efficient way. Both network summaries in Table I.

TABLE I. SUMMARIZES THE USE OF ENTERPRISE NETWORK AND ISP NETWORKS.

Aspect	Enterprise Networks	ISP Networks
Routing	OSPF – fast convergence, intra-domain	BGP – scalable, policy-based, inter-domain
MPLS Use	Traffic optimization, QoS support	VPNs, traffic engineering, service delivery
Scale	Medium to large (single AS)	Very large (multi-AS)
Policy Control	Limited	Extensive
Use Case	Campuses, data centers	ISP backbone, customer interconnect

V. LITERATURE REVIEW

This study's way of working not only reduces shutdowns but also keeps the quality high by including a backup mechanism in the network. In the simulations, the backup worked well and the quality of the network was not affected. The study shows that using a single-link failover and BGP is more effective.

Kontsek et al. (2025) offers a fresh approach to the development of IP routing protocols that are dual-stack, with an emphasis on resident relationship and routing message conveyance. Presently in use dual-stack IP routing protocols are defined, discussed, and illustrated in the first section. After that, four separate methods are outlined, using a variety of session neighbor combinations and routing message movement

protocols. Protocol Integration Solution Classes (PISCs) are defined as these permutations in this article. A formal approach to modelling each PISC is to use colored Petri nets (CPNs) [45].

Shen et al. (2024) investigates the possibility of detecting route leakage. By examining BGP routing data, they abstract the routing propagation link between ASs into a network topology graph. Then, at certain intervals, they extract graph properties from this graph. They find out whether a route leakage has happened recently by looking at the graph's structural resilience and centrality measurement properties [46].

Godfrey et al. (2023) demonstrate a clever, energy-efficient multi-objective routing system that makes use of DOS-RL and the RL algorithm. Because wireless IoT devices have such a limited battery life, minimizing disruptions and maximizing overall network performance should be top priorities when designing IoT networks. This is precisely what the proposed DOS-RL routing architecture seeks to accomplish by maximising energy use in these networks. The algorithm takes into account goals that are connected and uses rewards that are informative in shape to speed up the learning process [47].

Rahman et al. (2023) compared many routing protocols to find the best one based on variables including PDR, node health, energy consumption, and end-to-end latency. The simulation results show that Reliability and Adaptive Cooperation for Efficient UWSNs Using Sink Mobility (RACE-SM) performs the best overall when compared to alternative routing methods. The restricted power constraint has prompted the development of many routing techniques aimed at reducing energy use. No clear winner has emerged from the evaluations of the various routing protocols; each used a unique set of criteria [48].

Dogra et al. (2022) offers a method called ESEERP that strengthens the network's connection and makes it last longer, therefore solving the problems discussed before. It uses a multi-purpose, efficient optimization approach to choose the Cluster Head (CH). Consequently, there is minimization of drowsy sensor nodes and minimization of energy consumption. Certainly, once the CH selection is completed; To determine the best route to send data to the sink node, a Sail Fish Optimiser (SFO) is utilised. In terms of energy consumption, bandwidth, packet delivery ratio, and network longevity, the suggested methodology is mathematically analysed, and the outcomes are contrasted with comparable existing methods like particle swarm optimisation (PSO), genetic algorithms (GA), and Ant Lion optimisation (ALO) [49].

Kabir et al. (2021) special consideration of the role of routing table in defining the optimal path of data packet transmission. This paper deals with the performance of the large-scale business wireless sensor network in relation to three routing protocols namely: Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). Network link behaviour was also examined, including average point-to-point throughput (bits/sec), convergence time on flapping connections, and end-to-end packet latency. Lastly, the simulation's outcomes are contrasted with the efficacy and efficiency of these protocols placed in the internet-based RFID system and wireless LAN [50].

Table II provides a summary of the recent research on routing protocols, which demonstrates the improvement of the protocol integration, protocol security, protocol energy efficiency, protocol optimization, and protocol performance measurement in IoT, WSNs, and enterprise network deployments

