# Draft

*by* Ahmad Bilal

**Submission date:** 12-Jun-2022 11:06PM (UTC+0500)
**Submission ID:** 1855380353
**File name:** VARIOUS_PROTOCOLS_IN_NETWORKING_COMPARISON_OF_IPV4_AND_IPV6.docx (891.34K)
**Word count:** 3437
**Character count:** 18835

# VARIOUS PROTOCOLS IN NETWORKING & COMPARISON OF IPV4 AND IPV6

First A. Author, *Fellow, IEEE*, Second B. Author, and Third C. Author, Jr., *Member, IEEE*

***Abstract*— Network communication protocol is a system of regulations, conventions, and schema that control how gadgets transfer information through networks. To put it another way, internet standards may be equated to protocols that two or more gadgets must comprehend in order to transfer data efficiently, regardless of architecture or design variations. The Internet Protocol (IP) is a communications standard that is used to transport and identify information for connecting gadgets such as workstations, notebooks, and optical switching devices over an unique connection or a network of interlinked systems. The present editions of the Internet Protocol are IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). Is there a distinction among IPv4 and IPv6? Whichever is speedier: functioning or enjoying video sports? This article will lead you to the solution.**

***Index Terms*—**

## I. The OSI Model: How Network Protocols Work

To One should initially understand the Open Systems Interconnection (OSI) concept to completely appreciate the nuances of communication guidelines. The OSI paradigm is by far the largest frequently used conceptual framework for online operating connections, with this same OSI concept serving as the foundation for the bulk of transmission techniques today.

The OSI architecture separates two connected nodes' information exchange across seven stages. Any of those seven levels is assigned a job or a set of duties. Every one of the levels are self-sufficient, and they on their own can execute the tasks which are being assigned to them. Figure 1 depicts the exchange of information among several networking endpoints to bring things within context.

These tiers of the OSI structure are divided into two subgroups: top layered (layers 7, 6, and 5) and bottom layered (layers 4, 3, 2, and 1). The upper tiers deal with application issues, while the bottom tiers deal with information transmission.

Internet standards break down the information exchange into separate operations at each level of the OSI architecture. One or several networking standards are employed at every level of the information flow.

The OSI structure's framework is still utilized to organize procedure discussions and analyze and evaluate numerous methodologies, despite certain claims that it is now outdated and eclipsed by the Transmission Control Protocol (TCP)/IP networking architecture [1].

