**MODELING THE INTEGRATION OF IGP AND BGP BY KEEPING MPLS ARCHITECTURE**

**Abstract.** This article explores the key characteristics of integrating IGP and BGP protocols to enhance the scalability, resilience, and manageability of modern network infrastructures. The research addresses the limitations of operating IGP and BGP independently by proposing their integration into a unified MPLS-based architecture. This integration aims to improve scalability, reduce convergence time, and optimize resource management in increasingly complex network environments. The study includes an analysis of the theoretical foundations of IGP and BGP technologies and reviews current approaches to segmented and integrated routing. Special attention is given to the mathematical model involving RFC 3107 and RFC 4655 extensions, the Next-Hop Self function, and the role of border routers in bridging routing information exchange between local and global levels. Using analytical methods and computer simulations, the study demonstrates that the integrated model reduces convergence time (down to 50 ms) and enhances routing efficiency. The scientific novelty lies in the proposed new approach to implementing IGP and BGP within MPLS technology. The findings are particularly relevant for telecommunications professionals engaged in the detailed analysis and optimization of routing protocols, as well as researchers focused on the integration of IGP and BGP to improve network performance and scalability.

**Keywords:** MPLS, IGP, BGP, protocol integration, routing, resilience, scalability, unified architecture.

**Introduction**

The relevance of modeling the integration of IGP and BGP protocols for a unified MPLS architecture is driven by the continuous growth in the complexity of modern network infrastructures, the increasing volume of transmitted data, and the diverse service requirements imposed on next-generation networks. With the rapid development of cloud computing, virtualization, and mobile communications, traditional network management approaches, which rely on the separate operation of IGP (such as OSPF and IS-IS) and BGP, are no longer sufficient to provide the necessary scalability, performance, and fault tolerance. A unified MPLS architecture, combining the hierarchical mechanisms of IGP with the scalability and flexibility of BGP, has become a critical research direction in network technologies.

Research on modeling the integration of IGP and BGP for a unified MPLS architecture demonstrates a comprehensive approach that combines theoretical principles with practical implementations of network technologies. The work by Li Z. et al. [1] and the document "Unified MPLS Functionality, Features, and Configuration Example" [2], published on Cisco’s website, establish fundamental MPLS principles, describing the use of PCE as a central controller and detailing functional capabilities, configuration examples, and key operational aspects of this technology. Additional insights into the architectural foundations are provided in the study by Engineer D. J. S. D. S. [6], which focuses on architectural best practices ensuring high fault tolerance—an essential factor when integrating different control protocols.

On the other hand, the optimization of networks with integrated protocols is explored in the comparative analysis by Shahid K., Ahmad S. N., Rizvi S. T. H. [3]. The authors compare the characteristics of EIGRP, OSPF, and BGP in IPv6 environments, emphasizing load balancing and link redundancy mechanisms in case of failures, enabling an assessment of each protocol's efficiency under dynamic MPLS network conditions. This analysis helps determine optimal routing strategies when modeling complex network scenarios.

Equally important is the diagnosis and mitigation of failures in MPLS infrastructures. In this context, the study by Wankvar T., Witayangkurn A. [4] proposes a framework for automated failure cause analysis, significantly improving response efficiency and enabling the integration of diagnostic algorithms into the overall network management model utilizing IGP and BGP. Chen D., Chen J. [5]. The authors propose strategies for transitioning to SRv6, offering prospects for modernizing existing MPLS networks and integrating traditional and emerging control protocols to develop a more flexible and adaptive architecture.

Liang B. et al. [7] propose a method for automated configuration synthesis in segment routing, which reduces the complexity of manual network configuration and enhances architectural adaptability to changing operational conditions. Muniyappan Y., Thiruvalar N., and Kayathri K. [8] examine the deployment of BGP using both identical and distinct autonomous system numbers, allowing the protocol to be flexibly adapted to the varying requirements of different network operators. Additionally, Mansour M., Samood A., and Saud N. B. [9] evaluate queue management strategies aimed at improving Quality of Service (QoS), which is a critical factor in maintaining the resilience and performance of MPLS VPN networks.

