**18CSC302J-COMPUTER NETWORKS**

**Unit - I**

IP HEADER

IP FRAGMENTATION

ARP RARP

ICMP –INTRODUCTION

DEBUGGING TOOLS

ICMP PACKAGE

UDP DATAGRAM

UDP CHARACTERISTICS

TCP CONNECTION ESTABLISHMENT PROCESS

TCP ERROR CONTROL

TCP CONGESTION CONTROL

TCP FLOW CONTROL

*MULTICASTING*

*MULTICASTING AND MULTICAST ROUTING PROTOCOL*

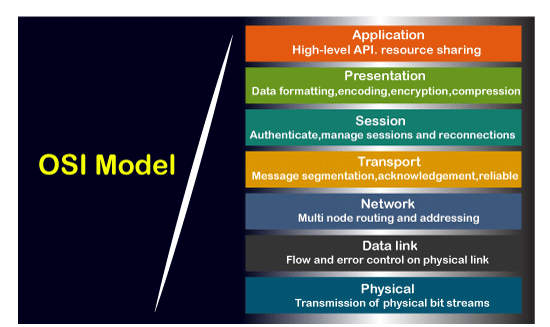
*STREAM CONTROL TRANSMISSION PROTOCOL*

*SIMPLE TCP/IP CLIENT SERVER COMMUNICATION*

**OSI vs TCP/IP**

**What is OSI model?**

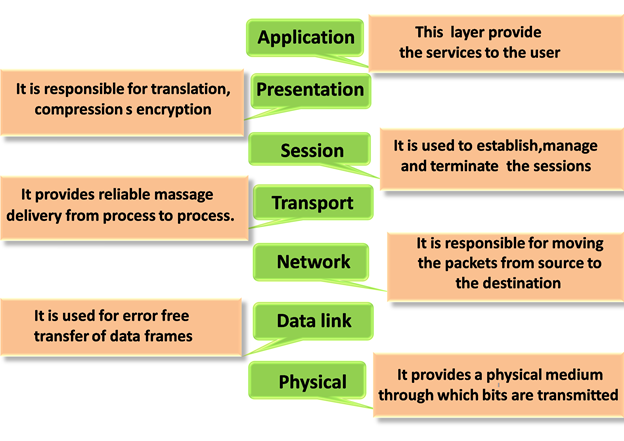
The OSI stands for Open System Interconnection, which was developed in 1980s. It is a conceptual model used for network communication. It is not implemented entirely, but it is still referenced today. This OSI model consists of seven layers, and each layer is connected to each other. The data moves down the OSI model, and each layer adds additional information. The data moves down until it reaches the last layer of the [OSI model](https://www.javatpoint.com/osi-model). When the data is received at the last layer of the OSI model, then the data is transmitted over the network. Once the data is reached on the other side, then the process will get reversed.



Functions of the OSI Layers

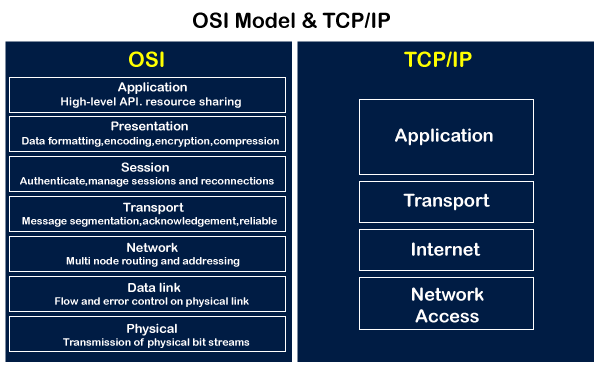
There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



What is TCP/IP model?

The TCP model stands for **Transmission Control Protocol,** whereas IP stands for **Internet Protocol**. A number of protocols that make the internet possibly comes under the TCP/IP model. Nowadays, we do not hear the name of the TCP/IP model much, we generally hear the name of the IPv4 or IPv6, but it is still valid. This model consists of 4 layers. Now, we will look at the diagrammatic representation of the [TCP/IP model](https://www.javatpoint.com/computer-network-tcp-ip-model).