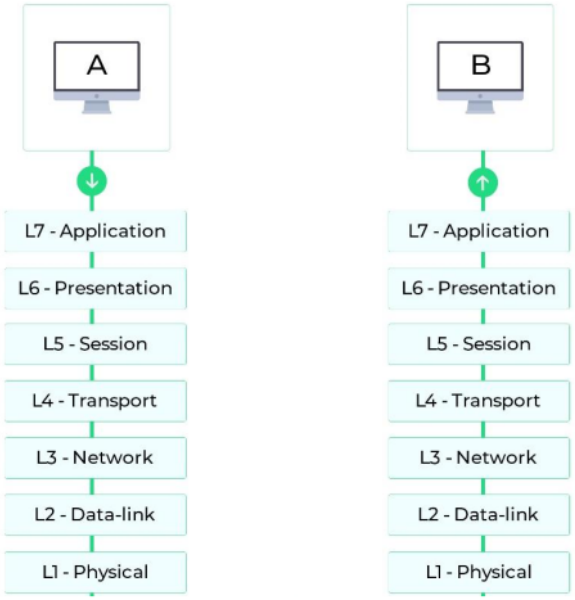


**Fig 1:** OSI network model

TABLE I
NETWORK LAYERS

| Layer | Description |
|---|---|
| **Layer 7: Application layer network protocols** | Standard capabilities consist of simulated stations, file relocations, and job events. |
| **Layer 6: Presentation layer network protocols** | The differences in filetypes among various platforms are obscured.<br>Information is classified and translated, zipped and unzipped, encrypted and decrypted, and so on. |
| **Layer 5: Session layer network protocols** | Interactions and engagements with clients are managed.<br>It establishes and terminates user interactions. |
| **Layer 4: Transport layer network protocols** | In networking, it manages the edge-to-edge transfer of data.<br>Message transmission is reliable and linear due to errors fixing and flow management techniques. |
| **Layer 3: Network layer protocols** | The unique networking gadget identities are used to transmit data.<br>This method conducts congestion and flow management to prevent internet asset degradation. |
| **Layer 2: Data link layer network protocols** | The messages are being framed.<br>Packet delivery faults are identified and repaired. |
| **Layer 1: Physical layer network protocols** | The internet medium and the gadgets using it have interfaces.<br>Describes an entity's optical, electronic, and physical qualities. |

## II. Classification of Network Protocols

Now that you know how the OSI architecture functions, you can get straight into protocols categorization. Several of the top extensively utilized standards in computer networks are mentioned as following.

### *A. Protocols of network in Application layer*

1) **DHCP**
DHCP (Dynamic Host Configuration Protocol) is an internet connectivity technique that enables system managers to regulate the issuance of IP addresses. A distinct IP identity is required per each gadget connected to the internet through an IP connection. DHCP enables system managers to disseminate IP's from a centralised point and immediately supply a fresh IP identifier whenever a machine is connected in from a separate point on the channel. It is considered client-server standard.

2) **DNS**
The DNS (Domain Name System) framework is used to translate host to IP address. DNS is a client-server architecture that uses a decentralized registry dispersed over a network of naming providers.
IP address is used to distinguish nodes, though even memorising one might be difficult due to its sophistication. Due to the versatile nature of IP addresses, linking url identities to IP's is very much vital. By converting webpage identifiers into mathematical IP addresses, DNS assists in the settlement of this issue.

3) **FTP**
FTP (File Transfer Protocol) is a framework that enables information to be shared between nearby and remote locations. TCP is used as a foundation. For information transmission, FTP initiates two TCP sessions (control session and data session). The data session transports the real data, but the control session communicates control parameters like login credentials, document retrieval and saving commands, etc. Each of such interconnections are operational at the similar moment throughout the data migration process.

4) **HTTP**
HTTP (Hyper Text Transfer Protocol) is a multimedia data framework application level method that is connected and cooperative. The internet browser serves as the user in this client-server paradigm. HTTP is a framework for transferring information via the Internet, like documents, images, as well as various interactive objects. A demand and reply technique is that wherein the user requests server a query, that the server analyzes prior to sending the user a reply.
Because HTTP is a connectionless procedure, the user and service provider till the time their link is established are known to one another. So the user and the service provider as soon as the connection is broken lose track of one another. As a consequence of such phenomenon, neither the service provider nor the user is able to keep track of data across queries.

5) **IMAP and IMAP4**
IMAP (Internet Message Access Protocol) is a message standard which enables clients to see and modify emails on an email service provider via an email application, exactly as if it is in a remote computer. IMAP is a client-server technology which enables many users to simultaneously see mails on the very similar email service provider. IMAP enables users to add, erase, and modify folders, and also monitor for incoming comments, completely erase emails, add and erase indicators, and perform a variety of other tasks. The current version 4 of IMAP with revision 1 is in play nowadays.

6) **POP and POP3**
The POP (Post Office Protocol) is a message standard as well as an emailing standard. This standard allows the customer to retrieve messages via the email service provider to its local mail program. When the messages are being stored offline, these can be accessed without an online access. Furthermore, the email system erases the messages once they have been transmitted to local storage, clearing valuable storage. On contrary to IMAP4, POP3 is never designed to do extensive modifications on the mails server's contents. The latest current edition is the POP3.

