Review Article

"The Comprehensive Review: Internet Protocol (IP) address a primer for digital connectivity"

Abstract: The Internet Protocol (IP) is the rule book that governs how data is addressed and routed across networks on the internet. Think of it as the postal system for the digital world. This addressing system allows routers, the digital mail carriers, to efficiently transfer packets between devices and networks until they reach their destination. It ensures data reaches the right place by assigning addresses and enabling efficient routing. IP also encompasses various protocols and services, such as ICMP (Internet Control Message Protocol) for error reporting and diagnostics, and DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment. Additionally, IP can be configured to support different transmission modes, including uni-cast, multicast, and broadcast, catering to diverse communication requirements. Adopting technology that has been researched and developed commercially offers the military a cost-effective method of implementation. IP systems enable the forces to share a common network that supports voice, video, and data sharing. This systematic review article initially highlighted the basics on IP and lastly the brief discussion regards data gram format, NAT, IPv4, IPV6 IP fragmentation, CIDR, TCP and UDP individually.

Keywords: Datagram format; addressing; network address translation; IPv2; IPv4; IPv6; IP fragmentation/ reassembly; CIDR; DHCP; TCP -UDP.

1. INTRODUCTION

The IP is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed [1]. The IP has a unique address to receive mail, IP gives each device on a network a special identification tag called an IP address. The IP stands as the linchpin, facilitating the exchange of information across diverse networks worldwide. Understanding the fundamentals of IP is essential for navigating the intricacies of modern connectivity. This approach, known as packet switching, allows for more efficient utilization of network resources and greater resilience to network disruptions. IP addresses serve as unique identifiers for devices connected to the Internet [1-2].

1.1. Genesis of Connectivity: The genesis of IP traces back to the nascent stages of computer networking, where the need to interconnect disparate systems gave rise to protocols that could facilitate data exchange. As networks expanded beyond localized domains, a standardized protocol was imperative to ensure seamless communication across heterogeneous environments.

1.2. Foundations of IP: It operates within the IP Suite, a comprehensive framework encompassing a myriad of protocols that collectively enable robust and versatile network communication. IP's primary responsibilities include addressing, routing, and fragmentation of data packets, ensuring that information traverses the network efficiently and reliably.

1.3. Connectionless Paradigm: This connectionless paradigm, facilitated by packet switching, allows for dynamic routing and efficient utilization of network resources. Moreover, it imbues IP with inherent resilience, enabling it to adapt to network fluctuations and disruptions seamlessly.

1.4. Addressing and Routing: These addresses, expressed in either IPv4 or IPv6 format, serve as virtual coordinates that enable routers to route packets to their intended destinations. IPv4, characterized by its 32-bit addressing scheme, was instrumental in laying the foundation of the Internet.

1.5. Protocol Ecosystem: IP encompasses a rich ecosystem of protocols and services that augment its functionality and reliability. From the Internet Control Message Protocol (ICMP), which facilitates error reporting and diagnostics, to the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which govern the transport layer of the Internet Protocol Suite, each protocol plays a vital role in shaping the landscape of digital communication [2-6].

2. DATAGRAM FORMAT

The format of data that can be recognized by IP is called an IP datagram. It consists of two components, namely, the header and data, which need to be transmitted. The fields in the datagram, except the data, have specific roles to perform in the transmission of data.

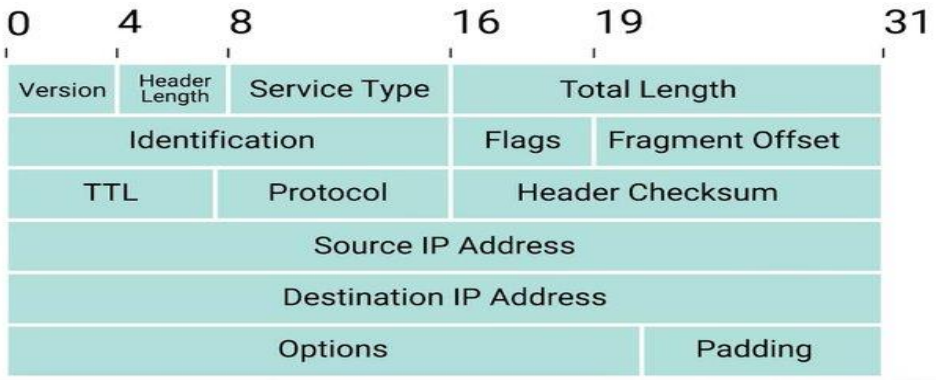

Figure 1: The representation of IP datagram format

However, datagram are often associated with the User Datagram Protocol (UDP), a transport layer protocol that utilizes datagram for data transmission [6-7]. The breakdown of datagram format in the context of UDP:

Structure: The datagram consists of two main parts, which are discussed below:

- **Header:** This is a small (usually 8 bytes) fixed-size section containing crucial information for routing the datagram. It typically includes fields like:
    - Source and destination port numbers (identifying applications on sending and receiving devices)
    - Length of the datagram (including both header and data)
    - Checksum for error detection
- **Payload (Data):** This is the actual user data being transmitted. The size of the payload can vary depending on the application and network limitations [8-9].

3. NAT: NETWORK ADDRESSING TRANSLATION

NAT, or Network Address Translation, is a fundamental technology used in computer networks to manage how devices connect to the internet. It acts as a translator, converting private IP addresses used within a local network to a single public IP address for communication with the wider internet. Network Address Translation is a technique used in networking to modify network address information in packet headers while in transit across a router or firewall [10]. Its primary purpose is to conserve IP addresses, improve security, and enable the sharing of a single public IP address among multiple devices in a private network.

The primary components of NAT include:

3.1. Private and Public IP Addresses: Private IP addresses are reserved for use within a private network and are not routable over the internet. Examples include IP addresses in the ranges of 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Public IP addresses, on the other hand, are globally unique addresses assigned to devices accessible over the internet

3.2. Translation: NAT translates private IP addresses to public IP addresses when packets leave the private network and vice versa. This translation occurs at the network layer of the OSI model.

Benefits: The several benefits discussed as below following:

- **Address Conservation**: NAT enables organizations to use private IP addresses internally, reducing the demand for public IP addresses.
- **Enhanced Security**: By hiding internal network details, NAT provides a level of security against unauthorized access and attacks from external sources.
- **IP Version Transition**: NAT facilitates the transition from IPv4 to IPv6 by allowing IPv6 hosts to access IPv4 resources and vice versa through translation mechanisms [10-11].

Drawbacks: **With** lots of benefits it is necessary to know the few drawbacks as following:

- **End-to-End Connectivity**: NAT can hinder certain applications that require direct communication between hosts, as it alters IP addresses and port numbers in packet headers.
- **Complexity**: Managing NAT configurations, especially in large networks, can be complex and may require careful planning to avoid issues such as address exhaustion or performance degradation [11-14].

4. IPv4 and IPv6

The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. This layer contains hardware devices such as routers, bridges, firewalls, and switches, but it actually creates a logical image of the most efficient communication route and implements it with a physical medium [15]. Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer. In the OSI model, the network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer) [15-17].

4.1. IPv4: IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best-effort delivery model, in which neither delivery is guaranteed, nor is proper sequencing or avoidance of duplicate delivery assured. IP Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type. IPv4 is defined and specified in IETF publication RFC 791. IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for multi-casting, while class E addresses are reserved for military purposes. IPv4 uses 32-bit (4-byte) addressing, which gives 232 addresses.

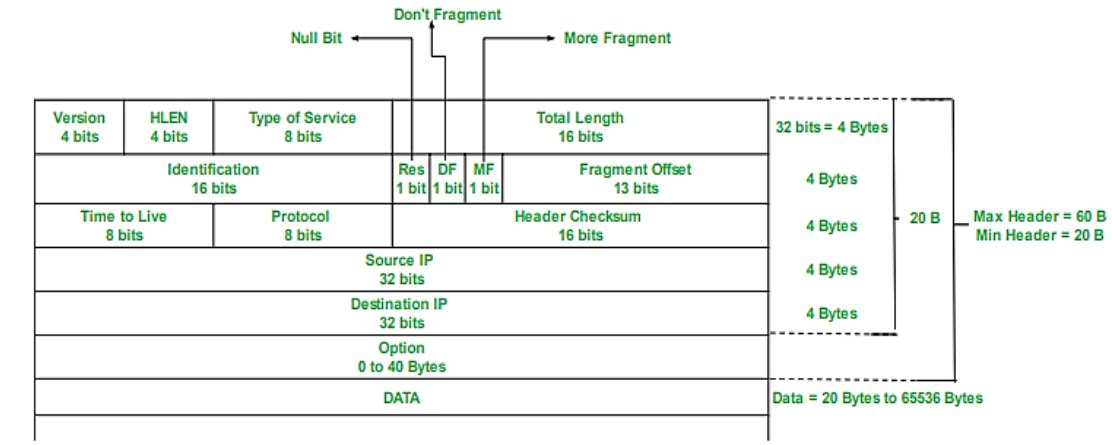

Figure 2: The flow representation of IPv4 datagram format

IPv4 is redesigned entirely. It offers the following features are:

- **Bit Addressing:** IPv4 addresses are 32 bits long, allowing for approximately 4.3 billion unique addresses. However, due to the growth of the Internet, IPv4 addresses are now exhausted in many regions.
- **Hierarchical Addressing Structure:** IPv4 addresses are organized hierarchically into classes (Class A, B, C, D, and E) based on the leading bits of the address, structure allows for efficient routing of packets across network.
- **Subnetting:** IPv4 supports subnetting, which allows a large network to be divided into smaller subnetworks. This enables more efficient use of IP addresses and better network management.
- **Address Resolution Protocol (ARP):** ARP is used in IPv4 networks to map IP addresses to MAC addresses. When a device wants to communicate with another device on the same network, it uses ARP to find the MAC address associated with the IP address.
- **Internet Control Message Protocol (ICMP):** ICMP is used by IPv4 for error reporting, diagnostics, and network management. It includes messages such as "ping" (echo request and echo reply) for testing connectivity between devices.
- **Network Address Translation (NAT):** NAT allows multiple devices on a local network to share a single public IPv4 address. It is commonly used in home and small office networks to conserve public IP addresses.
- **Dynamic Host Configuration Protocol (DHCP):** DHCP is used to dynamically assign IP addresses to devices on a network. It simplifies network administration by automatically providing IP configuration to devices when they connect to the network [17-20].

IPv4 packets consist of a header and a payload. The header contains information such as source and destination IP addresses, packet length, and protocol type. The header format includes fields for version, header length, and type of service, time-to-live, protocol, header checksum, source IP address, and destination IP address. IPv4 supports fragmentation of packets when they exceed the maximum transmission unit (MTU) size of a network. Fragments are reassembled at the destination to reconstruct the original packet. IPv4 does not inherently include built-in security features. However, security can be implemented at higher layers of the networking stack, such as using IPSec for secure communication over IP networks.

4.2. IPv6: Internet Protocol version 6 is the latest revision of the IP and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. This tutorial will help you in understanding IPv6 and its associated terminologies along with appropriate references and examples. This tutorial has been designed to help beginners understand the basic concepts of IPv6 required to work with any TCP/IP based protocols. After completing this tutorial you will find yourself at a moderate level of expertise of IPv6 from where you can take yourself to next levels. Trying to keep the basic functionalities of IP addressing [19-21].

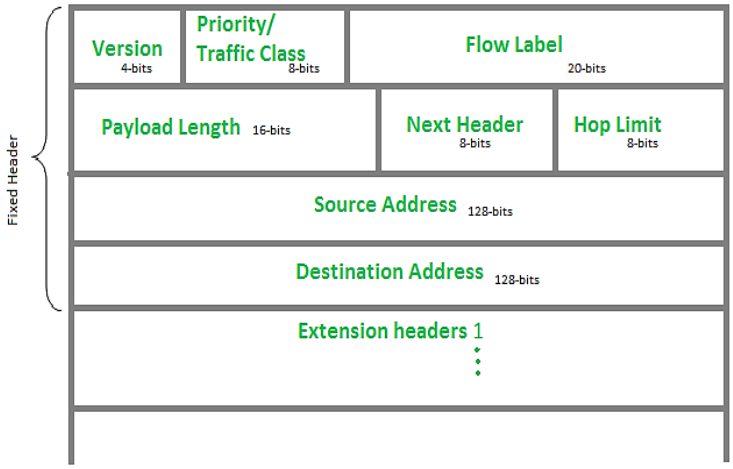

Figure 3: The flow representation of IPv6 datagram format

IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space:** In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses.
- **Simplified Header:** IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header.
- **End-to-end Connectivity:** Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.
- **Auto-configuration:** IPv6 supports both stateful and stateless auto configuration mode of its host devices.

- **Faster Forwarding/Routing:** Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions.
- **IPSec:** Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
- **Mobility:** IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address.
- **Smooth Transition:** Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required [21-24].