As shown in the above diagram, the TCP/IP model has 4 layers, while the OSI model consists of 7 layers. Diagrammatically, it looks that the 4 layers of the TCP/IP model exactly fit the 7 layers of the OSI model, but this is not reality. The application layer of the [TCP/IP](https://www.javatpoint.com/tcp-ip-full-form) model maps to the first three layers, i.e., application, session, and presentation layer of the OSI model. The transport layer of the TCP maps directly to the transport layer of the OSI model. The internet layer of the TCP/IP model maps directly to the network layer of the OSI model. The last two layers of the OSI model map to the network layer of the TCP/IP model. TCP/IP is the most widely used model as compared to the OSI model for providing communication between computers over the [internet](https://www.javatpoint.com/internet).

## Functions of TCP/IP layers:



Similarities between the OSI and TCP/IP model

**The following are the similarities between the OSI and TCP/IP model:**

* **Share common architecture**

Both the models are the logical models and having similar architectures as both the models are constructed with the layers.

* **Define standards**

Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

* **Simplified troubleshooting process**

Both models have simplified the troubleshooting process by breaking the complex function into simpler components.

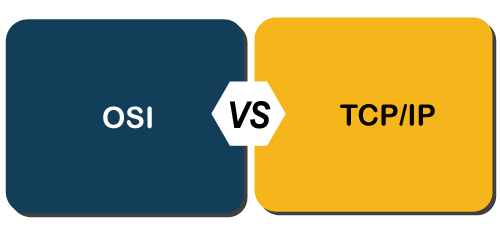
* **Pre-defined standards**

The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.

* **Both have similar functionality of 'transport' and 'network' layers**

The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

Differences between the OSI and TCP/IP model



**Let's see the differences between the OSI and TCP/IP model in a tabular form:**

|  |  |
| --- | --- |
| **OSI Model** | **TCP/IP Model** |
| It stands for **Open System Interconnection.** | It stands for **Transmission Control Protocol.** |
| OSI model has been developed by ISO (International Organization for Standardisation). | It was developed by ARPANET (Advanced Research Project Agency Network). |
| It is an independent standard and generic protocol used as a communication gateway between the network and the end user. | It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts. |
| In the OSI model, the transport layer provides a guarantee for the delivery of the packets. | The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model. |
| This model is based on a vertical approach. | This model is based on a horizontal approach. |
| In this model, the session and presentation layers are separated, i.e., both the layers are different. | In this model, the session and presentation layer are not different layers. Both layers are included in the application layer. |
| It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool. | It is an implemented model of an OSI model. |
| In this model, the network layer provides both connection-oriented and connectionless service. | The network layer provides only connectionless service. |
| Protocols in the OSI model are hidden and can be easily replaced when the technology changes. | In this model, the protocol cannot be easily replaced. |
| It consists of 7 layers. | It consists of 4 layers. |
| OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent. | In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent. |
| The usage of this model is very low. | This model is highly used. |
| It provides standardization to the devices like router, motherboard, switches, and other hardware devices. | It does not provide the standardization to the devices. It provides a connection between various computers. |

**What is IP?**

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., [TCP/IP](https://www.javatpoint.com/tcp-ip-full-form) and UDP/IP, so internet protocol is also known as [TCP/IP](https://www.javatpoint.com/computer-network-tcp-ip-model) or [UDP](https://www.javatpoint.com/udp-full-form)/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

History of Internet Protocol

The development of the protocol gets started in 1974 by **Bob Kahn and Vint Cerf**. It is used in conjunction with the Transmission Control Protocol (TCP), so they together named the [TCP/IP](https://www.javatpoint.com/tcp-ip-full-form).

The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.

After IPv4, the second major version of the internet protocol was IPv6, which was version 6. It was officially declared by the IETF in 1998. The main reason behind the development of IPv6 was to replace IPv4. There is a big difference between IPv4 and IPv6 is that IPv4 uses 32 bits for addressing, while IPv6 uses 128 bits for addressing.

