THE HIERARCHICAL ADDRESSING SYSTEM IN COMPUTER NETWORKS: ROLES OF IP ADDRESSES, MAC ADDRESSES, PORT NUMBERS, AND SOCKETS

Sudhir Agarmore
Assistant Professor, School of Allied Sciences, DMIHER, Sawangi Meghe, Wardha 442001, Maharashtra, India
sudhiragarmor@gmail.com
Hemant S. Mahalle
Principal, V.R.College, Savana. Dist. Yavatmal (M.S), India.
mahalle_hemant@yahoo.com
Dr. Shweta Shirpurkar
Head & Assistant Professor, Shri Mathuradas Mohota College of Science, Nagpur, Dist. Nagpur (MS), India
shwetashirpurkar20@gmail. com

Abstract

The research paper focuses on the enabling mechanisms of addressing that are used to provide reliable communication in computer networks. We examine the hierarchical association between four important elements namely MAC addresses, IP addresses, port numbers, and sockets, which are the data link layer, network layer, transport layer, and application programming interface respectively. This paper is able to show how all these elements interoperate together to support end-to-end communication on a network of networks, and each element of the network communication stack has a specific, but complementary role. The study identifies the synergy in the operational of these addressing mechanisms and the significance of their combination in the present networking infrastructure, its issue of concern, and the future perspectives of network addressing technologies.

1. Introduction

1.1 Background

The explosion of the number of networked machines and the expansion of internet services has added pressure on the necessity to provide strong, scalable addressing solutions. The existing internet architecture is based on a multi-layered addressing scheme that allows specific procedures of data packets delivery between the source and the destination using heterogeneous network infrastructures. The number of connected IoT devices is estimated to have reached 29.4 billion as of 2030 alone, as per Statista Research Department [1], which underscores the dire need to have an efficient addressing system.

1.2 Problem Statement

The different network addressing mechanisms and their unique roles and interactions are important to understand in order to design, troubleshoot, and implement security measures on a network. According to Zheng et al. [2], problems in understanding how these elements interact to facilitate smooth communication result in errors during the configuration of the networking and security weaknesses among many networking professionals and students.

1.3 Research Objectives

To specify the portion in the OSI and TCP/IP models of the duties of MAC addresses, IP addresses, port numbers, and sockets.

To examine the hierarchical interdependence and functioning relationship of these addressing mechanisms.

To illustrate their joint working in end-to-end communication using real life case studies.

To study the existing issues and future research trends in network addressing technologies.

2. Literature Review

2.1 Historical Development

The addressing scheme currently used was developed on the basis of the early networking protocols such as the ARPANET and the OSI model along with the development of TCP/IP protocols made important contributions to the scheme. Leiner et al. [3] reported the influence of the separation of concerns principle in the development of separate addressing mechanisms of the various layers of the network stack. The move towards hierarchical addressing made of hostname-based systems started with the writings of Postel [4] on the specifications of Internet Protocol.

2.2 Theoretical Framework

Layered network addressing is theoretically explained by the OSI (Open Systems Interconnection) model along with TCP/IP protocol stack. The OSI model of seven layers was proposed by Zimmermann [5], and the TCP/IP protocol proposed by Cerf and Kahn [6] is the foundation upon which the internetworking of the modern world is built. Every layer has its addressing scheme and depends on the services of the lower layers, establishing a powerful abstraction hierarchy.

3. Addressing Components Technical Analysis. Media Access Control Address (MAC).

3.1.1 Definition and Structure

MAC address is a hardware network identifier that is a 48-bit identifier that manufacturers assign to network interface controllers (NICs). The address format is based on IEEE 802 standard, which is established by IEEE Standards Association [7]. The address space has the following structure:

First 24 bits- Organizationally Unique Identifier (OUI) as given by IEEE.

Unknown 24 bits: Network interface controller specific.

Format: XX:XX:XX:XX:XX:XX (hexadecimal)

Example: 00:1B:44:11:3A:B7

3.1.2 Functional Role

- Layers 2 (Data Link Layer) of the OSI model.
- Offers physical devices identification at local network segments.
- Facilitates the delivery of frames within a similar broadcast area.

Switches and bridges use it to make forwarding decision based on Content Addressable Memory (CAM) tables.

3.1.3 Key Characteristics

According to Kurose and Ross, MAC addresses are non-routable (local), hardware-based and are usually permanent (MAC address). They are also necessary in Ethernet and WiFi communications and utilized in ARP (Address Resolution Protocol) to the mapping of IP-to-MAC as required in Plummer [9].

