DOI: 10.2478/sbeef-2025-0011

EXAMINING IP NETWORK ROUTING PROTOCOLS WITH PACKET TRACER AND CISCO EQUIPMENT

A. FRÂNCU[1], G. PREDUȘCĂ[1], LIANA DENISA CÎRCIUMĂRESCU[1], NICOLETA ANGELESCU[1], D.C. PUCHIANU[1], C. DUMITRACHE[2]

[1]Valahia University of Targoviste, Faculty of Electrical Engineering, Electronics, and Information Technology, [2]University of Pitești Interdisciplinary Doctoral School, Electronic Engineering, Telecommunications, and Information Technologies

E-mail: claudiufrancu859@yahoo.com, gabriel.predusca@valahia.ro, denisa.circiumarescu@gmail.com, nicoletaangelescu@yahoo.com, pdantgv@yahoo.com, dumitrache1978czr@yahoo.com

Abstract. ***This abstract discusses the examination of routing protocols within IP networks using Packet Tracer. Packet Tracer serves as a simulation tool to analyse the functionality and efficiency of various routing protocols such as RIP, OSPF, EIGRP, and BGP in an IP network environment. Through practical experimentation and simulation, this study aims to evaluate the performance, scalability, and reliability of different routing protocols under diverse network conditions. The analysis involves assessing factors like routing table updates, convergence time, and resource utilization. Insights gained from this research contribute to enhancing network design, optimization, and troubleshooting strategies, thereby improving the overall efficiency and effectiveness of IP network routing.***

Keywords: BGP, EIGRP, OSPF, RIP, Packet Tracer.

1. INTRODUCTION

Computer networks represent one of humanity's greatest discoveries. Long before the internet took over our daily lives, engineers and scientists worked to connect computers with each other. The work they did established our current networked state. The rapid expansion of digital networks has significantly influenced the performance of various routing protocols, especially in network environments that demand high availability and reliability. However, there is a lack of comprehensive studies that specifically evaluate the behavior of routing protocols in real-world scenarios with hardware-based simulation platforms. This research gap is critical in the context of ensuring optimal protocol performance under dynamic conditions, such as varying network loads, latency, and topology changes.

This study aims to bridge this gap by evaluating and comparing the performance of two major routing protocols, Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), on real Cisco hardware devices. The objective is to assess the impact of protocol choice on critical network parameters such as convergence time, throughput, and stability when tested under a variety of conditions, including both normal and adverse network scenarios.

Proper IP addressing and routing configuration are essential for inter-network communication; misconfigurations can cause packet loss, delays, or data loss. Routing can be configured statically - suitable for medium networks due to simplicity and resource efficiency - or dynamically, which suits larger networks. Routing protocols update routing tables, maintain connectivity, and select optimal paths to ensure reliable network performance [1-8].

Standardized in 2017, IPv6 addresses the limitations of IPv4, offering expanded addressing and improved efficiency to support growing internet demands. Its header structure differs significantly, making it non-interoperable with IPv4. During the transition, both protocols coexist via dual stack and tunneling mechanisms, ensuring global connectivity and scalable, future-proof communication across increasingly complex device networks [4]. The coexistence of multiple routing techniques shows that no universal solution exists. Routing protocols exchange information to build routing tables, which are then used to forward packets. Each protocol aims to find the shortest path but uses distinct methods. These protocols are generally categorized as Interior Routing Protocols (IRPs) or Exterior Routing Protocols (ERPs), depending on network scope [1-2, 4-8].

The Routing Information Protocol (RIP) is a distance-vector intradomain protocol used within an autonomous system. RIP version 1 calculates cost by hop count, sending updates every 30 seconds. It is easy to configure but suffers from high bandwidth use and slow convergence. Version 2 (RIPv2) improved functionality with CIDR, authentication, and route summarization support [8].

Open Shortest Path First (OSPF) is a link-state routing protocol used within an autonomous system. It exchanges LSR (Link-State Request) and LSA (Link-State Advertisement) packets to assess and share link status, while HELLO messages help discover and maintain neighbor relationships. OSPF builds a topological database, ensures fast convergence after changes, and supports authentication to enhance routing security [1-2, 8].

Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco, combines distance vector and link-state features. It uses the Diffusing Update Algorithm (DUAL) to select optimal paths and adapt quickly to network changes. EIGRP adjusts data rates based on bandwidth, improving efficiency. However, its proprietary design limits multi-vendor interoperability and lacks integrated authentication features [1-2, 6-8].

The Border Gateway Protocol (BGP) facilitates communication between Autonomous Systems (AS) by determining optimal routes based on current conditions and network topology. Each AS, identified by a unique Autonomous System Number (ASN), can represent ISPs, corporations, or universities. BGP, which replaced the Exterior Gateway Protocol (EGP), is crucial for managing routing scalability across the expanding Internet [8].

Several studies have evaluated the performance of EIGRP and OSPF in various networking environments, focusing on aspects such as convergence time, scalability, and fault tolerance. For example, a study by Ifeanyi et al. (2020) compared the convergence times of EIGRP and OSPF under various conditions, finding that EIGRP typically provides faster convergence than OSPF, particularly in scenarios involving high network instability [9]. Similarly, Bolanowski and Byczek (2018) assessed OSPF's scalability in large-scale networks, noting that while OSPF scales effectively in complex topologies, it tends to exhibit slower convergence times under certain failure conditions [10].

In contrast, a more recent study by Manzoor et al. (2020) Manzoor et al. (2020) compared EIGRP and OSPF using Cisco 7200 routers in GNS3, focusing on route redistribution and hardware behavior. Results showed EIGRP had faster convergence and higher throughput, while OSPF had lower delay. The study emphasizes how routing protocol performance varies with hardware and environment, offering insights into real-world network deployment efficiency [11].

However, there remains a lack of studies that incorporate both EIGRP and OSPF performance analysis on Cisco hardware under controlled simulation conditions that include adverse scenarios, such as link failures or network congestion. This study seeks to fill that gap by not only comparing these protocols in a controlled environment but also evaluating them under stress conditions to better understand their real-world applicability and limitations.

2. ROUTING PROTOCOL EXAMINATION UTILIZING CISCO PACKET TRACER

2.1 Configuration in Packet Tracer

This section describes the experimental setup using Cisco Packet Tracer, focusing on network topology, IP addressing, protocol configuration, and test procedures.

CISCO Systems created the computer network simulation software Packet Tracer. With hardware and protocols, users can design and simulate intricate networks. With the help of this platform, different network topologies may be configured and put into use, incorporating hardware like servers, routers, switches, firewalls, and wireless equipment. With Packet Tracer, users may test and comprehend a variety of network scenarios and concepts in a hands-on and interactive manner.

This work investigates alternative routing systems in terms of packet delivery time between source to destination. All the protocols are set up individually and evaluated with the CISCO Packet Tracer. Packet Tracer simplifies the setup of virtual protocols and the analysis of message delivery times in a controlled situation. Ring networks use an architecture in which devices are connected in the same physical ring, enabling scalability and redundancy. Because of their adaptability, ring networks can be readily expanded by adding additional devices to the network [1, 5].

The simulation topology includes three routers (R1, R2, R3), three switches (S1, S2, S3), and three end-user devices (PC1, PC2, PC3). Each router is connected to a switch, and each switch connects to one PC. The routers are interconnected in a triangular topology to enable multiple routing paths, as illustrated in Figure 1.

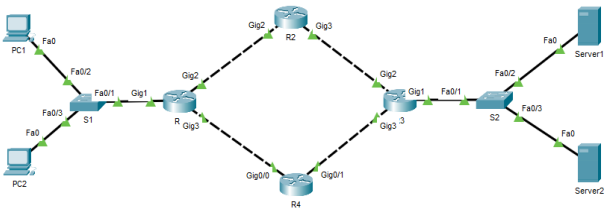

Figure 1. Building and connecting devices.