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow [25]. The several features of IPV4 and IPv6 discussed in the given **Table 1** as below following:

Table 1: The list of features IPv4 and IPv6 [22-25]

Feature	IPv4	IPv6
Address Size	32 bits	128 bits
Format	Dot-decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Space	Limited	Vastly larger
Security	No built-in security	Supports IPSec for encryption and authentication
Header Structure	More complex	Simpler and more efficient
Autoconfiguration	Requires DHCP server	Stateless Address Autoconfiguration (SLAAC)
Fragmentation	Can be done by sender or router	Done only by sender

5. IP FRAGMENTATION

IP fragmentation is a process used in computer networks to break down large packets into smaller fragments so they can be transmitted across a network that cannot handle large packets. This is necessary because different networks may have different Maximum Transmission Units (MTUs), which is the largest size of a packet that can be transmitted.

Basics of IP Fragmentation:

1. Packet Size and MTU: The MTU is the maximum packet size that a network link can handle without needing fragmentation. If a packet is larger than the MTU of a network segment, it must be fragmented into smaller packets.

2. Fragmentation Process: The original packet is broken down into smaller fragments. Each fragment has its own IP header. These fragments are transmitted separately over the network.

3. Reassembly: The receiving end must reassemble the fragments back into the original packet. This is done using fields in the IP header that help identify and order the fragments correctly [25-27].

Fields Involved in IP Fragmentation: Several fields in the IPv4 header are used to manage fragmentation and reassembly:

1. Identification: A unique identifier for each datagram. All fragments of a single packet share the same identifier.

2. Flags: They consists of 3 bits:

- **Reserved bit (must be 0)**.
- **DF (Don't Fragment) bit**: If set to 1, fragmentation is not allowed. If the packet size exceeds the MTU, it will be dropped.
- **MF (More Fragments) bit**: If set to 1, it indicates that more fragments are coming. The last fragment has this bit set to 0.

3. Fragment Offset: Indicates the position of a fragment within the original packet. This field helps the destination system reassemble the fragments in the correct order. It measured in units of 8 bytes (64 bits), meaning that all fragments accept the last one must be a multiple of 8 bytes in length.

4. Total Length: The length of the fragment including the IP header [25-28].

Fragmentation adds some overhead as the router needs to add header information to each fragment. In some cases, fragmentation can lead to inefficiencies or even packet loss if a fragment gets dropped during transmission. The modern networks often employ techniques like Path MTU Discovery to avoid fragmentation whenever possible. IP fragmentation is a necessary process for transmitting large packets over networks with varying MTUs [29]. While it introduces some performance and security concerns, it ensures data can traverse different network segments reliably.

6. CIDR: CLASSLESS INTER-DOMAIN ROUTING

CIDR allows network routers to route data packets to the respective device based on the indicated subnet. Instead of classifying the IP address based on classes, routers retrieve the network and host address as specified by the CIDR suffix.IT is a method of assigning IP addresses that improves the efficiency of address distribution and replaces the previous system based on Class A, Class B and Class C networks [29-30]. The group of IP addresses is called Block in Classless Inter - Domain. CIDR follows CIDR notation or Slash notation.

Properties of CIDR Block: The properties of CIDR block are as follows:

- The IP addresses in a block are continuous.
- The first address of a block should be exactly divisible by the number of addresses of a block.
- The size of the Block should be power of 2.

Use of CIDR: The different uses as following:

- Variable-length subnet masking is the foundation of CIDR (VLSM). It can now specify prefixes of any duration, making it much more powerful than the previous method.
- Two collections of numbers make up CIDR IP addresses. The network address is written as a prefix, similar to how an IP address is written (e.g. 192.255.255.255).
- The suffix, which means how many bits are in the whole address (e.g. /12), is the second component. A CIDR IP address will look anything like this when put together: 192.255.255.255/12.
- As part of the IP address, the network prefix is also defined. These changes are based on how many bits are needed. As an illustration, in the above example, the first 12 bits of the address are for the network, while the last 20 bits are for host addresses [29-31].

CIDR Notation: Using CIDR we can assign an IP address to host without using standard id address classes like Class A, B, and C.

In CIDR we simply tell how many bits are used for network id. The network id bits are provided after the '/' symbol. Like /10 means 10 bits are used for the network id part and remaining 32-10=22 bits are used for the host id part.