The study by Singh P. and Saini K. S. [10] presents the use of intelligent methods to ensure the security of traffic redistribution processes in DMVPN networks, which is particularly relevant for integrating technologies in distributed network environments. Finally, the work of Islam K., Hassan S. F., and Orel A. [11] proposes an edge-oriented network architecture, highlighting a key direction for building edge-driven networks. This approach may support the optimized allocation of computing and network resources, as well as the integration of IGP and BGP at the network edge.

Despite extensive research on architectural solutions, optimization strategies, and diagnostic methods, contradictions persist in existing studies. Some emphasize centralized management and optimization methods, while others advocate for distributed and adaptive algorithms, posing challenges in developing a universal model for IGP and BGP integration. Additionally, issues related to inter-domain interactions, dynamic adaptation to network failures, and practical aspects of transitioning from traditional MPLS technologies to emerging solutions such as SRv6 remain insufficiently explored. Addressing these gaps is essential to designing a truly unified and resilient network management architecture.

The aim of this study is to analyze the specific characteristics of the integration process between IGP and BGP within MPLS technology.

The scientific novelty lies in the proposal of a new approach to implementing IGP and BGP in the MPLS environment.

This research holds practical significance for contemporary telecommunication systems, as integrating IGP and BGP protocols into a unified MPLS architecture enhances the scalability and fault tolerance of networks. The practical application of the study’s findings enables more efficient distribution of network resources, reduces the number of control points, and simplifies diagnostics and fault recovery procedures—an especially critical factor for large-scale enterprise and service provider networks requiring high reliability and rapid response to unexpected disruptions.

Moreover, integrating IGP and BGP within a single MPLS-based framework offers a foundation for the continued evolution and adaptation of network technologies to meet the demands of the digital transformation era. This methodology also paves the way for incorporating additional technologies, such as SDN and NFV, facilitating the creation of flexible, software-defined networks with centralized management. As a result, it not only improves network performance but also reduces operational costs while ensuring high fault resilience and the ability to recover swiftly from outages.

The proposed hypothesis suggests that integrating IGP and BGP will enable optimal network resource allocation and enhance network resilience to failures by reducing the number of required control points and improving the efficiency of route information exchange.

The research methodology is based on a comprehensive approach, incorporating theoretical analysis, mathematical modeling, and computer simulation of network scenarios.

Thus, this study aims to fill the existing research gap in modeling the integration of IGP and BGP protocols for unified MPLS networks, which holds significant practical value for the advancement of modern network infrastructures.

**1. Theoretical foundations and prerequisites**

Multiprotocol Label Switching (MPLS) is a key technology that ensures high performance and scalability in modern network infrastructures. The core concept of MPLS is that each packet is assigned a label, allowing routers to make switching decisions based on the label value rather than IP addresses. This approach reduces packet processing time and simplifies the establishment of predefined Label Switched Paths (LSP), which is particularly important for implementing virtual networks and VPN services. MPLS has been widely adopted for integrating segmented network domains, enabling the use of both local routing protocols and global route exchange mechanisms.

Interior Gateway Protocols (IGP), such as OSPF, IS-IS, and EIGRP, are designed for efficient route distribution within an autonomous system. These protocols ensure high convergence speed, which is crucial for rapidly detecting topology changes and minimizing downtime [3,5]. However, as networks scale, IGP faces limitations in handling large routing tables, necessitating the use of a global routing protocol—BGP.

Border Gateway Protocol (BGP) facilitates route exchange between different autonomous systems while maintaining extensive routing tables. Additional extensions, such as label distribution via RFC 3107 and the Next-Hop Self function, enable BGP to be used not only for global routing but also for integration with local protocols, creating a unified routing information exchange environment. This is particularly important for building networks that require high scalability and fault tolerance [1, 7].

Modern network infrastructures are characterized by dynamic changes, high traffic loads, and the need for rapid failure recovery. Traditional approaches that involve the separate operation of IGP and BGP lead to fragmented network management, increasing administrative complexity and slowing convergence during failures. Integrating local routing protocols with global route exchange mechanisms within a unified MPLS architecture combines the advantages of both approaches. This synergy enables centralized network management, optimized label distribution, a reduction in the number of control points, and, consequently, improved system resilience [4,6].

To provide a detailed understanding of the comparative characteristics of the main network infrastructure components, Table 1 is presented below.

