IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study On Network Layer Protocols And Their Role In Packet Delivery Efficiency

Mr. Rahul Kumar (Assistant Professor)
Parul Kashyap (M.Tech Student)
Department of Computer Science & Engineering
Bharat Institute of Technology, Meerut, India

Abstract- A straightforward framework for creating wireless network protocols incorporates localized broadcasting and routing. The basic foundation is predicated on the cost-benefit ratio of specific choices, such cutting back on the number of distances. In this wireless network application, one of the main networks is the routing protocol. These are some of the most often used routing strategies in network layers. In the distributed routing in every node determines if routing through a certain neighbor is less expensive than using nodes that are already in use. Wireless channels in "adhoc" networks have bandwidth limitations. A localized strategy based on "on-demand route discovery" is employed in dynamic ad hoc networks by flooding destinations. However, because flooding has power and bandwidth limitations, it is ineffective as a routing technique in wireless networks. The term "localized protocols" refers to the quantity of data needed (i.e., it provides the typical number of messages sent by each protocol node). It can be either local or global in a purely localized protocol. As a result, the project's objective characterizes the idea as a broad framework of several current protocols. The cost measure, which is predicated on the assumptions for choosing the shortest routing path, and the progress measure, which is predicated on the advancements made towards the destination, form the basis of the proposed framework for the localized routing scheme. This scenario is implemented using a network simulator.

***Keywords:-* Packet Delivery, Routing Protocols, Network Layer, IPv4, IPv6, ICMP, RIP, and Network Efficiency**

I. INTRODUCTION

Computer networks are now essential due to the development of digital communication and the internet's rapid expansion. The Open Systems Interconnection (OSI) paradigm separates communication duties into many levels in order to handle complexity. The Network Layer (Layer 3) is the most important of these since it guarantees end-to-end packet delivery over intricate networks, particularly in cases where hosts are not physically connected. Packet forwarding, path determination, and logical addressing are all handled by this layer. Logical addressing systems are provided by protocols such as IPv4 and IPv6, while error handling and diagnostics are supported by ICMP. Routing protocols like BGP, OSPF, and RIP control how packets move across several networks to get to their destination. Enhancing the effectiveness, dependability, and scalability of data transfer requires an understanding of how these protocols operate. The impact of several network layer protocols on packet delivery performance is examined in this dissertation, with a focus on latency, packet loss, bandwidth usage, and route stability [1]. When sending a message from a source node to a destination node (in a sensor or ad hoc wireless network), the routing task is taken into consideration. The transmission radii are constrained by propagation path loss. As a result, routes between two network sites may include hops through additional network hosts [2]. The network's nodes can be moving (vehicles, humans, small robotic equipment), static most of the time (books, projectors, furniture), or static (thrown from an aircraft to a remote area or a poisonous environment). Since wireless sensor networks significantly increase our capacity to monitor and manage the physical environment from far-off places and enhance the accuracy of data gathered through cooperation among sensor nodes and online information processing at those nodes, they are probably going to be widely used in the near future. Information gathering and processing will be transformed in many instances by networking these sensors, which will enable them to coordinate among themselves on a bigger sensing goal[15]. Ad hoc networks are a type of wireless network that has drawn a lot of interest lately. Wireless hosts that connect to one another without a fixed infrastructure make up mobile ad hoc networks.

