DATA COMMUNICATION & COMPUTER NETWORKS

(IT 3rd Semester)

Presented by: Pankaj Gautam

राजकीय बहुतकनीकी, हमीरपुर(हि.प्र.)
GOVT. POLYTECHNIC, HAMIRPUR (H.P.)

Chapter -5

TCP/IP Protocol Suite

Topics discussed in this chapter:

- **TCP/IP Model - Layers**
- **Network Layer : IP**
- **Transport Layer : TCP UDP**
- **Application Layer : DNS TELNET FTP DHCP**

TCP/IP Model

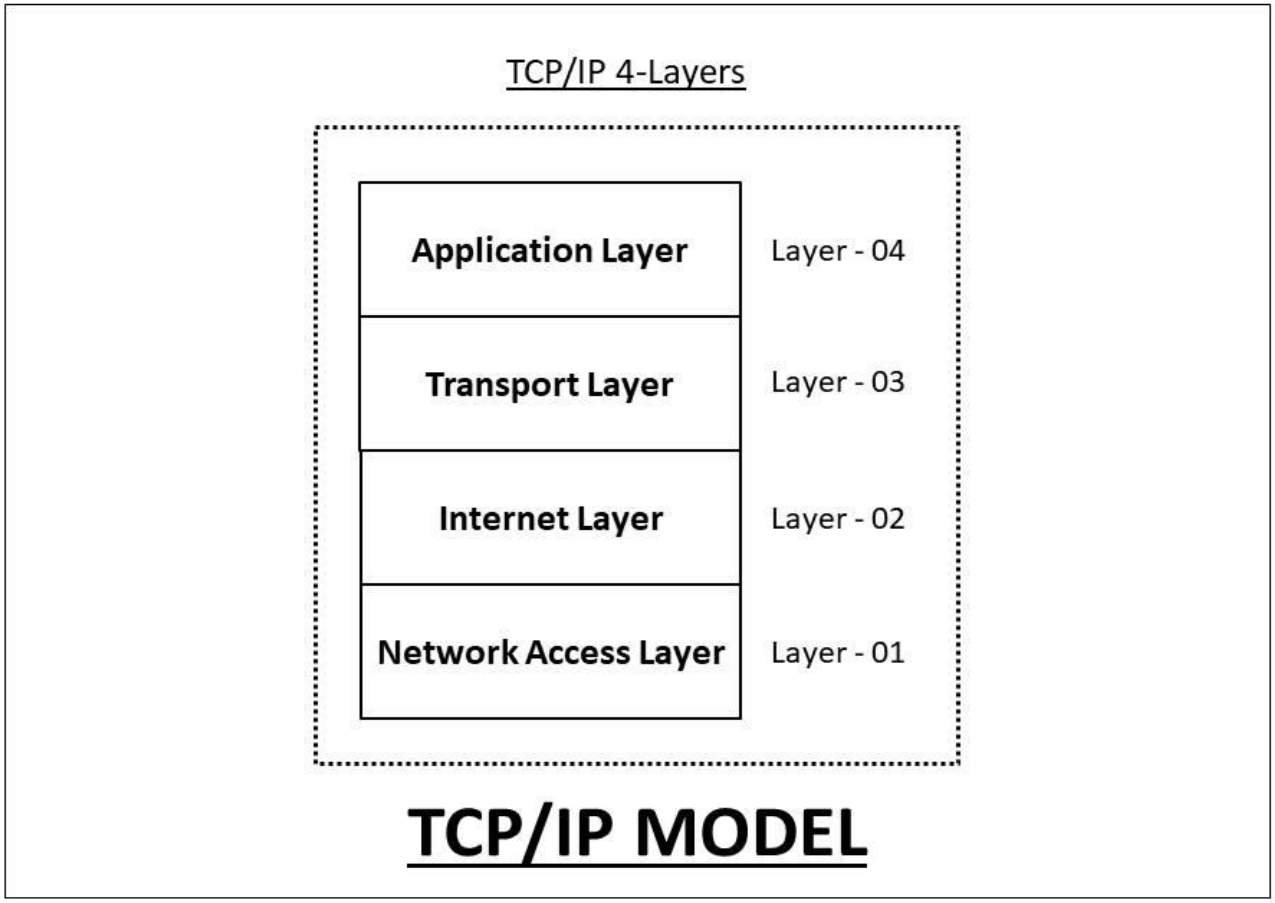
The TCP/IP reference model is a layered model developed by the Defense Project Research Agency(ARPA or DARPA) of the United States as a part of their research project in 1960.