Function

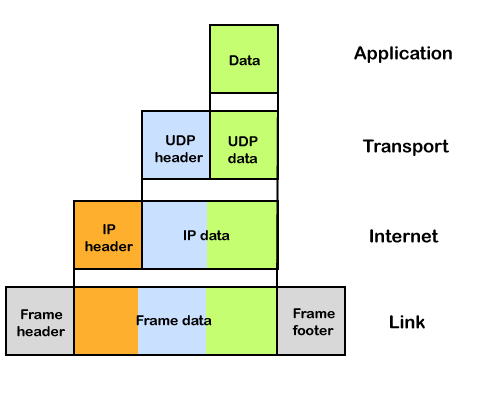
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more [IP](https://www.javatpoint.com/ip-full-form) networks. In order to achieve these functionalities, [internet](https://www.javatpoint.com/internet) protocol provides two major things which are given below.

**An internet protocol defines two things:**

* Format of IP packet
* IP Addressing system

What is an IP packet?

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

* Source IP address: The source is the one who is sending the data.
* Destination IP address: The destination is a host that receives the data from the sender.
* Header length
* Packet length
* TTL (Time to Live): The number of hops occurs before the packet gets discarded.
* Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

**Payload:** Payload is the data that is to be transported.

How does the IP routing perform?

IP routing is a process of determining the path for data so that it can travel from the source to the destination. As we know that the data is divided into multiple packets, and each packet will pass through a web of the router until it reaches the final destination. The path that the data packet follows is determined by the routing algorithm. The routing algorithm considers various factors like the size of the packet and its header to determine the efficient route for the data from the source to the destination. When the data packet reaches some router, then the source address and destination address are used with a routing table to determine the next hop's address. This process goes on until it reaches the destination. The data is divided into multiple packets so all the packets will travel individually to reach the destination.

**For example**, when an email is sent from the email server, then the TCP layer in this email server divides the data into multiple packets, provides numbering to these packets and transmits them to the IP layer. This IP layer further transmits the packet to the destination email server. On the side of the destination server, the IP layer transmits these data packets to the TCP layer, and the TCP layer recombines these data packets into the message. The message is sent to the email application.

What is IP Addressing?

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

**Types of IP addresses**

IPv4 addresses are divided into two categories:

* **Public address**
* **Private address**

Public address

The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

**Key points related to public address are:**

* The scope of the public address is global, which means that we can communicate outside the network.
* This address is assigned by the ISP (Internet Service Provider).
* It is not available at free of cost.
* We can get the Public IP by typing on Google "What is my IP".

Private address

A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smartphones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.

If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

**Key points related to private address are:**

* Its scope is local, as we can communicate within the network only.
* It is generally used for creating a local area network.
* It is available at free of cost.
* We can get to know the private IP address by simply typing the "ipconfig" on the command prompt.

IPv4 vs IPv6

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a [TCP/IP](https://www.javatpoint.com/tcp-ip-full-form). It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An [IP](https://www.javatpoint.com/ip-full-form) address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

* IPv4
* IPv6

What is IPv4?

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods, a.b.c.d. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

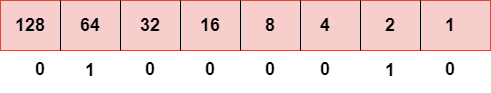
**Representation of 8 Bit Octet**

IPv4 vs IPv6

The above representation shows the structure of 8- bit octet.

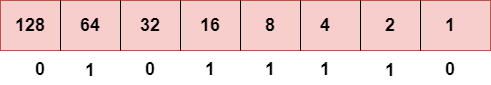
Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

**Step 1: First, we find the binary number of 66.**



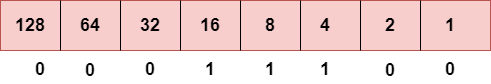
To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

**Step 2: Now, we calculate the binary number of 94.**



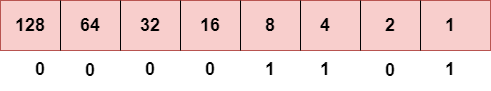
To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

**Step 3: The next number is 29.**



To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

**Step 4: The last number is 13.**



To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

What is IPv6?

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit **hexadecimal address**. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

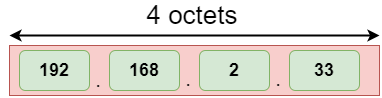
* **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
* **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
* **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4\*1038) addresses.