II. Literature Review

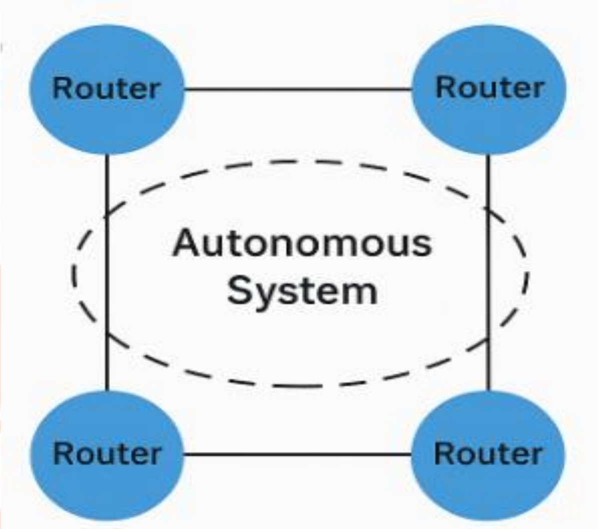
Since the beginning of the internet, a great deal of study has been done on the protocols of the Network Layer, which is the core of communication in a packet-switched network. A thorough analysis of the literature shows that network protocols are always changing, delivery methods are getting better, and scalability and fault tolerance are becoming more and more important. Postel (1981) explicitly defined Internet Protocol version 4 (IPv4), the fundamental protocol at the Network Layer, in RFC 791. While useful in the early days of networking, the 32-bit addressing system it established was insufficient as the number of devices linked to the internet increased exponentially. Huitema (1996) and other researchers stressed the need to switch from IPv4 to IPv6, which Deering and Hinden (1998) specified in RFC 2460. [4]A 128-bit address space was made available by IPv6, which also enhanced routing capabilities and added features like stateless address auto configuration (SLAAC) and increased QoS (Quality of Service) support. Routing protocols have a significant impact on network performance in addition to IP addressing. RFC 1058 outlines the Routing Information Protocol (RIP), a distance-vector protocol that use hop count as a routing metric [14]. RIP's sluggish convergence and vulnerability to routing loops have been cited as reasons for its inefficiency in large-scale networks [6], despite its seeming simplicity. Studies that have described the drawbacks of RIP and made the case for more sophisticated solutions include those by Stallings (2013) and Bhuyan & Pattanayak (2018). RFC 4271 describes the Border Gateway Protocol (BGP), which facilitates routing between autonomous systems (ASes) at the inter-domain level. BGP's capacity to offer loop-free pathways and handle intricate routing regulations was demonstrated by[3] Rekhter & Li (1995). BGP's policy-driven paradigm facilitates load balancing, route prioritization, and prefix filtering, and it plays a crucial role in maintaining the internet's global routing table [13]. Scholars such as Jain & Paul (2013) have examined how BGP and SDN (Software-Defined Networking) interact, highlighting BGP's flexibility in cloud-based systems. Error reporting and diagnostics are made easier by the Internet Control Message Protocol (ICMP), another essential Network Layer component. In RFC 792, Postel (1981) defined ICMP as a way to give input on network conditions. ICMP packets are used by tools like ping and traceroute to assess path quality and identify unreachable nodes. ICMP has proved essential for network administration and performance monitoring despite its portability.IPv4 and IPv6 performance comparisons are the main topic of more recent research. According to research by Saini & Gupta (2020), IPv6 improves mobility support and simplifies routing tables [5]. In a similar vein, Choudhury (2019) addressed security issues and claimed that, in contrast to IPv4, IPv6 has IPsec as a required feature. It has also been investigated how well routing protocols perform in Mobile Ad Hoc Networks (MANETs). A comparative analysis of RIP, OSPF, and more recent protocols like AODV and DSR in dynamic wireless environments was presented by Al-Sakran (2012). According to these results, adaptive routing techniques are necessary to enhance packet delivery in unstable topologies. Furthermore, theoretical statements have been validated using simulation-based research. By simulating network traffic under various loads using NS2 and GNS3, Radwan & Abdelghany (2020) demonstrated how protocol selection impacts throughput, packet delivery ratio, and end-to-end delay.

III. METHODOLOGY

A theoretical-comparative approach designed to comprehend the underlying workings of Network Layer protocols and how they affect the effectiveness of packet delivery. The study is set up to record and examine six important protocols: BGP, OSPF, RIP, ICMP, IPv4, and IPv6. These protocols' architectural layout, routing logic, scalability, fault tolerance, and function in end-to-end data transfer are all taken into consideration [16]. The study's main component is a qualitative analysis of current RFC documents, scholarly research publications, and network textbooks. Specific performance criteria, such as packet loss rate, average latency, route convergence time, and handling of dynamic network situations, serve as the basis for the evaluation. To compare protocol features in an organized manner, tabular representations and flow diagrams are used.