7) **SMTP**
SMTP (Simple Mail Transfer Protocol) is a protocol for sending and receiving email that is both reliable and efficient. POP and IMAP have been utilized to receive messages on the actual customer's end, while SMTP is a drive technique for delivering messages. SMTP is a mechanism for sending and receiving messages among pc's, as well as notifying clients whenever fresh messages turn up. A user may transmit a message over SMTP to some user on the local channel or any domain through a relaying or bridge link which is available on all domains.

8) **Telnet**
Telnet (Terminal emulation protocol) is an application level standard which enables a client to be connected to and interact with a remote computer. A Telnet listener is deployed on the customer's computer, that links to the cli of some other remote machine executing a Telnet service programme.
Telnet is commonly used by system managers to connect to and administer remote machines. After entering the faraway computer's IP address or domain id, a system manager will be given a virtualized interface through whom anyone may connect with the client.

9) **SNMP**
SNMP (Simple Network Management Protocol) is an application level standard for controlling IP - based components like switches, routers, workstations and servers. SNMP can be used by system managers to monitor networks efficiency, detect networks faults, and remediate problems. The SNMP standard is made up of three parts: a monitored gadget, an SNMP client, and an SNMP administrator.

The SNMP client is deployed on the monitored machine. The client is an application program which has localized understanding of administrative data and translates it to an SNMP-compatible version. The SNMP controller shows information via the SNMP client, enabling system managers to control devices effectively.

SNMP is currently offered in 3 different variants: v1, v2, and v3. SNMP v2 introduces additional standard features as well as other improvements, whereas editions 1 and 2 overlap most features. SNMP variant 3 (SNMP v3) adds privacy and online management capabilities to previous editions.

*B. Protocols of network in Presentation layer*

1) **LPP**

The LPP (Lightweight Presentation Protocol) assist and provide effective facility for OSI application functions in channels employing TCP/IP interfaces in specific constrained contexts. LPP is designed for a specific sort of OSI system, namely ones that only include an Association Control Service Element (ACSE) as well as a Remote Operations Service Element (ROSE). Organizations having a relatively extensive program architecture, like those with a Consistent Transmission System Component, really aren't suited for LPP.

*C. Protocols of network in Session layer*

1) **RPC**

RPC (Remote Procedure Call) is a communication system for seeking a function via programs on a remote devices without having to understand the fundamental networking infrastructure. RPC transports information among interacting programmes using TCP or UDP. RPC can also be used in a server-client environment. The customer is the computer which initiates the demand, whereas the service provider is the computer which fulfils it.

*D. Protocols of network in Transport layer*

1) **TCP**

TCP (Transmission Control Protocol) is a transport level procedure which employs ordered response to provide a reliable streamed transfer and virtualized link function to clients. TCP is a connection paradigm, this implies that information may only be transmitted when 2 programmes have established a link. With flow control and information acknowledgement, TCP enables extensive integrity checks. TCP ensures information ordering at the receiver side, guaranteeing that packets of data get in the right order. TCP enables for the re-transmission of packets of data that have been destroyed.

2) **UDP**

UDP (User Datagram Protocol) is a connectionless transport tier standard which offers a simple but unsure communication platform. UDP, apart from TCP, lacks characteristics such as reliability, flow control, and data integrity. UDP is useful whenever TCP's dependability features aren't necessary. The re-transmission of deleted information packets is indeed not possible with UDP.

*E. Protocols of network in Network layer*

1) **IP**

IPv4 (Internet Protocol) is a network level standard for transporting messages among a channel which includes addresses and management data. To transfer information bits through the internet, IP and TCP work jointly. Every client is assigned a 32-bit IP address, which is divided into 2 portions: the network identity and the host identity. The networks address specifies a network and is issued by the cloud, while the host address indicates a client on the channel and is given by a system operator. IP is only in charge of distributing messages, but TCP is in charge of sequencing them.