3.2 IP Address (Internet Protocol Address)

3.2.1 Definition and Structure

Internet protocol IP address is a logical numerical address that is used in devices in a computer network. In RFC 8200, Deering and Hinden [10] give the existing requirements of both IPv4 and IPv6 standards.

IPv4 (32-bit):

XXX.XXX.XXX.XXX (dotted decimal)

Example: 192.168.1.100

The possible addresses are approximately 4.3 billion.

IPv6 (128-bit):

Format XXXX: XXXX: XXXX: XXXX:

Example:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Address space virtually unlimited (3.4 $*10^{38}$ addresses)

3.2.2 Functional Role

Layer 3 (Network Layer) of the OSI model.

Logical network identification and location.

Supports inter-network routing.

Connectionless and connection-oriented support.

3.2.3 Address Classification

According to Comer [11], IP addresses are divided into a few types:

Public vs. Private: NAT (Network Address Translation) allows accessing to the public networks by private addresses.

Static vs. Dynamic: DHCP automates the addresses assignment.

Unicast, Multicast, Broadcast: The various patterns of communication.

3.3 Port Number

3.3.1 Definition and Structure

A port number is a 16-bit unsigned integer (0-65535) that is used to identify certain processes or network services. RFC 768 described the port number system in UDP, and RFC 793 described TCP in TCP, as described by Postel [12,13].

Port Categories:

Famous ports (0–1023) are reserved for system services such as HTTP (port 80), HTTPS (port 443), and SSH (port 22). Registered ports (1024–49151) are assigned to user applications, while dynamic or private ports (49152–65535) are used for temporary client connections.

3.3.2 Functional Role

Layers 4 (Transport Layer) of the OSI model.

Provides multiplexing/demultiplexing ability of multiple applications on one host.

Tasks differentiation of various network services on the same IP address.

TIMEOUT(s) TCP/UDP protocols.

3.4 Socket

3.4.1 Definition and Structure

A socket is a software endpoint and creates a two-way communication between processes, usually over a network. Stevens [14] constitutes it as the product of:

Socket = IP Address + Port Number + Protocol.

3.4.2 Functional Role

API Programming interface to the network applications.

Abstracts underlying the complexity of networks.

The connection state and data flow are managed.

Supports connection-oriented (TCP) and connectionless (UDP) communication.

3.4.3 Socket Types

According to Wright and Stevens [15], sockets are divided into three broad categories:

TCP provides reliable, connection-oriented stream sockets for dependable data transmission. Datagram sockets, based on UDP, offer an unreliable and connectionless mode of communication. Raw sockets, on the other hand, allow direct access to the underlying IP layer for custom network protocol implementations.

4. Hierarchical Relationship and Operational Synergy

4.1 Communication Flow Example

Consider a web browsing scenario where a client requests a webpage from a server:

4.1.1 Outbound Request

1. **Application Layer**: Browser creates HTTP request
2. **Transport Layer**: TCP socket created with source port (ephemeral) and destination port 80
3. **Network Layer**: IP header added with source and destination IP addresses
4. **Data Link Layer**: Ethernet frame created with source and destination MAC addresses

4.1.2 Address Resolution Process

Tanenbaum & Wetherall [16] describe the complete encapsulation process:

Application: HTTP Request → Transport: TCP + Ports → Network: IP Addresses → Data Link: MAC Addresses

4.2 The Complete Addressing Stack

Application Data	← Socket (IP + Port)
Transport Header (Port Numbers)	← Port Number
IP Header (IP Addresses)	← IP Address
Frame Header (MAC Addresses)	← MAC Address
Physical Transmission	

4.3 Practical Communication Example

Scenario: Client (192.168.1.100) connecting to Web Server (93.184.216.34)

Client Side:

Socket: 192.168.1.100:54321 → 93.184.216.34:80
MAC: 00:1B:44:11:3A:B7 → Router MAC

Server Side:

Socket: 93.184.216.34:80 → 192.168.1.100:54321
MAC: Server MAC → Next Hop MAC

5. Comparative Analysis

5.1 Addressing Scope and Lifetime

Component	Layer	Scope	Lifetime	Example
MAC Address	Data Link	Local Network	Permanent	00:1B:44:11:3A:B7
IP Address	Network	Global	Configurable	192.168.1.100
Port Number	Transport	Process	Session	80 (HTTP)
Socket	Multiple	Connection	Temporary	192.168.1.100:54321