Advantages of CIDR: The CIDR notation is that it reduces the number of entries in the routing table and also it manages the IP address space.

1) **Efficient IP Address Allocation**: CIDR allows for more efficient allocation of IP addresses by eliminating the rigid class boundaries (Class A, B and C). The networks can be sized more precisely, reducing wastage of IP addresses.
2) **Aggregation of Routes (Route Summarization)**: CIDR allows multiple IP addresses to be represented with a single network prefix. This reduces the number of routes in routing tables, improving router performance and reducing memory usage.

Disadvantages of CIDR: The disadvantages of using CIDR Notation are as follows −

- Using CIDR it is complex to determine the route. By using classful addresses, we are directly having separate tables for class A, Class B, Class C
- Used directly go to these tables by seeing the prefix of IP address. But by using CIDR, we don't have these tables separately. All entries are placed in a single table. So, it is difficult to find a route [31-35].

CIDR replaces the older class-based system, which had fixed blocks of IP addresses, with a more flexible approach that allows for variable-length subnet masking (VLSM). This flexibility enables more precise allocation of IP addresses, helping to reduce wastage and better accommodate the growing number of devices on the internet. CIDR notation, which uses a format like "192.168.0.0/24", specifies the IP address range and the number of significant bits in the subnet mask, enhancing routing efficiency and scalability in modern network infrastructures.

7. TCP & UDP

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two fundamental transport layer protocols in the Internet protocol suite. They serve different purposes and have distinct characteristics

7.1. TCP (Transmission Control Protocol): TCP is a connection-oriented protocol that ensures reliable data transmission between devices. It is designed to provide error detection, error correction, and flow control. TCP is suitable for applications where data integrity and order are crucial, such as web browsing, email, and file transfer.

Key Features of TCP: The several key features as below following:

1. **Connection-Oriented**: A connection must be established between the sender and receiver before data transmission.
2. **Reliable Delivery**: Ensures data is delivered accurately and in sequence.
3. **Error Checking and Correction**: Uses checksums to detect errors and retransmits lost or corrupted data.
4. **Flow Control**: Manages the rate of data transmission to prevent network congestion.
5. **Congestion Control**: Adjusts the data transmission rate based on network traffic conditions.
6. **Ordered Data Transfer**: Data packets are delivered to the application in the same order they were sent.
7. **Three-Way Handshake**: Uses a three-step process to establish a connection (SYN, SYN-ACK, ACK).

Segment Structure of TCP: The segment structure discussed as below:

- **Source Port**: The port number of the sender.
- **Destination Port**: The port number of the receiver.
- **Sequence Number**: The position of the first byte of data in the segment.
- **Acknowledgment Number**: The next expected byte from the receiver.
- **Data Offset**: The size of the TCP header.
- **Reserved**: Reserved for future use.
- **Flags**: Control flags (e.g., SYN, ACK, FIN).
- **Window**: Size of the receiver's buffer space.
- **Checksum**: Error-checking mechanism.

- **Urgent Pointer**: Indicates urgent data.
- **Options**: Additional options for extended functionality.
- **Data**: The actual payload.

Use Cases and Suitability: TCP is best suited for applications where reliability and data integrity are critical, such as:

- Web Browsing (HTTP/HTTPS)
- Email (SMTP, POP3, IMAP)
- File Transfers (FTP) [36-40]

7.1. UDP (User Datagram Protocol): UDP is a connectionless protocol that provides a simple, fast, and efficient way to send data without the overhead of establishing a connection. It is suitable for applications where speed is more critical than reliability, such as video streaming, online gaming, and voice over IP (VoIP).

Key Features of UDP: They key features of UDP discussed as below section:

1. **Connectionless**: Data is sent without establishing a connection between the sender and receiver.
2. **Unreliable Delivery**: Does not guarantee delivery, order, or error correction.
3. **No Error Checking or Correction**: Only a basic checksum is used for error detection; there is no retransmission of lost data.
4. **No Flow Control**: Does not manage the rate of data transmission, which can lead to packet loss in congested networks.
5. **No Congestion Control**: Does not adjust transmission rates based on network traffic.
6. **Fast and Efficient**: Minimal overhead makes it suitable for time-sensitive applications.

UDP Datagram Structure:

- **Source Port**: The port number of the sender.
- **Destination Port**: The port number of the receiver.
- **Length**: The length of the UDP header and data.
- **Checksum**: Error-checking mechanism.
- **Data**: The actual payload.