2) **IPv6**

IPv6 is by far the latest edition of the IP addressing Standard, a network level method for packets transportation which includes addresses and control data. IPv6 was created to replace IPv4 when it became obsolete. It increases the IP addresses capacity from 32 to 128 bits to allow greater degrees of referencing.

3) **ICMP**

ICMP (Internet Control Message Protocol) is a network level standard for exchanging warning signals and operations information between networking nodes. ICMP signals in IP datagrams are used to send out information concerning network functioning or failure. ICMP is a protocol that is intended to warn clients of networks issues, bottlenecks, and latencies, and to assist in debugging.

*F. Protocols of network in Data link layer*

1) **ARP**

On a localized networking, the Address Resolution Protocol (ARP) helps translate IP identifiers to actual device identifiers (or MAC identifiers for Ethernet). An ARP caching is used to preserve the relationship among an IP number and its MAC identity. ARP establishes the protocols for establishing such relationships and aids addressing translation across both ways.

2) **SLIP**

SLIP (Serial Line IP) is used for TCP/IP p2p serial connectivity. SLIP is a serial standard which is commonly employed on specialized serial wires and dial-up networks. The SLIP protocol makes it possible for clients and gateways to communicate alongside each other; common SLIP networking architectures comprises of edge-edge, edge-gateway, and gateway-gateway. SLIP is primarily a message structuring procedure: On a serial connection, it provides a character pattern which encapsulates IP messages. It doesn't have addresses, traffic class recognition, fault identification and correction, or compressing capabilities.

## III. IPV4 AND IPV6

*A. What Is IPv4?*

IPv4 is the 4th edition of the Internet Protocol, and it establishes the terms for digital networking based on the information interchange idea. It can precisely recognize machines attached to the networks using an addressing

scheme. Whenever a gadget (whether a switch, a PC, etc) links to the network, it is assigned a distinct numeric IP number, such as 192.168.100.250. IPv4 uses a 32-bit addressing scheme which enables for 2^32 values to be stored (4.19 billion addresses). IPv4 identifiers are becoming limited as the amount of individuals connecting to the Internet rises. To fulfil the rising need for IPv4 address, IPv6, the latest Internet address scheme, is getting introduced [2].

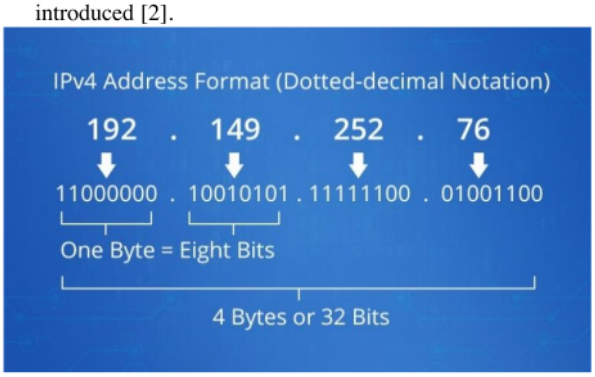


**Fig 2:** IPV4 address format

*B. What Is IPv6?*

Worries about the need for IP numbers will surpass the availability led to the implementation of IPv6 (Internet Protocol Version 6) in 1999. It allows the transmission of information and interaction via a networking. IPv6 is a 128-bit Internet identifier which can perhaps hold a maximum of 2 128 entries. IPv6 tackles not only the problem of finite network addressing allocations, as well as the challenges faced by diverse Internet accessibility gadgets. An instance of an IPv6 domain is as follows: 3fee:2901:fe21:4547:0100:0270:0892:0009 [3].

