TECHNICAL REPORT WRITING

Networking Fundamentals: Differences Between IPv4 and IPv6, TCP and UDP, and Address Mapping

NAME: RUPAK SARKAR

ROLL NO.: 14271024036

STREAM: MASTER OF COMPUTER APPLICATION

SUBJECT NAME: NETWORKING

SUBJECT CODE: MCAN-204

COLLEGE NAME: MEGHNAD SAHA INSTITUTE OF TECHNOLOGY

UNIVERSITY NAME: MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY

ABSTRACT

The evolution of networking technologies has led to the development of multiple protocols that ensure efficient communication over the internet. This report provides a comparative analysis of IPv4 and IPv6, highlighting their structural differences, addressing mechanisms, and transition strategies. Additionally, it examines the fundamental differences between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), focusing on their reliability, speed, and use cases in modern networking. Furthermore, the concept of address mapping is explored, detailing how IP addresses are mapped to physical addresses through protocols like ARP (Address Resolution Protocol) and NAT (Network Address Translation). By understanding these key networking principles, this report aims to provide insights into the strengths, limitations, and practical applications of these technologies in today's digital world.

CONTENTS

INTRODUCTION

Introduction

The internet relies on a variety of protocols to facilitate seamless communication between devices across networks. Among these, IPv4 (Internet Protocol Version 4) and IPv6 (Internet Protocol Version 6) play a crucial role in addressing and routing data packets. While IPv4 has been the dominant protocol for decades, the growing demand for IP addresses has led to the adoption of IPv6, which offers a significantly larger address space and improved efficiency.

In addition to addressing, data transmission over networks depends on transport layer protocols, primarily TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP provides reliable, connection-oriented communication, whereas UDP offers faster, connectionless data transmission, making them suitable for different types of applications.

Another essential aspect of networking is address mapping, which ensures that devices can communicate effectively by resolving IP addresses to physical addresses. Techniques such as ARP (Address Resolution Protocol) and NAT (Network Address Translation) play a key role in this process by enabling devices to locate each other within networks.

This report aims to explore the key differences between IPv4 and IPv6, analyze the functionalities of TCP and UDP, and examine various address mapping techniques. By understanding these fundamental networking concepts, we can better appreciate their impact on internet communication and modern network infrastructure.

TECHNICAL REPORT

IPv4 –

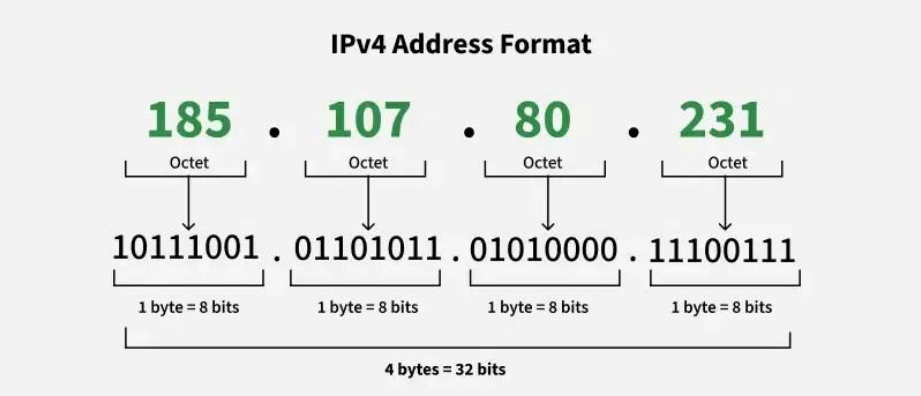
Introduction

IP stands for Internet Protocol version v4 stands for Version Four (IPv4), is the most widely used system for identifying devices on a network. It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address. This address helps data find its way from one device to another over the internet.

IPv4 was the primary version brought into action for production within the ARPANET in 1983. IP version four addresses are 32-bit integers which will be expressed in decimal notation. Example- 192.0.2.126 could be an IPv4 address.