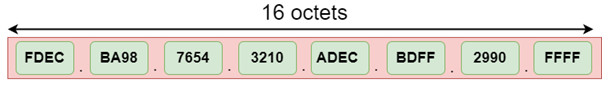
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

**The address format of IPv4:**



**The address format of IPv6:**



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

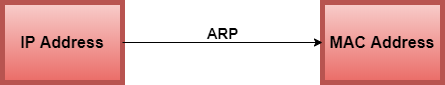
Differences between IPv4 and IPv6



|  |  |  |
| --- | --- | --- |
|  | **Ipv4** | **Ipv6** |
| **Address length** | IPv4 is a 32-bit address. | IPv6 is a 128-bit address. |
| **Fields** | IPv4 is a numeric address that consists of 4 fields which are separated by dot (.). | IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon. |
| **Classes** | IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E. | IPv6 does not contain classes of IP addresses. |
| **Number of IP address** | IPv4 has a limited number of IP addresses. | IPv6 has a large number of IP addresses. |
| **VLSM** | It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes. | It does not support VLSM. |
| **Address configuration** | It supports manual and DHCP configuration. | It supports manual, DHCP, auto-configuration, and renumbering. |
| **Address space** | It generates 4 billion unique addresses | It generates 340 undecillion unique addresses. |
| **End-to-end connection integrity** | In IPv4, end-to-end connection integrity is unachievable. | In the case of IPv6, end-to-end connection integrity is achievable. |
| **Security features** | In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind. | In IPv6, IPSEC is developed for security purposes. |
| **Address representation** | In IPv4, the IP address is represented in decimal. | In IPv6, the representation of the IP address in hexadecimal. |
| **Fragmentation** | Fragmentation is done by the senders and the forwarding routers. | Fragmentation is done by the senders only. |
| **Packet flow identification** | It does not provide any mechanism for packet flow identification. | It uses flow label field in the header for the packet flow identification. |
| **Checksum field** | The checksum field is available in IPv4. | The checksum field is not available in IPv6. |
| **Transmission scheme** | IPv4 is broadcasting. | On the other hand, IPv6 is multicasting, which provides efficient network operations. |
| **Encryption and Authentication** | It does not provide encryption and authentication. | It provides encryption and authentication. |
| **Number of octets** | It consists of 4 octets. | It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16. |

# Address Resolution Protocol (ARP)

ARP stands for **Address Resolution Protocol**, which is used to find the MAC address of the device from its known IP address. This means, the source device already knows the IP address but not the MAC address of the destination device. The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address. So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.



**Scenario 1: When the data packet is lost or erroneous.**

The purpose of ARP is to convert the 32-bit logical address (IPv4 address) to the 48-bit physical address (MAC address). This protocol works between layer 2 and layer 3 of the OSI model. The MAC address resides at layer 2, which is also known as the data link layer and IP address resides at layer 3, this layer is also known as the network layer.

#### Note: The ARP request is generated only when both the devices (source and destination) are in the same network.

**Example:** Suppose two devices (device A and device B) want to communicate with each other. The device A already knows the [IP](https://www.javatpoint.com/ip-full-form) address of the Device B. But in order to communicate with the device B, device A still needs the MAC address of the device B. The **IP address** is used to locate a device on a local area network and the **MAC address** is used to identify the actual device. The device A first look at its internal list known as ARP cache (table) to check if the IP address of the device B already consists of its MAC address or not. If the [ARP table](https://www.javatpoint.com/arp-table) consists of the MAC address of the device B, then device A simply use that MAC address and start communication.

If the table does not consist of the MAC address of device B, then device A sends an ARP broadcast message on the network to know which device has that specific IP address and ask for the MAC address of that particular device. Then the device that has matching IP address to the source address sends an ARP response message that consists of the MAC address of the device B. When device A obtains the MAC address of the device B, it will store the information in the ARP cache (table). The ARP cache is used to make the network more efficient. It stores the IP address of the device along with its MAC address. The stored information is used when device A wants to communicate with device B on a network, and it does not need to broadcast a message on the network again. It will simply check the ARP cache for the entries and then use it for communication.