To build the network, 4 CISCO 2911 routers were used, interconnected with twisted pair cables, two CISCO 2950-24 switches, two Server-PT servers, and two PC computers. For the network to function as shown in Figure 1, each interface of the equipment, whether GigabitEthernet, connected to routers (R1, R2, R3, R4), switches (S1, S2), computers (PC1, PC2), or servers (Server1, Server2), requires IP addresses to transmit and receive packets. For example, R1 has four configured interfaces: G 0/0 with IP address 192.168.1.1; G 0/1 with IP address 10.1.1.1; G 0/2 with IP address 10.1.4.2.

2.2 Results obtained in Packet Tracer

All configurations have been completed to enable communication and packet transmission across the entire created network. The next step is to verify if the devices can successfully communicate with each other. For this, we enter the command "ping 192.168.1.3" into the command line of the PC1 computer to test the connection to Server1, using the IP address "172.16.1.3". We will perform 50 successive tests to assess the consistency and quality of the connection.

The comparative results in terms of average times for each analysed protocol are presented in Tables 1 and 2.

Table 1. Results of the "ping" test from PC1 to Server1 and Server2

Protocol	PC / Server	Minimum (ms)	Maximum (ms)	Average (ms)
Without protocol	Server1	2	13	8
RIPv2		0	12	3
OSPF		0	10	4
EIGRP		*0*	*9*	*3*
BGP		*0*	*7*	*2*
Without protocol	Server2	1	14	6
RIPv2		0	12	5
OSPF		0	10	4
EIGRP		*0*	*9*	*4*
BGP		*0*	*8*	*2*

Table 2. Results of the "ping" test from PC2 to Server1 and Server2

Protocol	PC / Server	Minimum (ms)	Maximum (ms)	Average (ms)
Without protocol	Server1	1	13	8
RIPv2		0	11	4
OSPF		0	10	4
EIGRP		*0*	*10*	*3*
BGP		*0*	*8*	*2*
Without protocol	Server2	1	13	6
RIPv2		0	12	6
OSPF		0	10	5
EIGRP		*0*	*10*	*4*
BGP		*0*	*7*	*3*

The conclusions regarding the comparative results in terms of average times for each analysed protocol, based on communication between PC1 and Server1, Server2, as well as between PC2 and Server1, Server2, are as follows:

- For communication between PC1 and Server1: The BGP protocol exhibited the lowest average response time, at 2 milliseconds, followed by the EIGRP protocol with 3 milliseconds, RIPv2 with 3 milliseconds and OSPF with 4 milliseconds. The BGP protocol proved to be the most efficient for communication between PC1 and Server1.
- For communication between PC1 and Server2: The BGP protocol showed the lowest average response time, at 2 milliseconds, followed by EIGRP and OSPF with 4 milliseconds, and RIPv2 with 5 milliseconds. In this case, BGP proved to be the most efficient protocol for communication between PC2 and Server2.
- For communication between PC2 and Server1: The BGP protocol had the lowest average response time, at 2 milliseconds, followed by EIGRP with 3 milliseconds, OSPF and RIPv2 with 4 milliseconds. BGP provided the fastest average response times for communication between PC2 and Server2.
- For communication between PC2 and Server2: The BGP protocol exhibited the lowest average response time, at 2 milliseconds, followed by EIGRP with 4 milliseconds, OSPF with 5 milliseconds, and RIPv2 with 6 milliseconds. The BGP protocol proved to be the most efficient for communication between PC2 and Server2.

Overall, the BGP protocol exhibited the fastest average response times for all combinations of communication between computers and servers, followed by the EIGRP protocol. OSPF showed higher average response times, while RIPv2 had the highest average response times for some communication combinations.

The second step is to observe the routes taken by packets to reach their destination. For this, we used the "tracert 172.16.1.3" command. Figures 2 and 3 depict the best results obtained in the first scenario, where routers were not configured with any protocol.

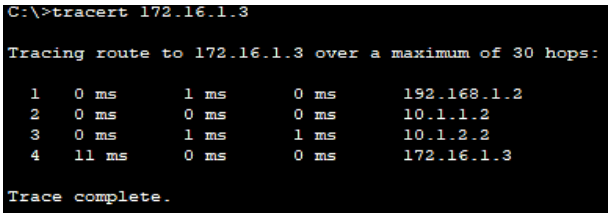

Figure 2. Visualizing the route and hops from PC1 to Server1, without protocol.