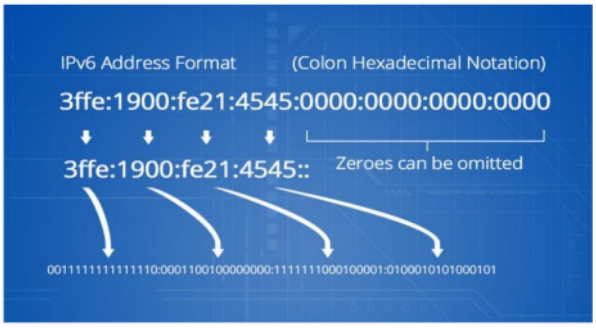


**Fig 3:** IPV6 address format

*C. Features of IPv4*

IPv4 has the following characteristics:

1) A Connectionless Protocol
2) Enables you to create a simple virtualized networking level that can be utilised by a wide range of gadgets.
3) It requires lesser storage and enables recalling identifiers simpler.
4) The standard is currently supported by millions of devices.
5) Media archives and also meetings are provided.

*D. Features of IPv6*

Features of IPv6 are as follows:

1) Layered naming and transportation architecture.
2) Both stateless and stateful implementations remain possible.
3) Quality-of-service assistance (QoS).
4) An ideal strategy for communicating with your peers.

*E. Main Differences Between IPv6 and IPv4*

The 2 categories of domains employed to distinguish machines on a network are IPv4 and IPv6. Both work in the identical manner in theory, though differ in practise. Which are the differences among them? The main differences among IPv4 and IPv6 are listed here [4].

TABLE II
IPV4 AND IPV6 DIFFERENCES

| Differences | IPv4 | IPv6 |
|---|---|---|
| Method of Addressing | Numeric address is separated by a dot (.) from its binary bits | A colon separates the binary bits of an alphanumeric address (:). Hexadecimal is also included. |
| Types of Addresses | Multicast, Broadcast and Unicast. | Multicast, Anycast and Unicast. |
| Masks in Address | Use for the selected network from the host part. | Not used. |
| Total Fields in Header | 12 | 8 |
| Fields length in Header | 20 | 40 |
| Checksum | Fields of checksum are available. | Fields of checksum are not available. |
| Total Classes | Five Classes (A to E). | There is no limit to the amount of IP addresses you can have. |
| Configuration | It is necessary to allocate IP addresses and routes. | Depends entirely on the functions needed, configuration is discretionary. |
| VLSM | Support | Not Support |
| Fragmentation | This is accomplished using sending and forwarding routes. | The sender has to complete the task. |
| Routing Information Protocol | The routed daemon is there to help. | IPv6 is not supported by RIP. Static routes are used. |
| Configuration of Networks | Manual configuration or by using DHCP. | Auto-configuration. |
| SNMP | The SNMP protocol is used to manage systems. | IPv6 is not supported by SNMP. |
| Mobility & Interoperability | Mobility and interoperability are limited by network topologies that are relatively restrictive. | IPv6 enables network devices to communicate with one another and to move around. |
| Records of DNS | IN-ADDR.ARPA DNS field, Pointer (PTR) data | Pointer (PTR) data, IP6.ARPA DNS field |
| Resolution among IP and | ARP Broadcast | Multicast Neighbor Solicitation |

| MAC | | |
|---|---|---|
| Mapping | ARP is used for mapping IP to MAC. | NDP is used for mapping IP to MAC. |
| Quality of Service (QoS) | In QoS packet bandwidth and priority allows you to demand for TCP/IP products. | IPVv6 is presently not supported by QoS implemented by IBM. |

## IV. Advantages of using IPV6

*A. Performance: Expanse of IP Address*

The basic distinction among IPv4 and IPv6 is the size of IP numbers. IPv4 names are 32 bits in length, whereas IPv6 domains comprise of 128 bits. IPv6 features a bigger addressing range and a more straightforward preamble than IPv4. IPv6 extends the IP range from 32 to 128 bits to accommodate growing addressing demands. As per estimations of 4x1018 IPv6 numbers per sq meter on the Earth 's surface, IP numbers would hardly ran short anytime soon. A CIDR-like design is used to encapsulate IPv6 names, making networking simpler.