Use Cases and Suitability: UDP is ideal for applications where speed is more important than reliability, such as:

- Video Streaming (e.g., Netflix, YouTube)
- Online Gaming (e.g., multiplayer games)
- Voice over IP (VoIP, e.g., Skype, Zoom)
- DNS queries [38-41]

Tables 2: The list of features for TCP and UDP [40-44]

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection Type	Connection-oriented	Connectionless
Reliability	Reliable (ensures data delivery)	Unreliable (no guarantee of delivery)
Error Checking	Yes (error checking and recovery)	Yes (error checking, but no recovery)
Flow Control	Yes	No
Congestion Control	Yes	No
Overhead	Higher (due to reliability features)	Lower (minimal overhead)
Data Packet Size	Variable (depends on protocol specifics)	Fixed
Header Size	20-60 bytes	8 bytes
Data Transfer Speed	Slower (due to reliability features)	Faster
Use Cases	Web browsing, email, file transfer	Streaming, online gaming, VoIP
Sequencing	Yes	No
Acknowledgments	Yes	No
Three-way Handshake	Yes	No
Example Protocols	HTTP, FTP, SMTP	DNS, DHCP, TFTP

TCP (Transmission Control Protocol) is a connection-oriented protocol that ensures reliable data transmission between devices over a network. It establishes a connection through a three-way handshake and provides mechanisms for error checking, flow control, and congestion control. This makes TCP ideal for applications where data integrity and order are crucial, such as web browsing, email, and file transfers. Its reliability features, however, result in higher overhead and slower data transfer speeds compared to UDP [45]. UDP on the other hand, is a connectionless protocol that provides a faster, but less reliable means of communication. It does not establish a connection before sending data, nor does it guarantee the delivery, order, or error recovery of the transmitted packets. This minimalistic approach results in lower overhead and faster transmission, making UDP suitable for real-time applications like streaming, online gaming, and VoIP, where speed is more critical than reliability.

8. CONCLUSION & FUTURE PROSPECTIVES

The evolution and utilization of IP addresses have been pivotal in shaping the modern internet landscape. From the early days of IPv4 to the gradual adoption of IPv6, the IP addressing scheme has undergone significant changes to meet the growing demands of internet connectivity. IP addresses serve as unique identifiers for devices, enabling efficient routing and communication across diverse networks. This review highlights the evolution of IP addressing, from IPv4 to the more expansive IPv6, addressing the challenges of address exhaustion and the increasing demand for connectivity. By demystifying the complexities of IP addresses, this primer provides a foundational understanding crucial for navigating the digital landscape, ensuring informed and effective participation in the ever-expanding world of digital connectivity.

Ethical contribution: Not applicable.

REFERENCES

1. Hon KW. Networking and IP addresses. InTechnology and Security for Lawyers and Other Professionals 2024 Jun 18 (pp. 266-287). Edward Elgar Publishing.
2. Zhang C. Ethical Review of Compulsory Display of User IP Addresses on Multiple Network Platforms. Journal of Social Science Humanities and Literature. 2024 Feb 29;7(1):113-7.
3. Li Z, Zhou F, Wang Z, Xu X, Liu L, Yin G. Measuring and classifying IP usage scenarios: a continuous neural trees approach. Scientific Reports. 2024 Mar 1;14(1):5144.
4. Sáez-Ortuño L, Forgas-Coll S, Huertas-Garcia R, Puertas-Prats E. Chasing spammers: Using the Internet protocol address for detection. Psychology & Marketing. 2024 Jun;41(6):1363-82.
5. Aslam JM, Kumar KM. Enhancing security of cloud using static IP techniques. The Scientific Temper. 2024 Mar 15;15(01):1790-8.
6. Tiwari MK, Pal R, Chauhan V, Singh V, Singh V, Dhamodaran S, Sharma S. A python programming widely utilized in the development of a twitter bot as a sophisticated advance technical tool.
7. Hon KW. Networking and IP addresses. InTechnology and Security for Lawyers and Other Professionals 2024 Jun 18 (pp. 266-287). Edward Elgar Publishing.
8. Isizoh AN, Okechukwu OP, Ani AA. ANALYSES OF THE MIGRATION TO INTERNET PROTOCOL VERSION SIX (IPv6). International Journal of Computing, Science and New Technologies (IJCSNT). 2024 Mar 24;2(1):11-23.
9. Sheikh AF. Networking Fundamentals. InCompTIA Linux+ Certification Companion: Hands-on Preparation to Master Linux Administration 2024 Jun 7 (pp. 215-243). Berkeley, CA: Apress.
10. Hsu A, Li F, Pearce P, Gasser O. A First Look At NAT64 Deployment In-The-Wild. InInternational Conference on Passive and Active Network Measurement 2024 Mar 11 (pp. 112-129). Cham: Springer Nature Switzerland.
11. Lencse G, Bazsó Á. Benchmarking methodology for IPv4aaS technologies: Comparison of the scalability of the Jool implementation of 464XLAT and MAP-T. Computer Communications. 2024 Apr 1;219:243-58.
12. Pal R, Pandey P, Rizwan M, Koli M, Thakur SK, Malakar RK, Gupta H, Khadam VK, Chawra HS. The Utilization of Response Surface Methodology (RSM) In the Optimization of Diclofenac Sodium (DS) Liposomes Formulate through the Thin Film Hydration (TFH) Technique with Involving Computational Method. Journal of Advances in Medicine and Medical Research. 2023 Oct 28;35(22):287-300.