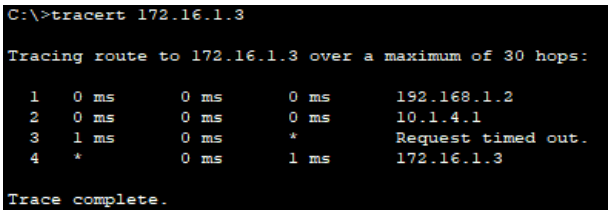

Figure 3. Visualizing the route and hops from PC2 to Server1, without protocol.

Following the tests conducted for the two scenarios (Figures 1–3), it is observed that the packets follow the path PC1 - R1 (192.168.1.1) - R2 (10.1.1.2) - R3 (10.1.2.2) - Server1 (172.16.1.3), and in the second case, they travel through PC2 - R1 - R4 - * - Server1. When devices are not configured with a specific protocol, the information is transmitted randomly across any available route, sometimes resulting in 'Request timed out' messages.

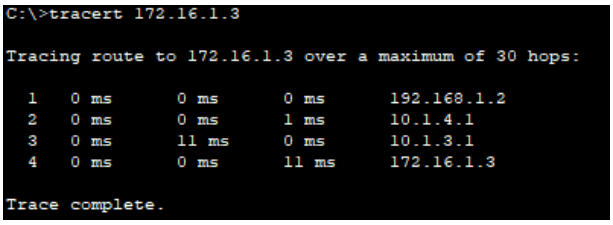

Figure 4. Visualizing the route and hops from PC1 to Server1, RIP.

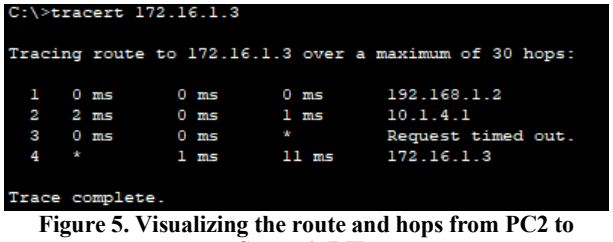

Figure 5. Visualizing the route and hops from PC2 to Server1, RIP.

For the RIP protocol, as shown in Figures 1 and 4–5, it was observed that packets from PC1 follow the path R1 – R4 (10.1.4.1) – R3 (10.1.3.1) – Server1, while those from PC2 follow the path R1 – R4 (10.1.4.1) – * – Server1. If the devices are configured with the RIP protocol, the route followed remains the same, but with occasional 'Request timed out' messages.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.2
  2    0 ms      0 ms      0 ms      10.1.1.2
  3    0 ms      11 ms     0 ms      10.1.2.2
  4    0 ms      10 ms     0 ms      172.16.1.3

Trace complete.
```

Figure 6. Visualizing the route and hops from PC1 to Server1, OSPF.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.1.2
  2    0 ms      0 ms      0 ms      10.1.1.2
  3    11 ms     0 ms      1 ms      10.1.2.2
  4    0 ms      0 ms      0 ms      172.16.1.3

Trace complete.
```

Figure 7. Visualizing the route and hops from PC2 to Server1, OSPF.

Unlike the RIP protocol, OSPF - illustrated in Figures 1 and 6-7 - enables packet transmission from PC1 (192.168.1.3) to Server1 (172.16.1.3) along the path R1 – R2 (10.1.1.2) – R3 (10.1.2.2), while packets from PC2 follow the same route: R1 – R2 – R3. Configuring the devices with the OSPF protocol ensures consistent data delivery without any 'Request timed out' occurrences.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      1 ms      1 ms      192.168.1.2
  2    0 ms      0 ms      0 ms      10.1.4.1
  3    1 ms      0 ms      1 ms      10.1.3.1
  4    11 ms     1 ms      11 ms     172.16.1.3

Trace complete.
```

Figure 8. Visualizing the route and hops from PC1 to Server1, EIGRP.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.2
  2    0 ms      0 ms      0 ms      10.1.1.2
  3    0 ms      12 ms     0 ms      10.1.3.1
  4    1 ms      11 ms     0 ms      172.16.1.3

Trace complete.
```

Figure 9. Visualizing the route and hops from PC2 to Server1, EIGRP.