#### Note: The ARP request message is broadcast in nature, but the ARP response message is unicast.

### Types of Mapping in ARP

**There are two different ways to map the IP address into the MAC address, which are given below:**

* Static Mapping
* Dynamic Mapping

**Static Mapping -** In the static mapping, a table consists of a logical address and corresponding physical address of the destination device. In this, the IP and MAC address of the device is entered manually in an ARP table. The source device has to access the table first if a source wants to communicate with the destination device.

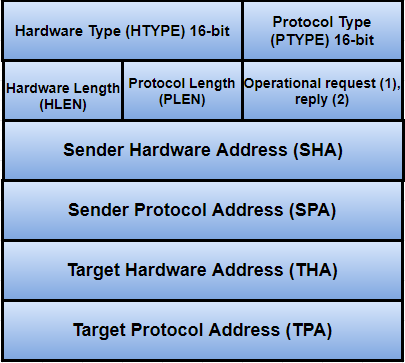
**Dynamic Mapping -** In the dynamic mapping, if a device knows the logical address of the other device, then by using the Address Resolution protocol, this device will also find the physical address of the device. The dynamic entries are created automatically when the source device sends an ARP broadcast request. These entries are not permanent and cleared periodically.

# ARP Packet Format

The address resolution protocol (ARP) uses a basic message format that contains either address resolution request or address resolution response. The ARP message size depends on the address size of the link layer and the network layer. The message header describes the network type used at each layer and the address size of each layer. The message header is complete with the help of the operation code, which is **1** for **request** and **2** for the **response**. The payload of the packet has four addresses, these are:

* Hardware address of the sender hosts
* Hardware address of the receiver hosts
* Protocol address of the sender hosts
* Protocol address of the receiver hosts

**The Packet format of the Address Resolution Protocol is shown in the figure:**



**HTYPE (Hardware Type) -** The size of the hardware type field is 16 bit. This field defines the network type that the local network needs to transmit the ARP message. There are some typical values for this field, which are given below:

|  |  |
| --- | --- |
| **Hardware Type (HTYPE)** | **Value** |
| Ethernet | 1 |
| IEEE 802 Networks | 6 |
| ARCNET | 7 |
| Frame Relay | 15 |
| Synchronous Transfer Mode (STM) | 16 |
| HDLC - High-level Data Link Control | 17 |
| Fibre Channel | 18 |
| Asynchronous Transfer Mode (ATM) | 19 |
| Serial Line | 20 |

**PTYPE (Protocol Type) -** The protocol type is a 16-bit field used to specify the type of protocol.

#### Note: ARP can be used with any higher-level protocol such as IPv4, IPv6, etc.

**HLEN (Hardware Length) -** The size of the hardware length field is 8-bit. This field specifies the length of the physical address in bytes.

**Example:** For this, the address length of Ethernet is 6.

**PLEN (Protocol Length) -** The size of the protocol length field is 8-bit long. It defines the length of the IP address in bytes.

**OPER (Operation) -** It is a 16-bit field that determines the type of ARP packet. There are two types of ARP packets, i.e., ARP request and ARP Reply. In the given table, the first two values are used for the ARP request and reply. The values for the other ARP frame format such as RARP, DRARP, etc. are also specified in this table.

|  |  |
| --- | --- |
| **ARP Message Type** | **Opcode (Operation Code)** |
| ARP Request | 1 |
| ARP Reply | 2 |
| RARP Request | 3 |
| RARP Reply | 4 |
| DRARP(Dynamic Reverse Address Resolution Protocol) Request | 5 |
| DRARP Reply | 6 |
| DRARP Error | 7 |
| InARP Request | 8 |
| InARP Reply | 9 |

**SHA (Sender Hardware Address) -** This field specifies the physical address of the sender, and the length of this field is not fixed.

**SPA (Sender Protocol Address) -** This field is used to determine the logical address of the sender, and the length of this field is not fixed.

**THA (Target Hardware Address) -** The target hardware address specifies the physical address of the target. It is a variable-length field. For the ARP request packet, this field contains all zeros because the sender does not know the physical address of the receiver.

#### Note: The default target hardware address is zero.

**TPA (Target Protocol Address) -** This field determines the logical address of the target. TPA is a variable-length field.