- ***BGP (Border Gateway Protocol)-***

Autonomous systems (ASes) on the internet can share reach ability and routing data using the Border Gateway Protocol (BGP) in Figure 1, a path vector routing protocol. Currently the de facto standard for inter-domain routing, it is defined in RFC 4271. As an Exterior Gateway Protocol (EGP), BGP makes it easier for networks that are independently managed to route to one another. Because BGP employs policy-based routing, network managers can specify routing choices based on policies as opposed to merely measurements like bandwidth or hop count [7]. It keeps track of IP networks, or "prefixes," and chooses the optimal path based on attributes such as AS path, next hop, and local preference. In contrast to distance-vector or link-state protocols, BGP supports intricate routing decisions worldwide and prevents loops through AS-path filtering.



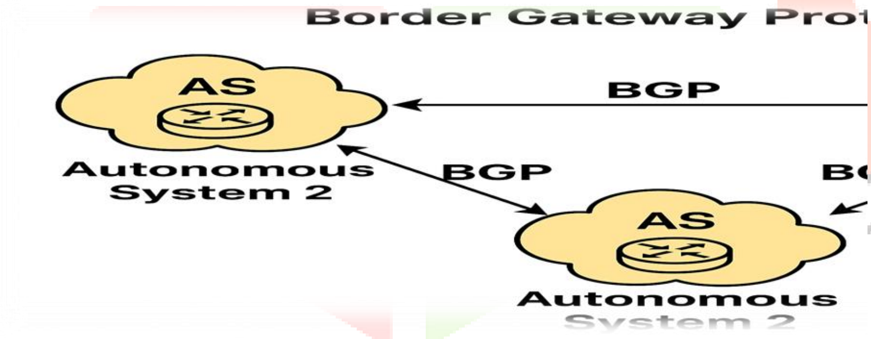


Figure 1: Diagram of Border Gateway Protocol

- ***OSPF (Open Shortest Path First) –***

One popular internal gateway protocol (IGP) for directing IP packets within a single autonomous system is called Open Shortest Path First (OSPF) Figure 2. This routing system is known as link-state, which means that every router keeps an exhaustive map of the network topology in a database known as the link-state database (LSDB). OSPF determines the optimal route to each destination using Dijkstra's Shortest Path First (SPF) algorithm. In order to lower routing cost and increase scalability, it divides big networks into smaller sections using a hierarchical structure [8]. All other areas must connect to Area 0, also referred to as the backbone area, which is located in the center. Internal routers, backbone routers, autonomous system boundary routers (ASBRs), and area border routers (ABRs) are the four types of routers that make up OSPF. Several OSPF message types, including Hello packets, Database Description (DBD), Link-State Request (LSR), Link-State Update (LSU), and Link-State Acknowledgment (LSAck), are used transmit routing information. *Figure 2: OSPF*