Table 1. Comparative analysis of the main components of the network infrastructure [1,2, 10]

| **Component** | **Main functions** | **Advantages** |
| --- | --- | --- |
| IGP (OSPF, IS-IS) | Local routing, fast convergence | Minimal delays, high recovery speed (convergence) |
| BGP | Global routing, label exchange (RFC 3107) | Scalability, support for large routing tables |
| MPLS | Packet switching via labels, LSP creation | Efficient traffic management, Quality of Service (QoS) |
| IGP+BGP Integration | Unification of local and global routing methods | Centralized management, enhanced fault tolerance, resource optimization |

These theoretical foundations demonstrate that MPLS, with its flexibility in establishing LSPs, serves as an effective tool for modern network systems. IGP provides high-speed local routing, while BGP ensures scalability and global route distribution. Integrating these protocols into a unified architecture offsets the limitations of individual solutions, forming the basis for building resilient and manageable next-generation networks. This integration is an essential step in addressing the shortcomings of existing network management approaches and lays a solid theoretical foundation for further research in this field.

**2. Modeling the integration of IGP and BGP**

The integration of IGP protocols (such as OSPF and IS-IS) with BGP represents a complex process aimed at ensuring consistency and efficiency in routing both within an autonomous system and between different autonomous systems. The primary objective of this integration is to enable BGP, as an external routing protocol, to accurately reflect the internal network topology managed by the IGP. To achieve this, BGP relies on next-hop reachability information obtained from the IGP, allowing it to correctly compute optimal routes and prevent scenarios in which routing decisions are based on outdated or incomplete data.

A key focus in this integration process is the redistribution of routes between the two protocols, which requires careful configuration of route filtering policies, route attributes (such as MED and LOCAL\_PREF), and synchronization between routing tables to avoid loops or route duplication. Modern implementations incorporate dynamic route redistribution and routing table synchronization, along with topology change management techniques—such as BGP Route Reflectors and Confederations—to reduce administrative overhead and enhance network scalability [1, 11].

This approach not only ensures the stability and fault tolerance of network infrastructure, but also promotes optimal bandwidth utilization, which is particularly critical under high traffic loads and rapidly changing network conditions [2]. The elements of the approach used in building the IGP and BGP integration model are illustrated in Figure 1.



Fig.1. Elements of the approach used in the process of building the IGP and BGP integration model [1,2].

The primary integration mechanism involves label exchange between IGP and BGP using extensions defined in RFC 3107. Within this model:

* Label transmission via BGP. BGP updates are supplemented with MPLS labels, ensuring LSP integrity when transitioning between network segments. This mechanism facilitates end-to-end path information transfer and reduces the load on IGP, as the latter retains only local routes.
* Utilization of the Next-Hop Self function. This function allows each router within a segment to see only the local next-hop, simplifying recursive route lookup and reducing the volume of information transmitted within IGP.
* The role of border routers (ABR) and route reflectors. In the integration of IGP and BGP, routers that connect network segments play a critical role. Implementing route reflection reduces the number of iBGP peerings, improving network scalability and simplifying management [1, 8].

RFC 4655 is applied to integrate IGP and BGP within the MPLS architecture through standardized label and route exchange, ensuring synchronization and operational consistency between these protocols. In this model, IGP (such as OSPF or IS-IS) constructs the topological database and identifies internal routes, while BGP manages interdomain route exchange and routing policy enforcement. RFC 4655 defines label distribution mechanisms linked to routes, creating a unified network view, accelerating failure recovery, and optimizing traffic distribution, thereby enhancing network stability, scalability, and management efficiency.

The conducted modeling demonstrated that integrating IGP and BGP significantly impacts key network parameters:

* Convergence time. The use of BGP Prefix Independent Convergence (PIC) mechanisms and local protection algorithms (LFA/rLFA) reduces failure recovery time to approximately 50 ms, significantly lower than traditional models [3,5].
* Scalability. The integration efficiently processes large volumes of routing information by delegating global label exchange to BGP, enabling support for thousands of routes without substantial computational overhead on IGP [2,6].
* Network management simplification. Centralized management of label and route exchange through an integrated system decreases the number of control points and simplifies network configuration, which is particularly important in dynamically changing topologies.