*B. IP Header Format: Reduce Header Bandwidth*

In IPv6 domains, many similar domains would have either being dropped or specified as enhanced prefixes in the IPv4 header structure. IPv6 headers are just 2 twice the size of IPv4 prefixes, considering the reality that IPv6 identifiers are 400% the capacity of IPv4 domains. It reduces traffic handling cost and headers capacity, enabling it to operate faster.

*C. Support for Options: Improvement of Routing Performance*

The preamble contains the IPv4 choices, while the IPv6 parameters are contained in a different, extended preamble. The header would only be executed unless a network is chosen, resulting in significantly faster navigation. Parameter size restrictions in IPv6 have been relaxed (up to 40 bytes for IPv4 possibilities), and new choices would be added as required. Most of IPV6's additional features are enabled through compatibility for IP level security (IPSEC), jumbogram, wireless IP, as well as other options.

*D. Network Security: More Secure and Confidential*

IPv4 transaction functionality includes Internet Protocol Security (IPSec), which is usually voluntary or obligatory. Although IPSec is essential for IPv6, it isn't really necessary for IPv4. Furthermore, IPv6 now provides identification authentication and information uniformity, significantly improving the platform's safety and privacy.

*E. Network Security: Faster Speed: Lack of NAT*

IPv6 is considered to be faster than IPv4 in terms of performance due to the removal of network address translation (NAT). This is why providers are incapable to provide each customer with a distinct IPv4 number (because there simply are not enough left to go around). The performance of IPv6 vs. IPv4 was measured by Akamai, an online and cloud solutions firm. "In comparison to IPv4, websites run 5% speedier in the mean and 15% speedier for the 95% on IPv6," they observed. As a result, IPv6 is a preferable solution for specified people that need to get stuff accomplished swiftly [5].

## V. Conclusion

As illustrated by the the above content, IPv6 is crucial for the Internet's future survival. If the Internet changes between IPv4 to IPv6, it would possess a far larger supply of IP numbers. Every gadget may get its unique public IP identity rather than remaining hidden under a NAT gateway. IPv4 and IPv6 overlap presently, although both originally not meant to be interoperable. Because of the cost and interoperability issues with IPv6, Identifiers could be used for a lengthy moment, but IPv6 identifiers will eventually be the norm.

## REFERENCES

[1] "Network protocols," Manage Engine Op Manager, [Online]. Available: https://www.manageengine.com/network-monitoring/network-protocols.html.

[2] P. Wu, Y. Cui, J. Wu, J. Liu and C. Metz, "Transition from IPv4 to IPv6: A State-of-the-Art Survey," *IEEE Communications Surveys & Tutorials,* vol. 15, no. 3, pp. 1407-1424, 2013.

[3] E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia-Social and Behavioral Sciences,* vol. 2, pp. 5285-5291, 2010.

[4] Margaret, "IPv4 vs IPv6: Which is Faster?," FS Community, 3 Nov 2021. [Online]. Available: https://community.fs.com/blog/ipv4-vs-ipv6-whats-the-difference.html.

[5] Ali and A. N. Abu, "Comparison study between IPV4 & IPV6," *International Journal of Computer Science Issues (IJCSI),* vol. 9, no. 3, p. 314, 2012.

# Draft

ORIGINALITY REPORT

| 10% | 9% | 3% | 5% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.manageengine.com<br>Internet Source | 5% |
| 2 | Submitted to Daegu Gyeongbuk Institute of Science and Technology<br>Student Paper | 2% |
| 3 | www.slideshare.net<br>Internet Source | 1% |
| 4 | www.coursehero.com<br>Internet Source | 1% |
| 5 | Submitted to National Tertiary Education Consortium<br>Student Paper | <1% |
| 6 | Submitted to University of Central England in Birmingham<br>Student Paper | <1% |
| 7 | docshare.tips<br>Internet Source | <1% |
| 8 | www.itap.purdue.edu<br>Internet Source | <1% |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On | | |

# Draft

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

**Instructor**

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6