# IPV4

internet protocol version-4

tutorialspoint

SIMPLYEASYLEARNING

## About the Tutorial

Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

This tutorial will help you in understanding IPv4 and its associated terminologies along with appropriate references and examples.

## Audience

This tutorial has been designed to help beginners understand basic concepts of IPv4 required to work with any TCP/IP based protocols. After completing this tutorial, you will find yourself at a moderate level of expertise of IPv4 from where you can take yourself to next levels.

## Prerequisites

Before you start proceeding with this tutorial, I'm making an assumption that you are already aware of basic computer and network concepts such as what is a protocol, why do we need protocol, Network Layers, etc.

## Copyright & Disclaimer

# Table of Contents

# 1. IPv4 – Overview

This era is said to be the era of computers. Computers have significantly changed the way we live. A computing device when connected to other computing device(s) enables us to share data and information at lightning fast speed.

## What is Network?

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network:

- **Hosts -** Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user's PC, an internet Server, a database server etc.
- **Media -** If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.
- **Hub -** A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.
- **Switch -** A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.
- **Router -** A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.
- **Gateways -** A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.
- **Firewall -** Software or combination of software and hardware, used to protect users' data from unintended recipients on the network/internet.

All components in a network ultimately serve the hosts.

## Host Addressing

Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called **Internet Protocol Address**.

# 2. IPv4 – The OSI Model

The International Standard Organization has a well-defined model for Communication Systems known as Open System Interconnection, or the OSI Model. This layered model is a conceptualized view of how one system should communicate with the other, using various protocols defined in each layer. Further, each layer is designated to a well-defined part of communication system. For example, the Physical layer defines all the components of physical nature, i.e. wires, frequencies, pulse codes, voltage transmission etc. of a communication system.

The OSI Model has the following seven layers:

| |
|---|
| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Datalink |
| Physical |

- **Application Layer (Layer-7):** This is where the user application sits that needs to transfer data between or among hosts. For example: HTTP, file transfer application (FTP) and electronic mail etc.

- **Presentation Layer (Layer-6):** This layer helps to understand data representation in one form on a host to other host in their native representation. Data from the sender is converted to on-the-wire data (general standard format) and at the receiver's end it is converted to the native representation of the receiver.

- **Session Layer (Layer-5):** This layer provides session management capabilities between hosts. For example, if some host needs a password verification for access and if credentials are provided then for that session password verification does not happen again. This layer can assist in synchronization, dialog control and critical operation management (e.g., an online bank transaction).

- **Transport Layer (Layer-4):** This layer provides end-to-end data delivery among hosts. This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission.
- **Network Layer (Layer-3):** This layer helps to uniquely identify hosts beyond the subnets and defines the path which the packets will follow or be routed to reach the destination.
- **Data Link Layer (Layer-2):** This layer takes the raw transmission data (signal, pulses, etc.) from the Physical Layer and makes Data Frames, and sends that to the upper layer and vice versa. This layer also checks any transmission errors and sorts it out accordingly.
- **Physical Layer (Layer-1):** This layer deals with hardware technology and actual communication mechanism such as signaling, voltage, cable type and length, etc.

## Network Layer

The network layer is responsible for carrying data from one host to another. It provides means to allocate logical addresses to hosts, and identify them uniquely using the same. Network layer takes data units from Transport Layer and cuts them into smaller unit called Data Packet.

Network layer defines the data path, the packets should follow to reach the destination. Routers work on this layer and provides mechanism to route data to its destination.

# 3. IPv4 – The TCP/IP Model

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers.