- ***RIP (Routing Information Protocol)-***

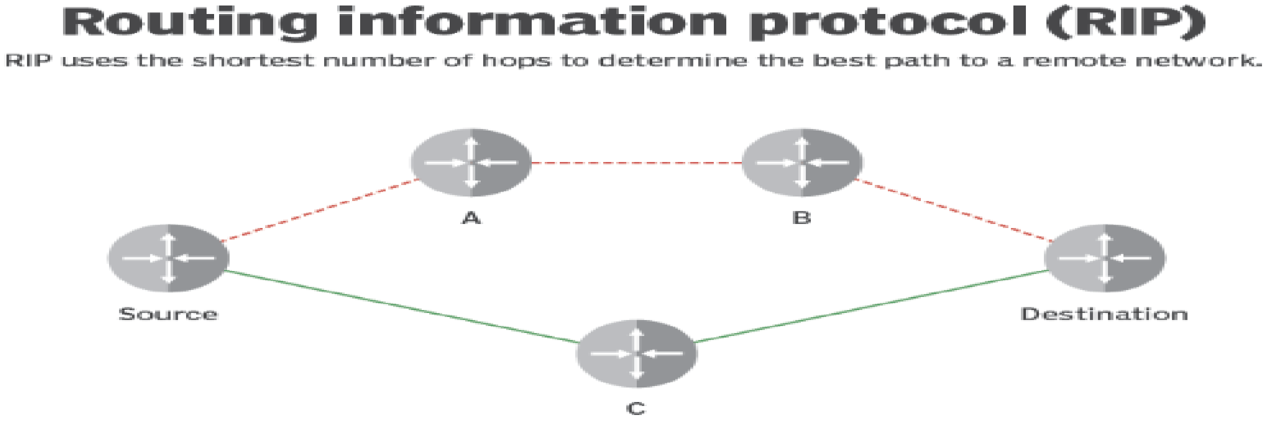

Routing information protocol (RIP)
RIP uses the shortest number of hops to determine the best path to a remote network.
A
B
Source
Destination
C

Figure 3: RIP

One of the earliest and most basic distance vector routing techniques utilized in computer networks is called (RIP). In Figure 3 a local area network or autonomous system, it facilitates information sharing among routers to identify the optimal data forwarding channel. Each hop signifies a switch from one router to another, and RIP utilizes hop count as its routing statistic. RIP is only appropriate for small networks since it has a maximum hop count of 15, which means that any destination more than 15 hops away is deemed unreachable. Every 30 seconds, RIP routers share all of their routing tables with nearby routers, which can result in high bandwidth consumption and sluggish convergence when the network topology changes. RIP determines the optimal route to a location using the Bellman-Ford algorithm [10]. There are three variations of RIP: RIPng (RIP next generation), RIP version 1 (RIPv1), and RIP version 2 (RIPv2). While RIPv2 is classless, allows CIDR, and offers authentication, RIPv1 is a classful protocol that does not support subnet information. RIPng adds capabilities appropriate for contemporary IP addressing and is made for IPv6 networks. Advanced capabilities like route summarization and policy-based routing, as well as hierarchical routing, are not supported by RIP. RIP is still utilized in legacy systems and for instructional purposes, even though it is mainly out of date for large networks. It is essential to comprehending routing protocols and how they have changed over time.

- ***ICMP (Internet Control Message Protocol)-***

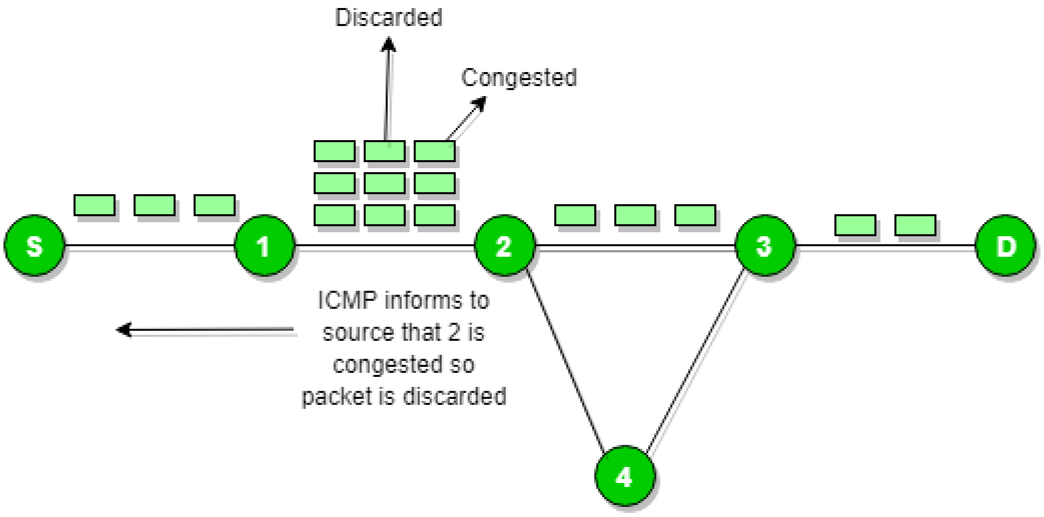

Discarded
Congested
S
1
2
3
D
4
ICMP informs to source that 2 is congested so packet is discarded