TABLE II. SUMMARIZING LITERATURE OF REVIEW BASED ON ROUTING ARCHITECTURES IN MULTI-PROTOCOL NETWORKS

Author(s)	Focus	Key Findings	Strengths	Challenges	Future Directions
Kontsek et al. (2025)	Design of dual-stack IP routing protocols (PISCs, CPN modelling)	Coloured Petri nets were used to simulate the 4 defined Protocol Integration Solution Classes (PISCs).	Novel classification (PISC), formal modeling approach	Complexity of dual-stack interactions, scalability of models	Further validation and simulation of PISCs in real-world scenarios
Shen et al. (2024)	BGP route leakage detection using graph-based features	Detected route leakage via structural and centrality graph metrics	Innovative use of graph theory for routing anomaly detection	May not detect zero-day or subtle leakage patterns	Application to real-time detection systems and diverse AS topologies
Godfrey et al. (2023)	Energy-efficient routing in IoT via RL and DOS	DOS-RL reduces energy use and adapts well to network changes	Adaptive learning, energy-aware, handles dynamic objectives	RL-based systems require significant training data and time	Extension to heterogeneous IoT and edge networks
Rahman et al. (2023)	Comparative evaluation of routing protocols in UWSNs	RACE-SM outperforms others in PDR, energy use,	Holistic performance evaluation	Inconclusive overall superiority due	Deeper exploration of hybrid models or adaptive protocol switching

		delay, and node longevity	across multiple metrics	to network variability	
Dogra et al. (2022)	Intelligent energy-saving routing with SFO and CH optimisation	ESEERP improves energy use, PDR, and network life over GA, ALO, and PSO	Strong optimization model, comprehensive comparison	Optimization complexity, CH selection overhead	Testing in larger networks and real-time deployment
Kabir et al. (2021)	Performance of routing protocols in mesh-based corporate WSNs	OSPF showed better convergence and throughput; EIGRP better in latency under flapping scenarios	Evaluates multiple performance factors in real environments	Limited to specific topologies, does not consider energy constraints	Inclusion of modern protocols (e.g., SDN-based) and energy-aware models

VI. CONCLUSION AND FUTURE WORK

The computer networking field has paid tremendous attention to the issue of network routing. Numerous researches have been developed on wired and wireless networks. Recent advancements in network routing technology have created new opportunities of studying the technology. This paper will focus on the critical nature of OSPF, BGP and MPLS in the modern network settings. OSPF is most applicable in fast intra-network routing, BGP is stable and can be applied across networks, and MPLS is known to be the best in terms of traffic management and providing access to VPNs and the quality of services. The compatibility of these protocols in multi-protocol networks adds better scalability, strength and flexibility, which is significant to business and service providers. Nevertheless, one should address such problems as varying protocols, complex setup, and possible security concerns of all processes to be completed in a proper way and in an efficient manner. The strengths, weaknesses and the most ideal applications of either protocol are discussed together in relative context; this helps designers to select the most suitable protocols to use in their network systems.

Future research can explore the combination of outdated routing protocols like OSPF, BGP, and MPLS with innovative technologies like SDN and AI. It would be of use to understand how these protocols developed by analyzing the advantages of IPv6 as well as how these protocols work within large networks. To make the management more efficient and secure, it is possible to develop more effective security solutions to various network protocols and the tools allowing managing and detecting issues automatically.

REFERENCES

1. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems," *Futur. Internet*, vol. 16, no. 9, 2024, doi: 10.3390/fi16090339.
2. R. Tandon and D. Patel, "Evolution of Microservices Patterns for Designing HyperScalable Cloud-Native Architectures," *ESP J. Eng. Technol. Adv.*, vol. 1, no. 1, pp. 288–297, 2021, doi: 10.56472/25832646/JETA-V1I1P131.
3. C. Pan, H. Lu, H. Shi, Y. Wang, and L. Qin, "Inverse Coupled Simulated Annealing for Enhanced OSPF Convergence in IoT Networks," *Electronics*, vol. 13, no. 22, 2024, doi: 10.3390/electronics13224332.
4. S. Kumara, "Zero Trust Identity Fabric for Multi-Layer Telecom Networks: Implications for Secure and Scalable Digital Infrastructure," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 6, 2025.
5. K. Obelovska, Y. Snaichuk, O. Liskevych, S.-A. Mitoulis, and R. Liskevych, "Mitigation of Risks Associated with Distrustful Routers in OSPF Networks—An Enhanced Method," *Computers*, vol. 14, no. 2, 2025, doi: 10.3390/computers14020043.
6. H. S. Chandu, "Performance Evaluation of AMBA-3 AHB-Lite Protocol Verification : Techniques and Insights," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, pp. 201–210, 2024, doi: 10.48175/IJARSCT-19836.
7. Z. A. Yau and K. C. Arun, "Comparative performance evaluation of RIP with OSPF routing protocol," *J. Appl. Technol. Innov. (e-ISSN 2600-7304)*, vol. 5, no. 3, p. 67, 2021.
8. S. K. Chintagunta, "Survey of Containerization , Orchestration , and CI / CD Integration on DevOps in Modern Software Development," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 6, pp. 610–618, 2023.
9. B. A. Scott, M. N. Johnstone, and P. Szewczyk, "A Survey of Advanced Border Gateway Protocol Attack Detection Techniques," *Sensors*, vol. 24, no. 19, 2024, doi: 10.3390/s24196414.
10. R. Rajagopalan and A. Dahlstrom, "Performance comparison of routing protocols in mobile ad hoc networks in the presence of faulty nodes," in *2012 IEEE International Conference on Wireless Information Technology and Systems, ICWITS 2012*, 2012. doi: 10.1109/ICWITS.2012.6417689.
11. H. P. Cyril, "Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations," *Int. J. Adv. Res. Comput. Sci.*, vol. 16, no. 6, pp. 75–82, Dec. 2025,