Initially, it was developed to be used by defense only. But later on, it got widely accepted. The main purpose of this model is to connect two remote machines for the exchange of information. These machines can be operating in different networks or have different architecture.

TCP/IP network model is named after two main protocols(TCP and IP) and is widely used in current internet architecture.

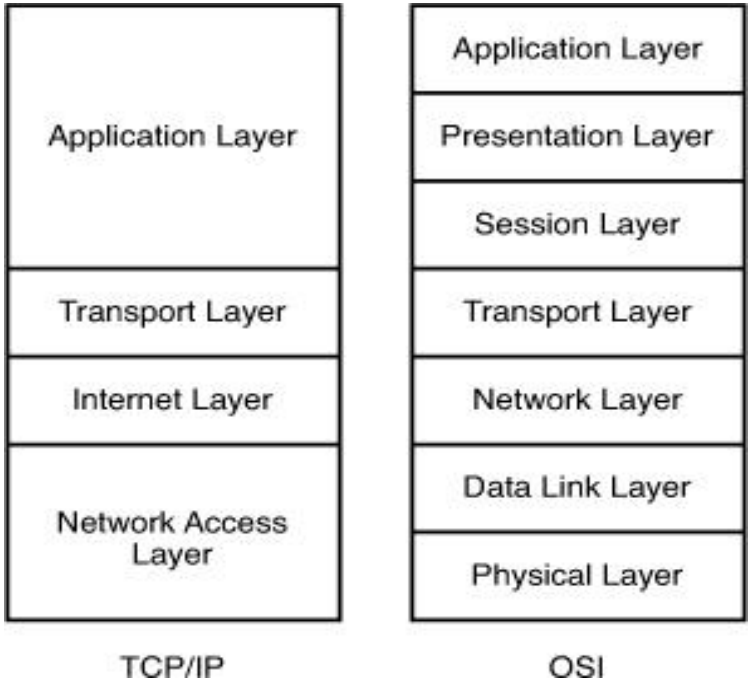
Layers in TCP/IP Model

In the early days, the TCP/IP reference model has four layers, as described below.