13. Muhammad AJ. Evaluation of Explainable AI Techniques for Interpreting Machine Learning Models.

14. Mixon-Baca B, Knockel J, Xue D, Ayyagari T, Kapur D, Ensafi R, Crandall JR. Attacking connection tracking frameworks as used by virtual private networks. Proceedings on Privacy Enhancing Technologies YYYY (X). 2024;1:18.

15. Durdağı E, Buldu A. IPV4/IPV6 security and threat comparisons. Procedia-Social and Behavioral Sciences. 2010 Jan 1;2(2):5285-91.

16. Ordabayeva GK, Othman M, Kirgizbayeva B, Iztaev ZD, Bayegizova A. A systematic review of transition from IPV4 To IPV6. InProceedings of the 6th International Conference on Engineering & MIS 2020 2020 Sep 14 (pp. 1-15).

17. Zakari A, Musa M, Bekaroo G, Bala SA, Hashem IA, Hakak S. IPv4 and IPv6 protocols: A Comparative performance study. In2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC) 2019 Aug 2 (pp. 1-4). IEEE.

18. Paul HC, Bakon KA. A study on IPv4 and IPv6: The importance of their co-existence. International Journal of Information System and Engineering. 2016 Nov;4(2).

19. Levin SL, Schmidt S. IPv4 to IPv6: Challenges, solutions, and lessons. Telecommunications Policy. 2014 Dec 1;38(11):1059-68.

20. Raicu I, Zeadally S. Evaluating IPv4 to IPv6 transition mechanisms. In10th International Conference on Telecommunications, 2003. ICT 2003. 2003 Feb 23 (Vol. 2, pp. 1091-1098). IEEE.

21. Ashraf S, Muhammad D, Aslam Z. Analyzing challenging aspects of IPv6 over IPv4. J. Ilm. Tek. Elektro Komput. Dan Inform. 2020 Jul;6(1):54-67.

22. Pal R, Pandey P, Maurya VK, Saxena A, Rizwan M, Koli M, Shakya S, Pinki K. Optimization and formulation of doxorubicin (DOX) loaded liposome well-used in chemotherapy involving quality by design (QbD): a transitory research. European Chemical Bulletin. 2023;12:4491-510.

23. Hyun J, Li J, Kim H, Yoo JH, Hong JW. IPv4 and IPv6 performance comparison in IPv6 LTE network. In2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS) 2015 Aug 19 (pp. 145-150). IEEE.

24. Isaac S, Abdu J. Comparative Analysis between IPv4 and IPv6. International Journal of Information Systems and Engineering (IJISE). 2015:20-4.

25. Shiranzaei A, Khan RZ. A comparative study on IPv4 and Ipv6. Int. J. Adv. Inf. Sci. Technol.(IJAIST). 2015;33:6-19.

26. Mikac M, Horvatić M, Mikac V. Networking case study in STEM education-IP fragmentation. InINTED2020 Proceedings 2020 (pp. 1068-1077). IATED.

27. Mikac M, Horvatić M, Mikac V. Networking case study in STEM education-IP fragmentation. InINTED2020 Proceedings 2020 (pp. 1068-1077). IATED.