doi: 10.26483/ijarcs.v16i6.7389.
12. D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.
13. M. Masood, "Multiprotocol Label Switching Network Optimization by Metaheuristic Algorithms," University of Strathclyde, 2020. doi: 10.48730/b6j6-7j09.
14. S. Tyagi, J. Xie, and R. Andrews, "E-VAN : Enhanced Variational AutoEncoder Network for Mitigating Gender Bias in Static Word Embeddings," in *Proceedings of the 2022 6th International Conference on Natural Language Processing and Information Retrieval*, 2022, pp. 57–64. doi: 10.1145/3582768.3582804.
15. N. K. Prajapati, "Cloud-based serverless architectures: Trends, challenges and opportunities for modern applications," *World J. Adv. Eng. Technol. Sci.*, vol. 16, no. 1, pp. 427–435, 2025, doi: 10.30574/wjaets.2025.16.1.1225.
16. S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019, doi: 10.5281/zenodo.15362327.
17. R. D. Verma, P. K. Keserwani, V. K. Jain, M. C. Govil, and V. Tilwari, "Utilizing Duplicate Announcements for BGP Anomaly Detection," *Telecom*, vol. 6, no. 1, 2025, doi: 10.3390/telecom6010011.
18. K. S. Hebbar, "Workload-Aware Machine Learning for Microservice Scaling in Kubernetes," *Int. J. Comput. Exp. Sci. Eng.*, vol. 11, no. 4, Dec. 2025, doi: 10.22399/ijcesen.4546.
19. R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, pp. 503–514, May 2023, doi: 10.48175/IJARSCT-11979B.
20. M. . Abdelhafez and Y. Fadlalla, "BGPsec Deployment Challenges and Optimization Efforts," in *2024 IEEE 22nd Student Conference on Research and Development (SCOReD)*, IEEE, Dec. 2024, pp. 277–281. doi: 10.1109/SCOReD64708.2024.10872667.
21. S. K. Davuluri, V. Challagulla, V. Mudapaka, and U. Konka, "AI-Driven DevOps in Telecommunications: Bridging Predictive Analytics with Continuous Delivery for Network Agility," in *2025 IEEE International Conference and Expo on Real Time Communications at IIT (RTC)*, Oct. 2025, pp. 1–4. doi: 10.1109/RTC66985.2025.11211551.
22. D. Turcanu, "Quality of Services in MPLS Networks," *J. Eng. Sci.*, vol. XXVII, no. 3, pp. 102–110, 2020, doi: 10.5281/zenodo.3949674.
23. S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, Oct. 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.
24. W. Wu, T. Yan, W. Cao, and H. Li, "Research on the application of cross-domain VPN technology based on MPLS BGP," in *Proceedings - 2022 6th International Conference on Wireless Communications and Applications, ICWCAPP 2022*, 2022. doi: 10.1109/ICWCAPP57292.2022.00044.
25. S. B. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, "Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration," *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.
26. A. A. Pranata, T. S. Jun, and D. S. Kim, "Overhead reduction scheme for SDN-based data center networks," *Comput. Stand. \& Interfaces*, vol. 63, pp. 1–15, 2019.
27. B. Oniga, A. Munteanu, and V. Dadarlat, "Open-source multi-protocol gateway for Internet of Things," in *Proceedings - 17th RoEduNet IEEE International Conference: Networking in Education and Research, RoEduNet 2018*, 2018. doi: 10.1109/ROEDUNET.2018.8514136.
28. V. M. L. G. Nerella, K. K. Sharma, S. Mahavratayajula, and H. Janardhanan, "A Machine Learning Framework for Cyber Risk Assessment in Cloud-Hosted Critical Data Infrastructure," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 4, pp. 2409–2421, 2025, doi: 10.52783/jisem.v10i4.12804.
29. S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems," *Int. J. Innov. Res. Creat. Technol.*, vol. 8, no. 2, pp. 1–8, 2022.
30. Y. Muni, "Understanding The Evolution Of Internet Protocols: An In-Depth Review Of Ipv4 And Ipv6: A Comparative Review Of Transition Challenges And Solutions," *Int. J. Adv. Res. Comput. Sci.*, vol. 16, no. 4, pp. 109–117, Aug. 2025, doi: 10.26483/ijarcs.v16i4.7307.
31. L. Argento and A. Furfaro, "A multi-protocol framework for the development of collaborative virtual environments," in *Proceedings of the 2015 IEEE 19th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2015*, 2015. doi: 10.1109/CSCWD.2015.7231001.
32. G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," vol. 4, no. 3, pp. 209–218, 2024,

doi: 10.56472/25832646/JETA-V4I3P122.