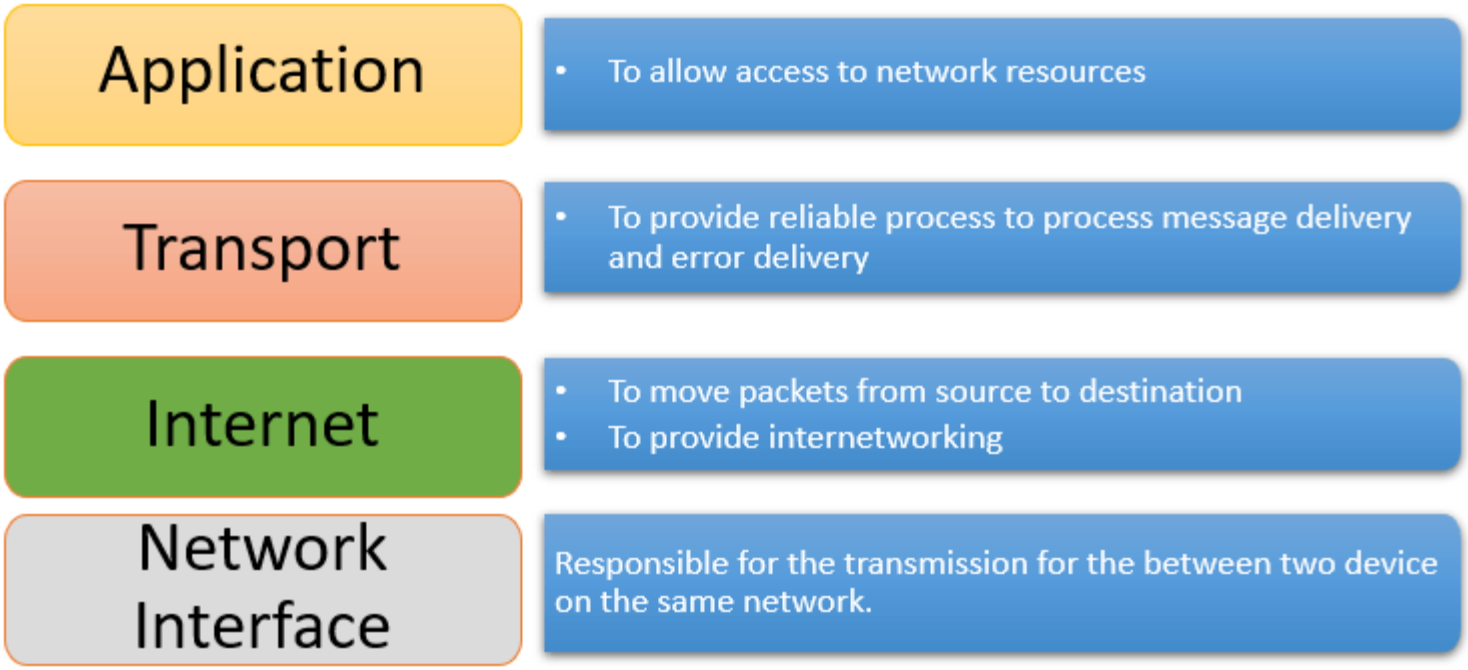


Layers in TCP/IP Model

These layers are much similar to the layers of the OSI model. The Application layer in the TCP/IP model has approximately the same functionality as the upper three layers(Application, Presentation, and Session layer) of the OSI model. Also, the Internet layer acts as the Network layer, and the Network Access layer acts as the lower two layers(Physical and Data-Link layer) of the OSI model.

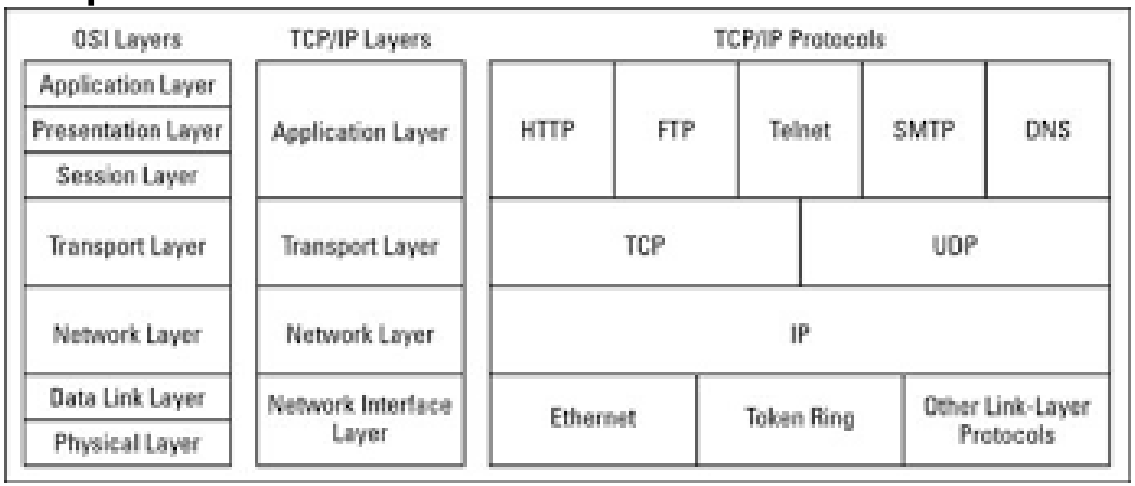


Layers in TCP/IP Model



TCP/IP Protocol Suite

The TCP/IP protocol suite, also known as the Internet Protocol Suite, is a set of networking protocols and standards that form the foundation for the Internet and most modern networks. It was developed in the 1970s and 1980s and has become the basis for communication in the digital world. The suite is named after its two most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). The TCP/IP suite is organized into four layers, which are responsible for different aspects of network communication:



TCP/IP Protocol Data units

In telecommunications, a protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network. It is composed of protocol-specific control information and user data.

Protocol data units for the TCP/IP protocol suite are:

- The transport layer PDU is the **TCP segment** for TCP, and the **datagram** for UDP

- The Internet layer PDU is the **packet**.