Figure 4: ICMP

A fundamental protocol in the Internet Protocol (IP) family, Internet Control Message Protocol (ICMP) is primarily used for network diagnostics and issue reporting. In Figure 4 contrast to TCP or UDP, ICMP is used to deliver control messages between network devices, such routers and hosts, rather than to send user data. It is crucial for preserving a network's functionality and health and functions at the network layer (Layer 3). Network tools like ping and traceroute, which assist administrators in determining connection and tracking packet paths, frequently employ ICMP. ICMP returns error messages such as "Destination Unreachable," "Time Exceeded," or "Redirect" when a packet is unable to reach its destination.[9] The sender can better understand what went wrong with the help of these messages. For instance, a router will utilize ICMP to transmit a "Time Exceeded" message if it discards a packet because its TTL (Time to Live) has passed. Typically, IP packets incorporate ICMP messages.ICMP messages come in various forms and codes. The ping command uses Echo Request and Echo Reply to check for host availability. ICMP is not regarded as trustworthy and does not ensure delivery. Additionally, it only alerts the source to the issue rather than fixing it. Neighbor Discovery Protocol (NDP) and other more sophisticated capabilities are included in ICMPv6, which replaces ICMP in IPv6.

- ***IPv4 (Internet Protocol version 4)-***

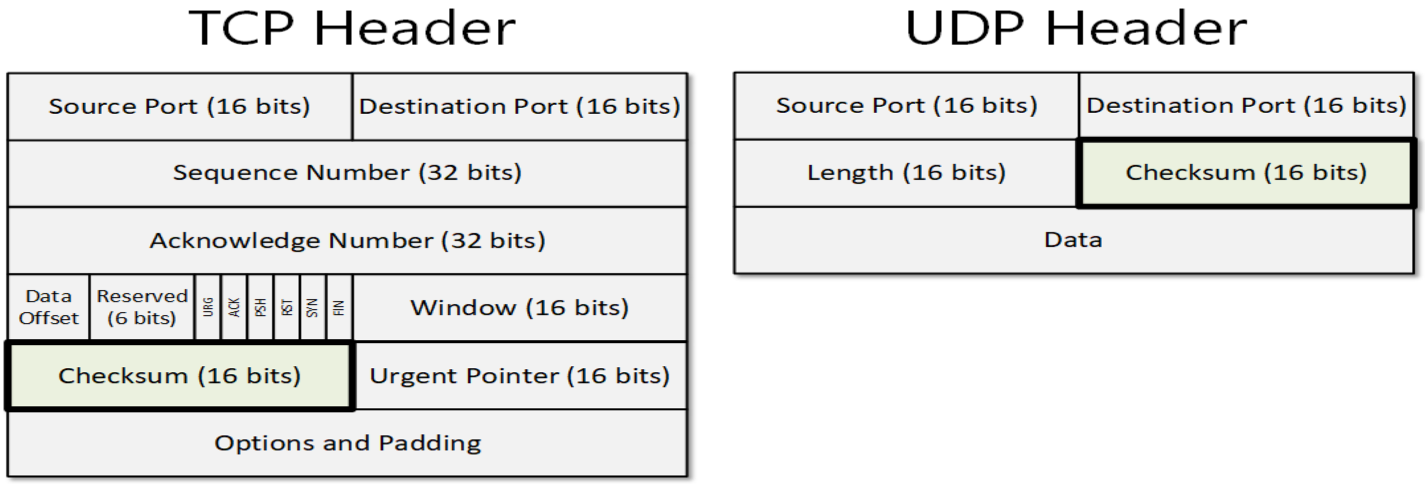


Figure 5: IPv4

One of the most popular networking protocols is IPv4 (Internet Protocol version 4), Figure 5 which was created to make it easier for devices to communicate with one another over the internet. Despite the advent of more recent iterations, including IPv6, it was created in the 1980s and continues to serve as the foundation for internet communication. Because IPv4 addresses are 32-bit, there are approximately 4.3 billion possible unique IP addresses[18]. These addresses, like 192.168.1.1 [11], are usually written in a dotted-decimal format with four octets, each of which is represented by an integer between 0 and 255. In order to ensure that data reaches its intended destination, the protocol, which functions at the network layer, is in charge of routing data packets between devices. One of IPv4's main advantages is its ease of use and broad acceptance, which makes it the most widely used protocol for internet device address assignment. However, worries regarding IPv4 address exhaustion have arisen as a result of the internet's explosive expansion and the rise in connected devices [17]. The switch to IPv6, which provides a far bigger address space, was spurred by this scarcity. Network Address Translation (NAT), which enables several devices in a private network to share a single public IPv4 address, is one method by which IPv4 and IPv6 continue to coexist in spite of this.