33. O. Seker and G. Dalkilic, "Implementation and Performance Analysis of a Multi-Protocol Gateway," in *Proceedings - 2022 Innovations in Intelligent Systems and Applications Conference, ASYU 2022*, 2022. doi: 10.1109/ASYU56188.2022.9925244.
34. S. Narang and G. K. V, "Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, 2025, doi: 10.56975/ijrar.v12i3.319048.
35. S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.
36. S. Amrale, "Proactive Resource Utilization Prediction for Scalable Cloud Systems with Machine Learning," *Int. J. Res. Anal. Rev. (IJRAR*, vol. 10, no. 4, pp. 758–764, 2023.
37. V. Shah, "Managing Security and Privacy in Cloud Frameworks : A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 606–618, 2022, doi: 10.14741/ijcet/v.12.6.16.
38. M. Bhandure, G. Deshmukh, and V. J. N, "Comparative Analysis of Mpls and Non-MPLS Network," *Int. J. Eng. Res. Appl. www.ijera.com*, vol. 3, no. 4, pp. 71–76, 2013.
39. A. M., R. Daniel, D. D. Rao, E. Raja, D. C. Rao, and A. Deshpande, "Optimizing Routing in Nature-Inspired Algorithms to Improve Performance of Mobile Ad-Hoc Network," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 8s, pp. 508–516, 2023.
40. P. Chandrashekar, "A Survey of Tools, Techniques, and Best Practices: CI/CD Integration in DevOps Workflows," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1366–1376, Jul. 2023, doi: 10.48175/IJARSCT-11978V.
41. S. S. Ahmed, A. B. A. Mustafa, and A. A. Osman, "Comparative Study between OSPF and MPLS network using OPNET Simulation," vol. 10, no. 6, pp. 40–43, 2015, doi: 10.9790/2834-10634043.
42. N. Raveendran, "Comparative Evaluation of Persistent vs. In-Memory Stream Exchange in Big Data Systems: A Technical Review," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 7, pp. 172–182, Jul. 2025, doi: 10.32996/jcsts.2025.7.7.15.
43. A. M. Sllame and M. Aljafari, "Evaluating the Impact of Routing and Queuing Techniques on the QoS of VoIP Over IP/MPLS Networks," *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO Certif. Organ.*, vol. 3297, no. 12, pp. 7130–7139, 2007.
44. P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.
45. M. Kontsek, P. Segec, M. Moravcik, and J. Smiesko, "Neighbor Session Solutions for Integrated Routing Protocols," *Appl. Sci.*, vol. 15, no. 1, 2025, doi: 10.3390/app15010293.
46. C. Shen, R. Wang, X. Li, P. Zhang, K. Liu, and L. Tan, "Border Gateway Protocol Route Leak Detection Technique Based on Graph Features and Machine Learning," *Electronics*, vol. 13, no. 20, 2024, doi: 10.3390/electronics13204072.
47. D. Godfrey, B. Suh, B. H. Lim, K.-C. Lee, and K.-I. Kim, "An Energy-Efficient Routing Protocol with Reinforcement Learning in Software-Defined Wireless Sensor Networks," *Sensors*, vol. 23, no. 20, 2023, doi: 10.3390/s23208435.
48. T. Rahman, I. Ahmad, A. Zeb, I. Khan, G. Ali, and M. ElAffendi, "Performance Evaluation of Routing Protocols for Underwater Wireless Sensor Networks," *J. Mar. Sci. Eng.*, vol. 11, no. 1, 2023, doi: 10.3390/jmse11010038.
49. R. Dogra, S. Rani, Kavita, J. Shafi, S. Kim, and M. F. Ijaz, "ESEERP: Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes," *Sensors*, vol. 22, no. 16, 2022, doi: 10.3390/s22166109.
50. M. H. Kabir, M. A. Kabir, M. S. Islam, M. G. Mortuza, and M. Mohiuddin, "Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols," *Eng. Proc.*, vol. 10, no. 1, 2021, doi: 10.3390/ecsa-8-11285.