- The network interface layer PDU is the **frame**.

Network Interface Layer

The network interface layer is the lowest layer of the TCP/IP model and is concerned with the physical transmission of data. It is also called a host-to-network layer or link layer. It can be considered as the combination of physical layer and data link layer of the OSI model.

The functions of this layer are :

1. It defines how bits are to be encoded into optical or electrical pulses.
2. It accepts IP packets from the network layer and encapsulates them into frames. It synchronizes the transmission of the frames as well as the bits making up the frames, between the sender and the receiver.
3. It states the transmission mode, i.e. simplex, half duplex or full duplex
4. It states the topology of the network, i.e. bus, star, ring etc.

The protocols that this layer supports are :

Ethernet, Frame Relay, Token Ring, and ATM

Internet Layer

The Internet layer is responsible for logical transmission of data packets over the internet. It can be compared to the network layer of the OSI model.

The functions of this layer are :

1. It transmits data packets to the network interface layer.
2. It routes each of the data packets independently from the source to the destination, using the optimal route.
3. It reassembles the out-of-order packets when they reach the destination.
4. It handles the error in transmission of data packets and fragmentation of data packets.

The protocols that this layer supports are :

1. **IP (Internet Protocol),**
2. **ICMP (Internet Control Message Protocol),**
3. **IGMP (Internet Group Management Protocol),**
4. **ARP (Address Resolution Protocol),**
5. **RARP (Reverse Address Resolution Protocol)**

Internet Layer

IP (Internet Protocol):

It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called datagrams that travel over different routes across multiple nodes.

ICMP (Internet Control Message Protocol):

It monitors sending the queries as well as the error messages.

IGMP (Internet Group Management Protocol):

It allows the transmission of a message to a group of recipients simultaneously.

Internet Layer

ARP (Address Resolution Protocol):

This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.

RARP (Reverse Address Resolution Protocol):

This is to find the Internet address of a host when its physical address is known.

IP Addressing

An IP address (internet protocol address) is a logical numeric address which is used to uniquely identify a device on a computer network.

There are two versions of IP in use today, IPv4 and IPv6.

Addresses in **IPv4** are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses. The original IPv4 protocol is still used today on both the internet, and many corporate networks.

However, the IPv4 protocol only allowed for 2^{32} addresses. This, along with how addresses were allocated, led to a situation where there would not be enough unique addresses for all devices connected to the internet.

IP Addressing

Addresses in **IPv6** are 128-bits, which allows for 3.4 x 10^{38} (2^{128}) unique addresses.

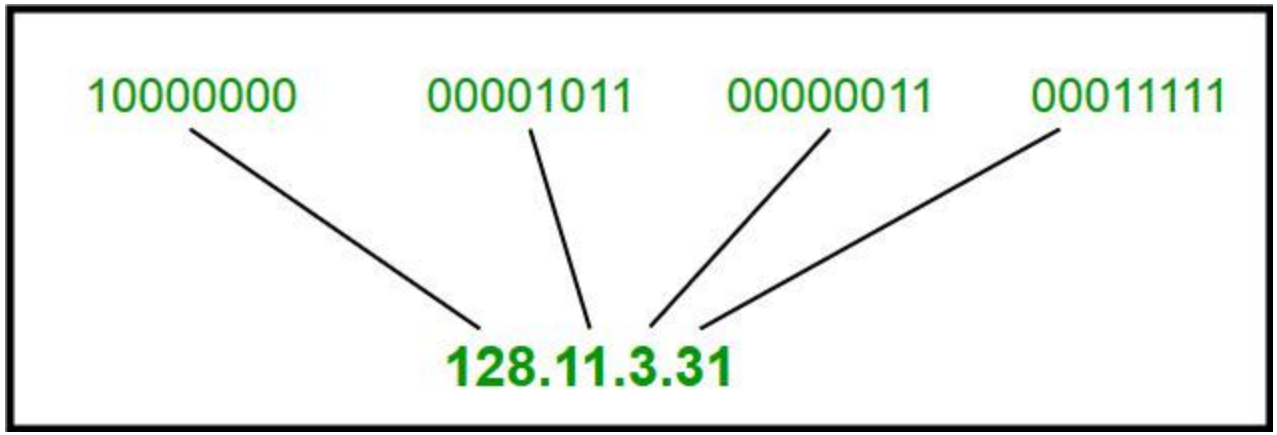
IPv6 was developed by the Internet Engineering Task Force (IETF), and was formalized in 1998. This upgrade substantially increased the available address space and allowed for 2^{128} addresses. In addition, there were changes to improve the efficiency of IP packet headers, as well as improvements to routing and security.

IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

IPv4 Addresses

IPv4 addresses are actually 32-bit binary numbers.

An IPv4 address is typically expressed in dotted-decimal notation, with every eight bits (octet) represented by a number from 0 to 255, each separated by a dot. An example IPv4 address would look like this: **128.11.3.31**
In other words, the address **128.11.3.31** represents the 32-bit binary number 10000000 00001011 00000011 00011111



IPv4 Addresses

IPv4 addresses are composed of two parts, The first part identifies the network and second identifies the host to that network, with an imaginary boundary separating the two. A subnet mask specifies which part of an address is the network identifier, and which part is host identifier.

Subnet Mask:

Subnet mask is a 32-bit bitmask that is when applied to a given IP address gives the Network Identifier. In simple words subnet mask is a 32-bit binary number containing a stream of 1's followed by 0's. 1's in subnet mask refer to network identifier in associated IP address, and 0's refer to host identifier.

For Example : 255.255.255.0

IPv4 Addresses

Subnet Mask Example:

IP address	**192.160.13.21**	**11000000**	**10100000**	**00001101**	**00010101**
Subnet mask	**255.255.255.0**	**11111111**	**11111111**	**11111111**	**00000000**
N/W Address	**192.160.13.0**	**11000000**	**10100000**	**00001101**	**00000000**
Host address	**0 . 0. 0. 21**	**00000000**	**00000000**	**00000000**	**00010101**

IPv4 Address Classes

During the development of the TCP/IP protocol stack IP addresses were divided into five classes: A, B, C, D & E.

Class	Range of IP v4 Addresses	Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D (Multicast)	224.0.0.0 to 239.255.255.255	
E (Reserved)	240.0.0.0 to 255.255.255.255	

IPv4 Address Classes

Class	Leading bits	Subnet Mask	Number of bits in Network Identifier	Number of bits in Host Identifier	Number of networks	Host Addresses per network	Starting address	Last address
Class A	0	255.0.0.0	8	24	2^7	2^{24} - 2	0.0.0.0	127.255.255.255
Class B	10	255.255.0.0	16	16	2^{14}	2^{16}- 2	128.0.0.0	191.255.255.255
Class C	110	255.255.255.0	24	8	2^{21}	2^8- 2	192.0.0.0	223.255.255.255
Class D (multicast)	1110	255.255.255.255	N/A	N/A	N/A	N/A	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

IPv4 Address Classes

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.
The network ID is 8 bits long.
The host ID is 24 bits long.
In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.
The total number of networks in Class A = 2^7 = 128 (**0.0.0.0 to 127.0.0.0).** However, any address that begins with 127. is considered a loopback address.
The total number of hosts per network in Class A = 2^{24} - 2 = 16,777,214
Example for a Class A IP address: **2.134.213.2**

IPv4 Address Classes

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.
The Network ID is 16 bits long.
The Host ID is 16 bits long.
In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.
The total number of networks in Class B = 2^{14} = 16384 (128.0.0.0 to 191.255.0.0)
The total number of hosts per network in Class B = 2^{16} - 2 = 65534
Example for a Class B IP address: **162.42.137.25**

IPv4 Address Classes

Class C

In Class C, an IP address is assigned to only small-sized networks.
The Network ID is 24 bits long.
The host ID is 8 bits long.
In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.
The 8 bits of the host ID determine the host in a network.
The total number of networks = 2^{21} = 2097152 network address (192.0.0.0 to 223.255.255.0)
The total number of hosts per network in Class C = 2^8 - 2 = 254

Example for a Class C IP address: **212.142.7.205**

IPv4 Address Classes

Class D

Class D addresses are used for **multicasting** applications. Unlike the previous classes, the Class D is not used for "normal" networking operations. Class D addresses have their first three bits set to “1” and their fourth bit set to “0”. Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group’s IP address for receiver purposes.