5.2 Functional Comparison

Aspect	MAC Address	IP Address	Port Number	Socket
Uniqueness	Global	Network	Host	Connection
Routable	No	Yes	N/A	N/A
Configuration	Hardware	Software	Software	Dynamic
Protocol Dependency	Ethernet	IP	TCP/UDP	TCP/UDP

6. Implementation Considerations

6.1 Security Implications

- Network addressing presents several security concerns:
- MAC address spoofing allows an attacker to masquerade as a legitimate device.
- IP address spoofing, such as in DDoS attacks, enables an attacker to forge source addresses.
- Port scanning helps an attacker discover vulnerable services.
- Socket hijacking enables the attacker to take over an existing session.

6.2 Performance Optimization

Keshav [18] talks about network addressing optimal methods:

Efficient socket management reduces resource usage, while proper port allocation helps avoid conflicts. Effective IP address planning optimizes routing, and MAC address tables in switches enable fast packet forwarding.

6.3 Scalability Challenges

Donahoo and Calvert [19] point to scalability problems of network addressing:

The exhaustion of IPv4 addresses has made the adoption of IPv6 essential. However, challenges such as port number limitations in high-connection environments, restricted MAC address table sizes in network devices, and socket descriptor limits in operating systems still persist. A case study on web server communication highlights these issues in practical scenarios.

7. Case Study: Web Server Communication

7.1 Setup

Network Architecture:

The case study examines a typical client-server web interaction across multiple network segments. The network topology consists of three main components arranged in a hierarchical structure:

Internet Cloud
↓
Web Server Network (203.0.113.0/24)
↓
Border Router
↓
Home Network (192.168.1.0/24)

Device Specifications:

Web Server:

- IP Address: 203.0.113.45 (Public)
- MAC Address: 00:1C:B3:09:85:15
- Services: HTTP (Port 80), HTTPS (Port 443)
- Operating System: Ubuntu Server 22.04 LTS

Client Workstation:

- IP Address: 192.168.1.150 (Private)
- MAC Address: 00:1B:44:11:3A:B7
- Browser: Chrome v115.0
- Operating System: Windows 11

Home Router:

- WAN IP: 198.51.100.25 (Public)
- LAN IP: 192.168.1.1 (Private)
- MAC Address: 00:1D:7E:2A:55:33
- NAT Enabled: Yes

7.2 Communication Process

Fall & Stevens [20] describe the entire process of communication:

1. DNS Resolution: The client looks up domain to IP 203.0.113.45.

2. Creation of Socket: Client makes socket 192.168.1.150:62000 203.0.113.45:80.

3.ARP Request: Customer learns the MAC address of router.

4.Packet Encapsulation:

HTTP data + TCP header (ports) and IP header (addresses) and Ethernet header (MACs).

5.Routing: Router is used to send packet based on IP addresses.

6.Final Delivery: Web server takes requests in accordance with port 80.

8. Future Trends and Developments.

8.1 Emerging Technologies

Zhang et al. [21] find that there are a few trending network addressing trends:

The complete transition from IPv4 to IPv6 represents a full replacement aimed at addressing the limitations of IPv4. With Software-Defined Networking, network addresses can be managed dynamically, enhancing flexibility. IPv6 also provides effective solutions for the massive addressing needs of billions of IoT devices. Furthermore, emerging technologies like Quantum Networking introduce entirely new paradigms of network addressing for future communication systems.

8.2 Research Directions

Future research priorities are summarized by Clark as follows:

- ➢ Automatic address configurations and management.
- ➢ Optimized security in address resolving procedures.
- ➢ Techniques of cross-layer optimization.
- ➢ Discussing mobile and ad-hoc networks schemes.

9. Conclusion

The hierarchical addressing system comprising MAC addresses, IP addresses, port numbers, and sockets forms the backbone of modern computer networking. Each component plays a distinct yet interdependent role in enabling reliable, efficient communication across global networks. Peterson & Davie [23] emphasize that understanding these relationships is fundamental to network architecture and design.

MAC addresses provide physical device identification at the local network level, IP addresses enable global routing and logical addressing, port numbers facilitate application multiplexing, and sockets serve as the programming interface for network applications. The continued evolution of these addressing mechanisms, particularly the transition to IPv6 and development of new socket programming models, will be crucial for supporting future network growth and innovation.