For the EIGRP protocol, as shown in Figures 1 and 8–9, the results are as follows: packets from PC1 (192.16.1.3) to Server1 (172.16.1.3) are transmitted via the path R1 – R4 (10.1.4.1) – R3 (10.1.3.1), while packets from PC2 to Server1 follow the path R1 – R2 (10.1.1.2) – R1 – R4 – R3 (10.1.3.1). With EIGRP, there are no 'Request timed out' messages, as the system continuously analyzes alternative routes.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.2
  2    1 ms      1 ms      0 ms      10.1.4.1
  3    1 ms      1 ms      1 ms      10.1.2.2
  4    11 ms     0 ms      0 ms      172.16.1.3

Trace complete.
```

Figure 10. Visualizing the route and hops from PC1 to Server1, BGP.

```
C:\>tracert 172.16.1.3

Tracing route to 172.16.1.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.2
  2    0 ms      0 ms      1 ms      10.1.4.1
  3    1 ms      3 ms      0 ms      10.1.2.2
  4    0 ms      1 ms      11 ms     172.16.1.3

Trace complete.
```

Figure 11. Visualizing the route and hops from PC2 to Server1, BGP.

For the BGP protocol, as shown in Figures 1 and 10–11, the route from PC1 to Server1 follows R1 – R4 – R1 – R2 – R3, while the route from PC2 to Server1 is the same: R1 – R4 – R1 – R2 – R3. Configuring the devices with the BGP protocol allows for the transmission of information along different routes without any 'Request timed out' occurrences.

The results of the conducted tests are presented in Table 3.

Table 3. Results of the "tracert" Test to Server1

Protocol	Source	Chosen route	Destination
Without protocol	PC1	R1 → R2 → R3	Server1
	PC2	R1 → R4 → *	
RIPv2	PC1	R1 → R4 → R3	
	PC2	R1 → R4 → *	
OSPF	PC1	R1 → R2 → R3	
	PC2	R1 → R2 → R3	
EIGRP	PC1	R1 → R4 → R3	
	PC2	R1 → R2 → R1→ R4 → R3	
BGP	PC1	R1 → R4 → R1 → R2 → R3	
	PC2	R1 → R4 → R1 → R2 → R3	

Considering that the asterisk (*) represents a 'Request timed out', we can conclude:

- Without a protocol: The route for PC1 is R1 → R2 → R3, while for PC2, there is a delay (Request timed out) after R1 → R4, indicating a lack of connectivity.
- RIPv2: For PC1, the route is R1 → R4 → R3, and for PC2, there is again a delay (Request timed out) after R1 → R4, indicating that there hasn't been a significant improvement compared to the absence of a protocol.
- OSPF: For both PCs, the route is R1 → R2 → R3, without any interruptions, representing a significant improvement compared to the absence of a protocol and compared to other protocols like RIPv2.

- The EIGRP protocol provides an optimal route to Server1 for both PCs, without any delay or "Request timed out." Thus, in this specific scenario, EIGRP is as efficient as OSPF in providing a minimal path to the destination.
- The BGP protocol provides the same route to Server1 for both PCs, but the route is longer and involves more hops than OSPF and EIGRP. Although there are no delays or "Request timed out" in this route, its complexity and length could potentially affect performance and efficiency depending on the network configuration and specific requirements.
- Therefore, in this scenario, OSPF and EIGRP remain the most efficient choices for obtaining a minimal path to Server1.

3. ROUTING PROTOCOLS ANALYSIS USING CISCO EQUIPMENT

Cisco 880 routers are fixed configurable devices providing secure communication solutions. They offer various connectivity options, including 3G, Metro Ethernet, and DSL technologies, ensuring adaptability to available network environments. With 802.11n wireless functionality, they enable LAN and WAN mobility crucial for remote connections. Advanced security services like firewall and VPN encryption protect networks and data against cyber threats. QoS features prioritize voice and video traffic, ensuring consistent performance. Cisco Configuration Professional simplifies setup, while centralized management capabilities facilitate remote network monitoring and administration, enhancing efficiency and convenience without physical presence at the router location [12].

The Cisco 1900 ISR (Integrated Services Router) is a modular, flexible device designed for small to medium-sized networks. It excels in:

- Efficiently managing data, voice, and video traffic simultaneously with robust processing power.
- Modularity and flexibility through expansion slots.
- Versatile connectivity, including LAN and WAN ports, and support for wireless technologies.
- Advanced security features.
- Integrated services such as routing, switching, VoIP, and unified communications.
- Advanced management capabilities provided by the Cisco IOS operating system and support for standard management protocols [12].

In the physical implementation of the project, we used a Maguay Workstation along with its network cards to build the proposed network. It is a high-powered workstation utilizing Xeon and Intel Core Haswell processors, suitable for data server or application emulation purposes. To precisely monitor data from the simulated network below, we utilized a laptop directly connected to the studied network. Tests were conducted using the laptop's network card, linked to a router interface. The technical specifications of the HP 250 G7 Laptop include an i5 processor, Ethernet port, and Windows 11 operating system.

The network topology, illustrated in Figure 12, comprised three CISCO 800 (881) routers, denoted as R1, R2, and R3, and one CISCO 1900 (1921) router serving as R4.

Figure 12. The physical network topology.

Each device had to be configured as in Packet Tracer. The connections between routers were made using 5m FTP cables. Just like in the Packet Tracer simulation, 50 successive tests were performed from one device to another. The ping test results from the laptop to the PC are presented in Table IV.

Table 4. Results of the "ping" Test from Laptop to Pc, 5m Cable

Protocol	Test number	Minimum (ms)	Maximum (ms)	Average (ms)
Without protocol	Test 1 and 50	3	6	4
RIPv2	Test 3	<1	6	4
OSPF	Test 1, 12 and 15	<1	4	3
EIGRP	Test 4 and 15	<1	3	2

BGP protocol could not be currently implemented due to equipment limitations.

Strict analysis of performance, based on minimum, maximum, and average values from the given table, shows that the EIGRP protocol is the best because:

- EIGRP has the lowest minimum and average times, indicating excellent performance and consistency in providing routes with very short response times.
- Additionally, EIGRP has the lowest maximum time, meaning there are no extremely high values negatively impacting overall performance.
- The obtained data suggests that EIGRP is the most efficient and consistent protocol in providing routes with short response times between the Laptop and PC devices.

Therefore, based on the data from the table, EIGRP can be considered the best protocol in terms of performance in this specific network.

4. CONCLUSIONS

From the obtained data (Figures 2–12 and Tables 1–4), many of the time values are 0 milliseconds, indicating that transit through intermediate nodes occurred almost instantaneously, which is unlikely in real-world

conditions. However, in some instances, routers may report response times of 0 ms due to either their inability to precisely measure transit time or because the actual delay is extremely small. Therefore, such values should be interpreted as sub-millisecond rather than truly zero, reflecting the limitations of time measurement rather than actual performance.

A critical observation is that minimum values should not exceed maximum values. When such inconsistencies occur—as seen in the case of BGP at hop 4 (minimum: 10 ms; maximum: 0 ms)—they indicate irregularities in measurement, possibly caused by temporary network congestion, processing delays, or anomalies in response reporting.

Based on the overall analysis, the EIGRP protocol demonstrated the best performance, followed by BGP, OSPF, RIPv2, and finally the configuration without a specified routing protocol.

Comparative insights based on Tables 1, 2, and 4 are as follows:
- EIGRP: Minimum and average times are similar, with the maximum time being lower in the physical implementation.
- OSPF: Minimum and average times are also close, and the maximum time is again lower in the physical implementation.
- RIPv2: Minimum and average times remain consistent, but the maximum time is higher in the simulation.