28. Hamadeh I, Kesidis G. Performance of ip address fragmentation strategies for ddos traceback. InProceedings of the 3rd IEEE Workshop on IP Operations & Management (IPOM 2003)(IEEE Cat. No. 03EX764) 2003 Oct 3 (pp. 1-7). IEEE.

29. Pal R, Pandey P, Rai B, Koli M, Chakrabarti M, Thakur P, Rizwan M, Saxena A. Chitosan: as highly potential biopolymer obtainable in several advance drug delivery systems including biomedical applications. Environmental science. 2023;3(4).

30. Kimsanov UO. ONE OF THE OPTIMAL METHODS FOR DETERMINING ROUTES AND ADDRESSING NETWORK EQUIPMENT. Bulletin of Bokhtar State University named after Nosir Khusrav. Humanities and Economics Series. 2021(1-1):134-7.Malgosa J, Flores A, Munoz JP, Manzanares P. Solving IP exhaustion with maskless inter-domain routing (MIDR) scheme. In2017 Sixth International Conference on Future Generation Communication Technologies (FGCT) 2017 Aug 21 (pp. 1-5). IEEE.

31. Fuller V, Li T. RFC 4632: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.

32. Rahul M. A comparative evaluation of classless routing protocols (EIGRP) and classful routing protocols (RIP). Asian Journal of Technology & Management Research [ISSN: 2249–0892]. 2014 Jan;4(01).

33. Hon KW. Networking and IP addresses. InTechnology and Security for Lawyers and Other Professionals 2024 Jun 18 (pp. 266-287). Edward Elgar Publishing.

34. Yang Q, Ma L, Tu S, Ullah S, Waqas M, Alasmary H. Towards blockchain-based secure BGP routing, challenges and future research directions. Computers, Materials and Continua. 2024 May 15;79(2):2035-62.

35. Pal R, Pandey P, Koli M, Srivastava K, Tiwari V, Gaur AK, Dutta P. The Comprehensive Review: Exploring Future Potential of Nasopulmonary Drug Delivery Systems for Nasal Route Drug Administration. Journal of Drug Delivery and Therapeutics. 2024 Mar 15;14(3):126-36.

36. Simpson A, Alshaali M, Tu W, Asghar MR. Quick UDP Internet Connections and Transmission Control Protocol in unsafe networks: A comparative analysis. IET Smart Cities. 2024 May 17.

37. Pustovoitov P, Voronets V, Voronets O, Sokol H, Okhrymenko M. ASSESSMENT OF QOS INDICATORS OF A NETWORK WITH UDP AND TCP TRAFFIC UNDER A NODE PEAK LOAD MODE. Eastern-European Journal of Enterprise Technologies. 2024 Jan 15.

38. Nie L, Wang M, Yan H, Li Z, Tian Y. Command filtered backstepping control of multiple transmission control protocol/active queue management networks with user datagram protocol flows. Asian Journal of Control. 2024.

39. Pal R, Pandey P, Rai B, Koli M, Chakrabarti M, Thakur P, Rizwan M, Saxena A. Chitosan: as highly potential biopolymer obtainable in several advance drug delivery systems including biomedical applications. Environmental science. 2023;3(4).

40. Kiran P, Shilpa S. Secure Communication Protocols for the IoT. InSecure Communication in Internet of Things 2024 (pp. 142-152). CRC Press.

41. Poranen T, Systä K. ANALYSING THE PERFORMANCE AND BEHAVIOUR OF SNMP O Liu H. Network and Communication Protocols in Cyber-Physical Systems. InA Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations 2024 (pp. 25-88).

42. de Oliveira GH, de Melo Valeira G, Akamine C. A Proposal to Use ROUTE/DASH in the Advanced ISDB-T. IEEE Transactions on Broadcasting. 2024 Jun 3.

43. Pal R, Pandey P, Jha D, Dutta P, Sahoo S, Gupta R, Rizwan M, Keskar MS, Kumar V, Chawra HS. The Utilization of 32Full Factorial Design (FFD) for Optimization of Lincomycin Hydrochloride (LNH) Loaded Nanogel Involving; Design of Experiments (DoE) an Advanced Approach. Advances in Research. 2023 Dec 21;24(6):272-81.

44. Liu R, Zenke C, Liu C, Holmes A, Thornton P, Malan DJ. Teaching CS50 with AI: leveraging generative artificial intelligence in computer science education. InProceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1 2024 Mar 7 (pp. 750-756).