Example for a Class D IP address: **232.42.78.165**

IPv4 Address Classes

Class E

Class E networks are defined by having the first four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is used as a broadcast address.

Example for a Class E IP address: **242.181.89.221**

IPv4 Addresses

Private addresses :

Within the address space, certain networks are reserved for private networks. Packets from these networks are not routed across the public internet. This provides a way for private networks to use internal IP addresses without interfering with other networks. The private networks are :

Network Class	Private Addresses
A	10.0.0.0 TO 10. 255.255 .255
B	172.16.0.0 TO 172.31.255.255
C	192.168.0.0 TO 192.168.255.255

IPv4 Addresses

Classless Inter-Domain Routing (**CIDR**) **:**

CIDR is a method for allocating IP addresses and for IP routing. The Internet Engineering Task Force introduced CIDR in 1993 to replace the previous **classful network addressing** architecture on the Internet. Its goal was to slow the rapid exhaustion of IPv4 addresses.
CIDR notation is a compact representation of an IP address and its associated network mask. CIDR notation specifies an IP address, a slash ('/') character, and a decimal number. The decimal number is the count of leading *1* bits in the subnet mask. The number can also be thought of as the number of bits in the network identifier.
112.16.1.14/8 represents the IPv4 address 112.16.1.14 with 8 bit network identifier(equivalent to 255.0.0.0 subnet mask).

Subnetting

***Subnetting* is a method for dividing a larger network in to a group of sub networks . It divides the entire address-space in to contiguous blocks(groups) and assigns them to each sub network formed.**

An organization that is granted a large block of addresses may want to create group of smaller networks (called subnets) and divide the addresses between the different subnets.
The rest of the world still sees the organization as one entity; however, internally there are several subnets.
All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets.
The organization, however, needs to create small sub-blocks of addresses, each assigned to specific subnets.

Subnetting

These sub-blocks are created by making change to the subnet mask.

***Subnetting* is done by increasing the number of 1's in the subnet mask.**

When we increase number of 1's in subnet mask it means that the bits which were previously being used for host id in the IP address will now becomes the part of network id. Which in-turn divides the address space in to smaller groups each having its own network id, that can be assigned to subnets.

Subnetting

Example: As an example, suppose an organization is given the block 197.12.40.0/24, which contains 256 addresses. The organization has four offices and needs to divide the addresses into four sub-blocks of 64 addresses each.

We can find the new masks as follows :-

no. of subnets to be formed = 4;
size of each subnet = 64
Therefore no. of bits to be shifted from host id to network id = 2 (as 4 = 2^2)
Given subnet mask = 255.255.255.0
(11111111 11111111 11111111 00000000)
Therefore new subnet mask = 255.255.255.192
(11111111 11111111 11111111 11000000)

Subnetting

Subnet 1 : Sub-network Id = 197.12.40.0
subnet mask = 255.255.255.192
IP Addresses: 197.12.40.0 – 197.12.40.63

Subnet 2 : Sub-network Id = 197.12.40.64
subnet mask = 255.255.255.192
IP Addresses: 197.12.40.64 – 197.12.40.127

Subnet 3 : Sub-network Id = 197.12.40.128
subnet mask = 255.255.255.192
IP Addresses: 197.12.40.128 – 197.12.40.191

Subnet 4 : Sub-network Id = 197.12.40.192
subnet mask = 255.255.255.192
IP Addresses: 197.12.40.192 – 197.12.40.255

IPv4 Addresses

Supernetting :