- ***IPv6 (Internet Protocol version 6)-***

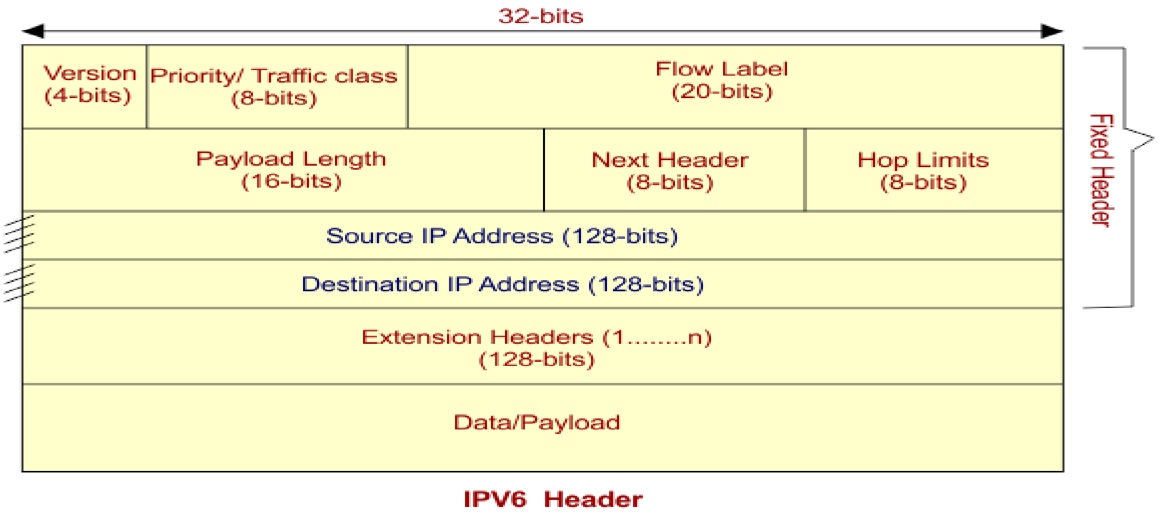


Figure 6: IPv6

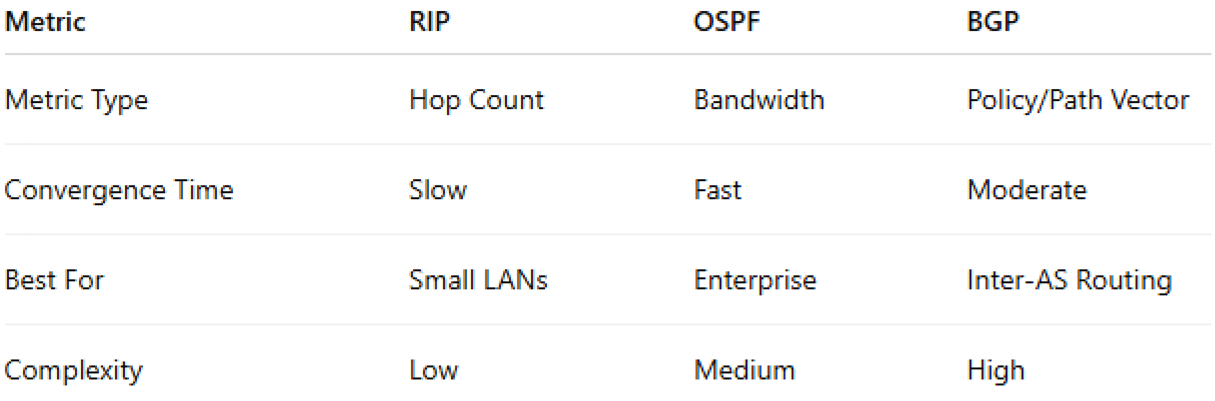
The most recent iteration of the Internet Protocol, known as IPv6 (Internet Protocol version 6), was created to overcome the shortcomings of IPv4 [20]. With a substantially bigger address space than IPv4's 32-bit addresses, IPv6 was introduced in response to the growing need for devices connected to the Internet. About 340 undecillion (3.4×10^38) unique IP addresses are made possible by this extension, more than enough to handle the increasing number of Internet-connected devices worldwide. By enabling automatic IP address assignment and simplifying network configuration, Figure 6 IPv6 also makes managing big networks simpler. The enhanced security model of IPv6 is one of its key characteristics [12]. With improved encryption and authentication methods for safe data transfer, IPv6 was created with IPsec (Internet Protocol Security) support as a required feature. Compared to IPv4, which depends on other protocols for security, IPv6 is more resistant to assaults because of its inherent security. Additionally, IPv6 enhances network speed with features like streamlined header formats and more effective routing. Additionally, it facilitates multicast communication, which eases network congestion and makes better use of available bandwidth. Despite these benefits, IPv6 adoption has been sluggish, mostly because of incompatibilities with current IPv4 infrastructure.

IV. COMPARISON AND CHALLENGES

RIP: Hop-count based; sluggish convergence and prone to routing loops. Ideal for static, tiny networks.

OSPF: To increase efficiency, networks are divided into sections using Dijkstra's algorithm. It is suitable for enterprise LANs and converges quickly.

BGP: Facilitates policy-based routing and inter-AS communication. For the internet backbone, it is intricate yet incredibly adaptable.