IPv4 Address Format

An IPv4 address consists of 32 bits (binary digit), grouped into four sections of known as octets or bytes. Each octet has 8 bits and these bits can be represented only in 0 or 1 form, and when they grouped together, they form a binary number. Since each octet has 8 bits, it can represent 256 numbers ranging from o to 255. These four octets are represented as decimal numbers, separated by periods known as dotted decimal notation. For example, IPv4 address 185.107.80.231 consists of four octets.



Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.

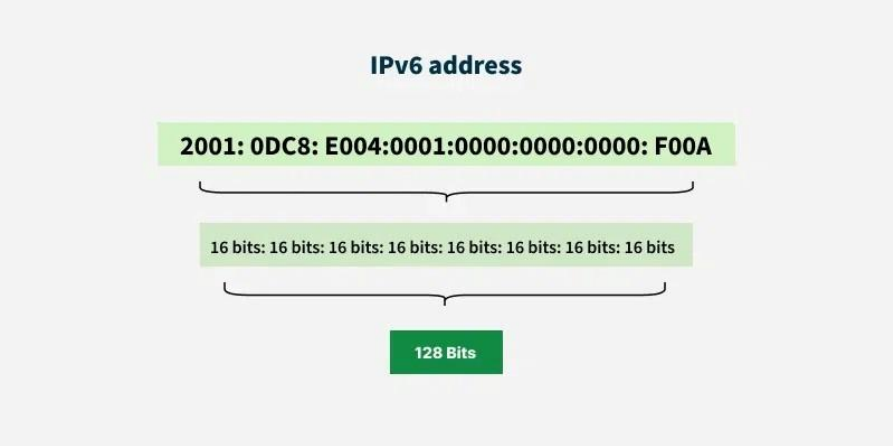
Limitations of IPv4

- IP relies on network layer addresses to identify end-points on the network, and each network has a unique IP address.
- The world's supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
- If there are multiple hosts, we need the IP addresses of the next class.

IPv6 –

Introduction

The next generation Internet Protocol (IP) address standard, known as IPv6, is meant to work in cooperation with IPv4. To communicate with other devices, a computer, smartphone, home automation component, Internet of Things sensor, or any other Internet-connected device needs a numerical IP address. Because so many connected devices are being used, the original IP address scheme, known as IPv4, is running out of addresses. This new IP address version is being deployed to fulfil the need for more Internet addresses. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 support a theoretical maximum of 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456.



Advantages

- **Faster Speeds:** IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- **Stronger Security:** IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.

Disadvantages

- **Conversion:** Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- **Communication:** IPv4 and IPv6 machines cannot communicate directly with each other.

Difference between IPv4 and IPv6 –

Features	IPv4	IPv6
Address Length	32-bit address (e.g., 192.168.1.1)	128-bit address (e.g., 2001:db8::1)
Address Format	Decimal, separated by dots.	Hexadecimal, separated by colons.
Address Space	Supports around **4.3 billion** addresses	Supports **340 undecillion** (vastly larger)
Header Size	20 bytes	40 bytes
Broadcasting	Supports broadcasting	No broadcasting; uses multicast and anycast instead
Fragmentation	Done by sender and routers	Done only by the sender
Checksum	Includes a checksum field	No checksum
Routing Efficiency	Relatively complex due to fragmented networks	More efficient due to simplified header and hierarchical addressing
NAT	Commonly used due to address shortage	Not required due to vast address space
Configuration	Can be manual (static), DHCP-based, or automatic	Supports auto-configuration and DHCPv6
Security	Security depends on external protocols like IPSec	Built-in IPSec support for enhanced security
Support for Mobility	Limited support for mobile devices	Better mobility and multi-homing support

TCP –

Transmission Control Protocol (TCP) is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. It is one of the main protocols of the TCP/IP suite. In OSI model, it operates at the transport layer (Layer 4). It lies between the Application and Network Layers which are used in providing reliable delivery services. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

UDP –

User Datagram Protocol (UDP) is one of the core protocols of the Internet Protocol (IP) suite. It is a communication protocol used across the internet for time-sensitive transmissions such as video playback or DNS lookups. Unlike Transmission Control Protocol (TCP), UDP is connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.