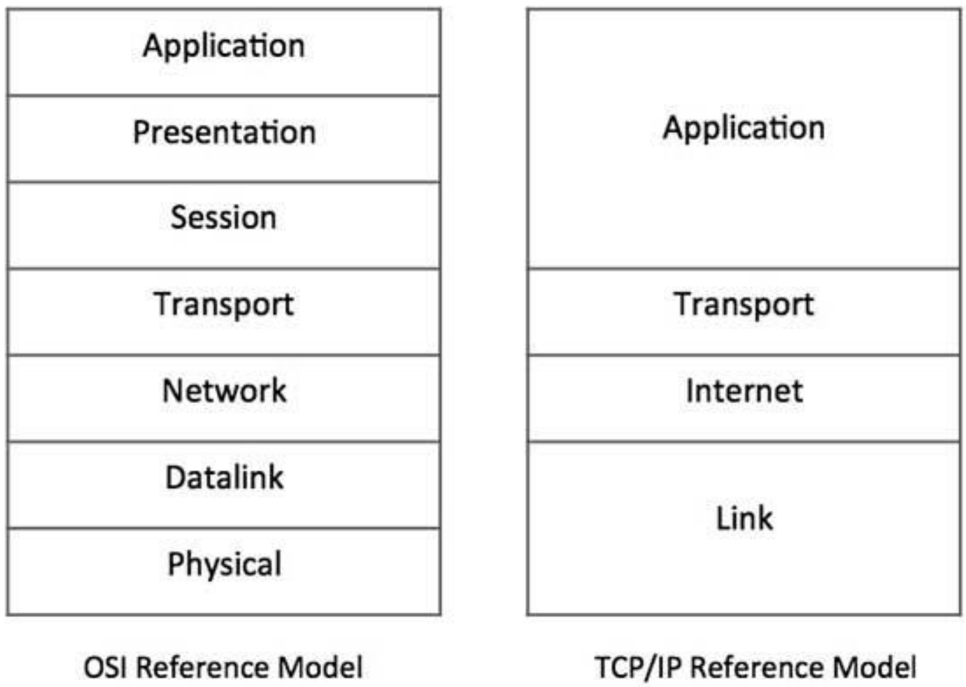



**Figure**: Comparative depiction of OSI and TCP/IP Reference Models

This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies. Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

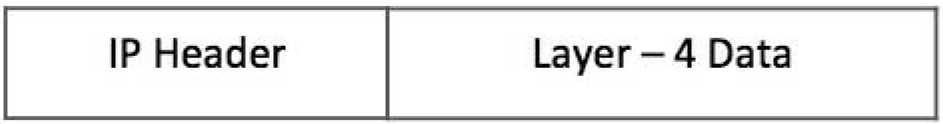
## Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

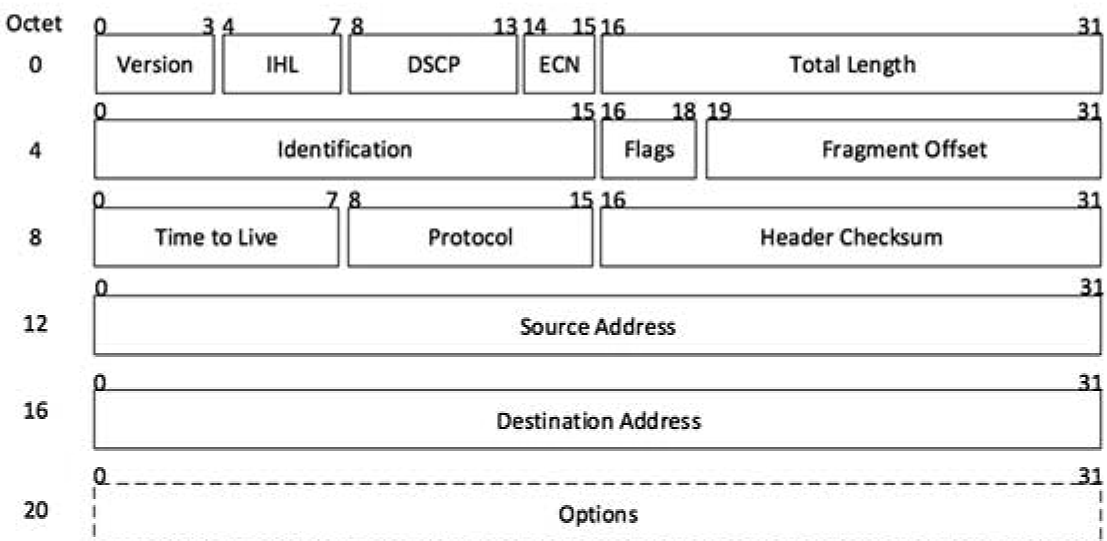
# 4. IPv4 – Packet Structure

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.




(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.




[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.

- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tell if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.