Metric	RIP	OSPF	BGP
Metric Type	Hop Count	Bandwidth	Policy/Path Vector
Convergence Time	Slow	Fast	Moderate
Best For	Small LANs	Enterprise	Inter-AS Routing
Complexity	Low	Medium	High

Table: 1 Comparison between RIP, OSPF and BGP

- ***Challenges in Packet Delivery***

i. **Changes in Dynamic Topology**:- The route to the target might change quickly in networks with constantly shifting configurations (such as mobile or Internet of Things networks). [19]Outdated routing tables result from this, causing packets to be lost or delayed until convergence.

ii. **Overflowing buffers and congestion:-** Packet loss or queuing delays may result from high traffic loads exceeding the router buffer capacity. Especially in core networks, congestion results in higher latency and lower throughput.

iii. **Loops in Routing:-** Packets may repeatedly circulate without ever reaching their destination if routing tables are not updated appropriately. Timeouts and bandwidth waste result from this, hence loop avoidance algorithms or TTL fields must be used to stop it.

iv. **Unbalanced Routing:-** The return path is not the same as the path from the source to the destination. In addition to making diagnostics challenging, this can interfere with protocols that rely on symmetric paths, including those that use RTT (round trip time) measurements.

v. **Fragmentation of packets:-** Packets are fragmented when they surpass a link's maximum transmission unit (MTU), which raises processing overhead and loss risk. Data delivery that is not complete can result from improper processing of fragments.

vi. **Absence of guarantees for Quality of Service (QoS):-** VoIP and real-time video are examples of important traffic that may experience jitter or delays in the absence of QoS systems. All packets are handled equally on best-effort networks, which frequently jeopardize timely delivery.