References

1. Statista Research Department, Internet of Things (IoT) connected devices worldwide 2030, Statista, 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
2. K. Zheng, M. Liu, and Y. Zhang, "Network Addressing Education: Challenges and Solutions," Journal of Network and Computer Applications, vol. 185, p. 103067, 2021. https://doi.org/10.1016/j.jnca.2021.103067
3. B.M. Leiner, V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D.C. Lynch, J. Postel, L.G. Roberts, and S. Wolff, "A Brief History of the Internet," ACM SIGCOMM Computer Communication Review, vol. 39, no. 5, pp. 22-31, 2009. https://doi.org/10.1145/1629607.1629613
4. J. Postel, Internet Protocol, RFC 791, IETF, 1981. https://doi.org/10.17487/RFC0791
5. H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, vol. 28, no. 4, pp. 425-432,

1980. https://doi.org/10.1109/TCOM.1980.1094702

6. V.G. Cerf and R.E. Kahn, "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, vol. 22, no. 5, pp. 637-648, 1974. https://doi.org/10.1109/TCOM.1974.1092259
7. IEEE Standards Association, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, IEEE Std 802-2014, 2014. https://doi.org/10.1109/IEEESTD.2014.6847097
8. J.F. Kurose and K.W. Ross, Computer Networking: A Top-Down Approach, 7th ed., Pearson, 2017.
9. D.C. Plummer, An Ethernet Address Resolution Protocol, RFC 826, IETF, 1982. https://doi.org/10.17487/RFC0826
10. [S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 8200, IETF, 2017. https://doi.org/10.17487/RFC8200
11. D.E. Comer, Internetworking with TCP/IP: Principles, Protocols, and Architecture, 6th ed., Prentice Hall, 2014.
12. J. Postel, User Datagram Protocol, RFC 768, IETF, 1980. https://doi.org/10.17487/RFC0768
13. J. Postel, Transmission Control Protocol, RFC 793, IETF, 1981. https://doi.org/10.17487/RFC0793
14. W.R. Stevens, UNIX Network Programming: Networking APIs: Sockets and XTI, vol. 1, Prentice Hall, 1998.
15. G.R. Wright and W.R. Stevens, TCP/IP Illustrated: The Protocols, vol. 2, Addison-Wesley, 1995.
16. A.S. Tanenbaum and D.J. Wetherall, Computer Networks, 5th ed., Prentice Hall, 2011.
17. W. Stallings, Data and Computer Communications, 10th ed., Pearson, 2017.
18. S. Keshav, Mathematical Foundations of Computer Networking, Addison-Wesley, 2012.
19. M.J. Donahoo and K.L. Calvert, TCP/IP Sockets in C: Practical Guide for Programmers, 2nd ed., Morgan Kaufmann, 2009.
20. K.R. Fall and W.R. Stevens, TCP/IP Illustrated: The Protocols, vol. 1, 2nd ed., Addison-Wesley, 2012.
21. Y. Zhang, L. Wang, and H. Liu, "Future Internet Architectures: Addressing and Routing Challenges," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 500-533, 2022. https://doi.org/10.1109/COMST.2022.3147890
22. [22] D.D. Clark, S. Shenker, and A.L. Chapin, "New Directions in Network Architecture: The Role of Addressing Systems," ACM Computing Surveys, vol. 55, no. 3, pp. 1-35, 2023. https://doi.org/10.1145/3547132
23. L.L. Peterson and B.S. Davie, Computer Networks: A Systems Approach, 6th ed., Morgan Kaufmann, 2021.
24. B.A. Forouzan, TCP/IP Protocol Suite, 4th ed., McGraw-Hill, 2012.
25. J.D. Day, Patterns in Network Architecture: A Return to Fundamentals, Prentice Hall, 2008.
26. C. Metz, IP Addressing and Subnetting Incuding IPv6, Sybex, 2020.
27. B.A. Miller and C. Bisdikian, Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications, 2nd ed., Prentice Hall, 2009.
28. C.M. Kozierok, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, No Starch Press, 2005.
29. J. Liu, X. Wang, and M. Chen, "Software-Defined Networking: Addressing Management Challenges," Computer Networks, vol. 191, p. 108015, 2021. https://doi.org/10.1016/j.comnet.2021.108015
30. A. Meddeb and N. Samaan, "IPv6 Deployment and Security Challenges: A Comprehensive Survey," IEEE Access, vol. 10, pp. 34567-34589, 2022. https://doi.org/10.1109/ACCESS.2022.3162456