A comparative analysis of key performance parameters between traditional and integrated MPLS network models is provided in Table 2.

Table 2. Comparative performance analysis of traditional and integrated MPLS network models [1,2, 9]

| **Parameter** | **Traditional model (separate IGP and BGP operation)** | **Integrated model (IGP + BGP)** |
| --- | --- | --- |
| Convergence time | > 200 ms | ~ 50 ms (via BGP PIC, LFA/rLFA) |
| Scalability | Limited, as increasing routes overload IGP | High, global information delegated to BGP |
| Management complexity | Multiple control points, complex configuration and monitoring | Centralized management, reduced peerings |
| Fault tolerance | Dependent on local mechanisms, less flexible in failures | Enhanced via integrated protection mechanisms |

The developed integration model of IGP and BGP demonstrates significant advantages over traditional solutions. Centralized label exchange management, the use of BGP extensions (RFC 3107), and Next-Hop Self functions optimize routing, enhance scalability, and reduce network convergence time. These results support the hypothesis that merging local and global routing protocols within a unified MPLS architecture is an effective approach for modern network infrastructures.

**Conclusion**

A comprehensive analysis and modeling of the integration of IGP and BGP protocols for a unified MPLS architecture have been conducted, addressing critical challenges in modern network infrastructure. The studied model, based on RFC 3107 and RFC 4655 extensions, demonstrates that combining local routing mechanisms (IGP) with BGP’s global functions significantly improves network parameters: convergence time is reduced to approximately 50 ms, network scalability is enhanced by delegating label exchange to BGP, and overall network management complexity is reduced through centralized control.

The practical significance of the obtained results lies in their applicability to real-world scenarios where routing optimization and reduced convergence time are crucial for ensuring network stability. The findings of this study create opportunities for further developments aimed at extending the functionality of unified MPLS architecture and integrating additional technologies such as SDN and NFV, enabling more efficient management of modern network infrastructures.

COMPETING INTERESTS

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer (Artificial intelligence)

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

Option 2:

Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology

Details of the AI usage are given below:

1.

2.

3.

**References**

1. Li Z. et al. RFC 9689: Use Cases for a PCE as a Central Controller (PCECC). – 2024. – pp. 1-37.
2. Unified MPLS Functionality, Features, and Configuration Example. [Electronic resource] Access mode: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/118846-config-mpls-00.html ( date of request: 03/07/2025).
3. Shahid K., Ahmad S. N., Rizvi S. T. H. Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems //Future Internet. – 2024. – Vol. 16 (9). – pp. 339.
4. Wankvar T., Witayangkurn A. A Framework for Automatic Root Cause Analysis of Network Failure on MPLS Network //2024 21st International Joint Conference on Computer Science and Software Engineering (JCSSE). – IEEE, 2024. – pp. 40-46.
5. Jin M., Chen D., Chen J. Overview of Strategies for Evolution to SRv6 //Guide to SRv6 Network Deployment. – CRC Press, 2025. – pp. 77-114.
6. Engineer D. J. S. D. S. Architectural Best Practices for Ensuring High Availability. – 2025. – pp.1-9.
7. Liang B. et al. AutoSRv6: Configuration Synthesis for Segment Routing over . -2025. – pp.1-15.
8. Muniyappan Y., Thiruvalar N., Kayathri K. Implementation of BGP with similar and distinct AS numbers in MPLS VPN networks //AIP Conference Proceedings. – AIP Publishing, 2024. – Vol. 3112 (1). – pp.2 – 10.
9. Mansour M., Samood A., Saud N. B. Assessing Queue Management Strategies to Enhance Quality of Service in MPLS VPN Networks //Libyan Journal of Informatics. – 2024. – Vol. 1 (2). – pp. 29-48.
10. Singh P., Saini K. S. Intelligent Security of Redistribution Management in DMVPN-Based IoT Networks //International Conference on Artificial Intelligence and its Application. – Singapore : Springer Nature Singapore, 2024. – pp. 163-177.
11. Islam K., Hassan S. F., Orel A. An Architecture for Edge Driven Networks //2024 International Symposium on Networks, Computers and Communications (ISNCC). – IEEE, 2024. – pp. 1-5.