V. CONCLUSION

The smooth operation of data communication across networks depends on the Network Layer. Logical addressing, routing, and effective packet forwarding are its duties, and they serve as the foundation for dependable and expandable network architecture. The internal workings, benefits, and drawbacks of several important network layer protocols, such as IPv4, IPv6, ICMP, RIP, OSPF, and BGP, were investigated in this paper. Every protocol has different uses and contexts, and how well they transmit packets depends largely on the size, traffic patterns, topology, and policy requirements of the network. Even though it is still widely used, IPv4 has issues with scalability and address exhaustion. In contrast, IPv6 offers remedies through better packet processing and a bigger address space. ICMP, which is frequently underutilized, is essential for identifying and fixing network problems. From hop-based distance vectors to complex policy-driven and link-state models, routing protocols like RIP, OSPF, and BGP demonstrate a range of approaches for route discovery and management.External issues including congestion, routing loops, changing topologies, and asymmetric networks also affect how efficiently packets are delivered. Network administrators must carefully select and configure protocols that complement their infrastructure capabilities and corporate goals in order to guarantee reliable and effective delivery. Additionally, network-layer solutions must be flexible and robust due to the growing complexity of network systems brought about by cloud services, mobile computing, and Internet of Things devices. The study emphasizes how crucial it is to choose the right protocols and optimize their deployment with the right error-handling, QoS, and real-time monitoring. To sum up, the study offers a solid theoretical basis for comprehending network layer protocols and how they affect the effectiveness of packet delivery. Future studies can focus on the security implications of protocol design and implementation, the impact of SDN in dynamic routing, and real-time protocol simulations.

REFERENCES

[1] Deering, S., & Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification* (RFC 2460). Internet Engineering Task Force. https://doi.org/10.17487/RFC2460

[2] Postel, J. (1981). *Internet Protocol* (RFC 791). Internet Engineering Task Force. https://doi.org/10.17487/RFC0791

[3]Postel, J. (1981). *Internet Control Message Protocol* (RFC 792). Internet Engineering Task Force. https://doi.org/10.17487/RFC0792

[4]Rekhter, Y., & Li, T. (2006). *A Border Gateway Protocol 4 (BGP-4)* (RFC 4271). Internet Engineering Task Force. https://doi.org/10.17487/RFC4271SCIRP

[5] Moy, J. (1998). *OSPF Version 2* (RFC 2328). Internet Engineering Task Force. https://doi.org/10.17487/RFC2328

[6] Hedrick, C. (1988). *Routing Information Protocol* (RFC 1058). Internet Engineering Task Force. https://doi.org/10.17487/RFC1058SCIRP

[7]Baker, F. (1995). *Requirements for IP Version 4 Routers* (RFC 1812). Internet Engineering Task Force. https://doi.org/10.17487/RFC1812

[8] Callon, R. (1990). *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (RFC 1195). Internet Engineering Task Force.
https://doi.org/10.17487/RFC1195

[9]Rosen, E. C., & Rekhter, Y. (1999). *BGP/MPLS VPNs* (RFC 2547). Internet Engineering Task Force. https://doi.org/10.17487/RFC2547

[10] Rosen, E. C., Viswanathan, A., & Callon, R. (2001). *Multiprotocol Label Switching Architecture* (RFC 3031). Internet Engineering Task Force. https://doi.org/10.17487/RFC3031ResearchGate

[11] Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson Education.

[12] Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

[13] Stallings, W. (2017). *Data and Computer Communications* (10th ed.). Pearson.

[14] Forouzan, B. A. (2017). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.

[15] Al-Sakran, H. O. (2012). A comparative study of routing protocols in mobile ad hoc networks. *International Journal of Computer Science and Network Security*, 12(2), 89–98.

[16] Bhuyan, B., & Pattanayak, B. K. (2018). Comparative study of RIP and OSPF routing protocols. *International Journal of Advanced Research in Computer Science*, 9(2), 45–49.

[17] Choudhury, T. R. (2019). IPv6 deployment and security considerations. *International Journal of Computer Applications*, 182(23), 20–25.

[18] Saini, J., & Gupta, N. (2020). Network layer performance analysis in IPv4 and IPv6. *Journal of Emerging Technologies and Innovative Research*, 7(5), 1015–1019.

[19] Jain, R., & Paul, S. (2013). Network virtualization and SDN for cloud computing: A survey. *IEEE Communications Magazine*, 51(11), 24–31. https://doi.org/10.1109/MCOM.2013.6658648

[20] Radwan, A., & Abdelghany, M. (2020). Performance evaluation of routing protocols in MANETs. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2020.01.008