Difference between TCP and UDP –

Features	TCP	UDP
Type of Protocol	Connection-oriented	Connectionless
Reliability	Reliable	Unreliable
Error Checking	Performs error checking and correction	Performs error checking but no correction
Data Transmission	Data is sent in **sequence** and received in order	Data may arrive **out of order**
Speed	Slower due to error correction and acknowledgments	Faster due to minimal overhead
Header Size	Larger (20-60 bytes)	Smaller (8 bytes)
Flow Control	Uses **flow control**	No flow control
Congestion Control	Implements **congestion control**	No congestion control

Address Mapping –

Address mapping in computer networks is the process of associating a logical address with a physical address. This is done using protocols like Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and Dynamic Network Address Translation (DNAT).

1. Address Resolution Protocol (ARP) –

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address. In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.

2. Reverse Address Resolution Protocol (RARP) –

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address. When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

3. Dynamic Host Configuration Protocol (DHCP) –

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other network configurations (such as subnet masks, default gateways, and DNS servers) to devices on a network. Instead of manually configuring each device, a DHCP server dynamically allocates IP addresses from a defined pool, ensuring efficient IP address management and preventing conflicts. When a device (client) connects to the network, it sends a DHCP Discover request, to which the server responds with an available IP address via a DHCP Offer. The client then requests the offered address (DHCP Request), and the server confirms the assignment (DHCP Acknowledgment). This process simplifies network administration, particularly in large networks, and supports both IPv4 and IPv6 environments.

4. Domain Name System (DNS) –

Domain Name System (DNS) is a hierarchical and distributed system that translates human-readable domain names (e.g., www.example.com) into numerical IP addresses (e.g., 192.168.1.1) required for locating and identifying devices on a network. When a user enters a URL in a web browser, a DNS query is sent to a DNS server, which resolves the domain name to its corresponding IP address, allowing the browser to connect to the requested website. DNS operates using a network of servers, including recursive resolvers, root servers, top-level domain (TLD) servers, and authoritative name servers. This system ensures efficient, fast, and scalable access to websites and online services, playing a crucial role in the functioning of the internet.

CONCLUSION

This report explored fundamental networking concepts, focusing on the differences between IPv4 and IPv6, TCP and UDP, and address mapping techniques. The comparison of IPv4 and IPv6 highlighted the limitations of IPv4, such as limited address space and reliance on NAT, while emphasizing IPv6's larger address space, improved security, and routing efficiency. The analysis of TCP and UDP demonstrated the trade-offs between reliability and speed, showcasing how TCP ensures accurate data transmission, whereas UDP is optimized for fast, real-time communication.

Additionally, the discussion on address mapping provided insights into how devices communicate efficiently over networks using ARP (Address Resolution Protocol) and NAT (Network Address Translation). Understanding these concepts is essential for network engineers, developers, and IT professionals, as they form the backbone of modern communication systems.

As the internet continues to evolve, the transition from IPv4 to IPv6, the choice between TCP and UDP based on application requirements, and efficient address mapping will play a crucial role in ensuring seamless connectivity and performance in networking infrastructure.

ACKNOWLEDGEMENT

I would like to acknowledge all those without whom this report would not have been successful. Firstly, I would wish to thank my teacher Mrs. Sankhamita Sinha who guided me throughout the report and gave her immense support. She made us understand how to successfully complete this report and without her, the report would not have been complete.

I would also like to thank my parents who have always been there whenever needed. Once again, thanks to everyone for making this report successful.