- Without protocol: All values are lower in the Packet Tracer simulation compared to the physical setup.
- BGP: Could not be physically implemented; hence, it was excluded from direct comparison.

The discrepancies between simulation results (Packet Tracer) and physical implementations using Cisco hardware are attributable to several factors. Simulations abstract and simplify many network processes for ease of modeling and faster execution, lacking the hardware-specific processing delays, interface characteristics, and external factors (e.g., electromagnetic interference) present in real-world environments. Additionally, the software emulation of protocols may not fully capture proprietary or low-level operational nuances of actual Cisco devices.

Notably, the superior performance of EIGRP in hardware environments can be attributed to several architectural and protocol-specific advantages. EIGRP, being a Cisco proprietary protocol, benefits from tight integration with Cisco hardware, allowing optimized performance through mechanisms such as rapid convergence, efficient use of Diffusing Update Algorithm (DUAL), and caching of neighbor and routing information. This reduces processing overhead and enables faster decision-making during route changes. In contrast, OSPF, while standardized and interoperable across platforms, involves more complex SPF calculations and periodic link-state advertisements, which can increase CPU load and convergence time, especially in large or dynamic topologies. These differences explain why EIGRP tends to outperform OSPF in Cisco-based physical environments.

5. REFERENCES

[1] C.G. Dumitrache, G. Predusca, L.D. Circiumarescu, N. Angelescu, D. Puchianu, „Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer," 5th International Symposium on Electrical and Electronics Engineering (ISEEE), 2017, pp.1-6.

[2] A. Nastase, L.D. Circiumarescu, G. Predusca, N. Angelescu, D.C. Puchianu, „Simulation based of comparative study of Routing Protocols for Real Time Applications," 22nd International Conference on Control Systems and Computer Science, 2019, pp.531-535.

[3] [Online], available: https://www.ietf.org/blog/ipv6-internet-standard/ accessed on March 15, 2025.

[4] S.V. Mantena, S. Jayasundar, D.K. Sharma, J. Veerappan, M. A. Bennet, S. Sengan, R. Rangasam, „Design of Dual-Stack, Tunneling, and Translation Approaches for Blockchain-IPv6," Intelligent Systems and Sustainable Computing. Smart Innovation, Systems and Technologies, Springer, 2022, vol. 289.

[5] S. Khan, A. Chugh, „Comparative Analysis of Dyanamic Routing Protocol using Packet Tracer 6.0.2 with Dyanamic BW," International Journal of Science and Research, 2018, pp.1176-1183.

[6] H. Karna, V. Baggan, A.K. Sahoo, P.K. Sarangi, „Performance analysis of interior gateway protocols (IGPs) using GNS-3," 8th International Conference System Modeling and Advancement in Research Trends (SMART), 2019, pp.204-209.

[7] M.A. Kamal, M.M. Alam, M.S. Mazliham, „Routers perspective simulation-based analysis of EIGRP and OSPF routing protocol for an organization model," International Journal of Innovative Technology and Exploring Engineering, volume 9, issue 4, 2020, pp.2013-2019.

[8] Zeeshan Basit, Mujahid Tabassum, Tripti Sharma, Muhammed Furqan, Abdul Quadir Md, „Performance analysis of OSPF and EIGRP convergence through IPsec tunnel using Multi-homing BGP connection," Materials Proceedings, vol.62, 2022, pp.4853-4861.

[9] J.O. Ifeanyi, D.E. Ikiomoye, "Comparative Study of EIGRP and OSPF Protocols based on Network Convergence" *International Journal of Advanced Computer Science and Applications,* vol. 11, no. 6, 2020, 39-45.

[10] M. Bolanowski, T. Byczek, „Measure and compare the convergence time of network routing protocols," ITM Web of Conferences, vol. 21, 2018, pp.1-9.

[11] A. Manzoor, M. Hussain, S. Mehrban, „Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols", Computer Standards & Interfaces, vol. 68, 2020.

[12] [Online], available: https://www.cisco.com/c/en/us/ products/ collateral/routers, accessed on March 15, 2025.