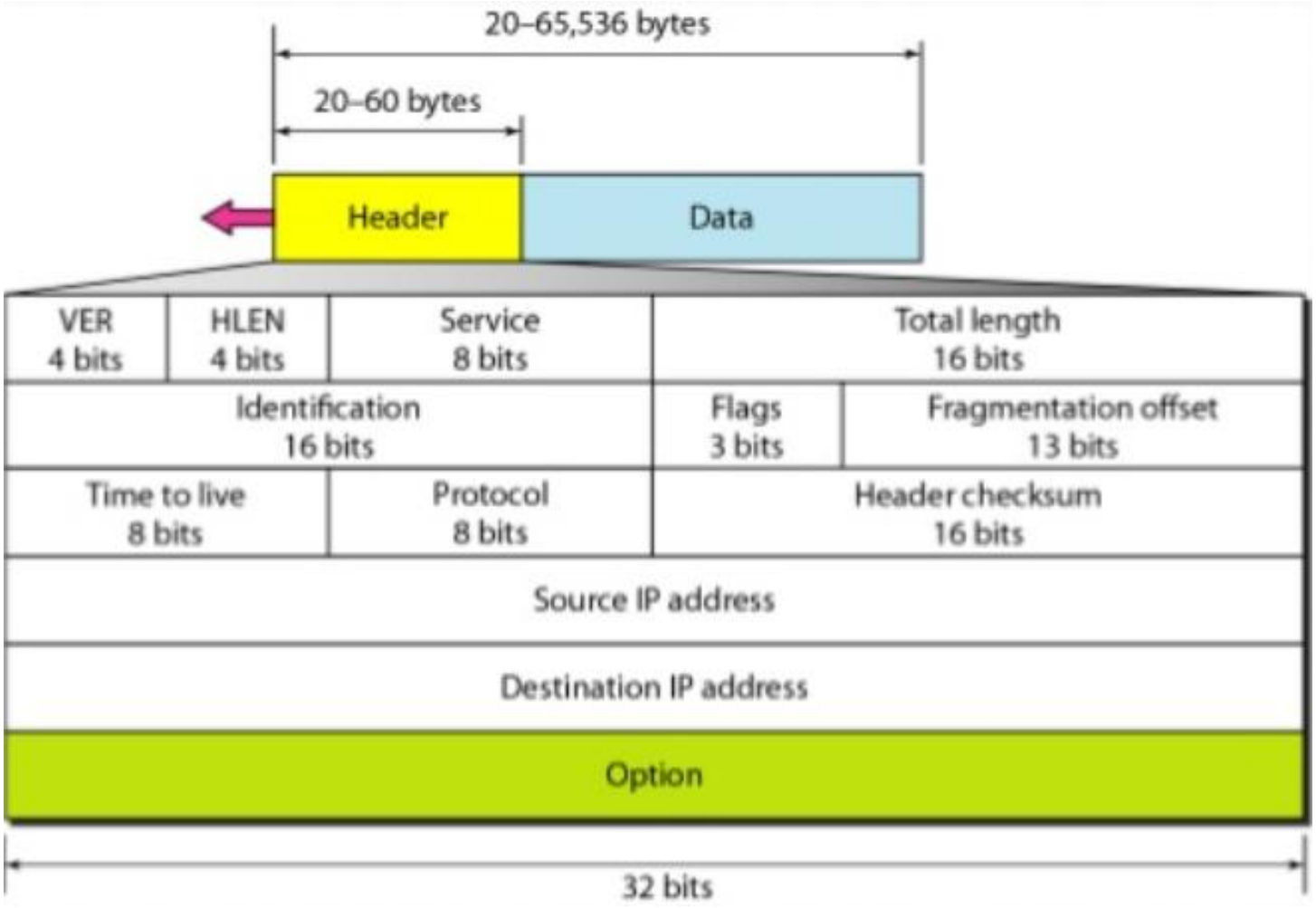
In supernetting, an organization can combine several class C blocks to create a larger range of addresses. In other words, several networks are combined to create a supernetwork or a supernet. An organization can apply for a set of class C blocks instead of just one. For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one super network.

Supernetting decreases the number of Is in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22.

However, classless addressing eliminated the need for supernetting.

IPv4 Header

IPv4 Header : Packets in the IPv4 layer are called datagrams. Following figure shows the IPv4 datagram format.



IPv4 Header

A datagram is a variable-length packet consisting of two parts: **header** and **data**. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.
It is customary in TCP/IP to show the header in 4-byte sections.
A brief description of each field is in order :

1. Version (VER): This 4-bit field defines the version of the IPv4 protocol. This field tells the IPv4 software running in the processing machine that the datagram has the format of version 4. All fields must be interpreted as specified in the fourth version of the protocol. If the machine is using some other version of IPv4, the datagram is discarded rather than interpreted incorrectly.

IPv4 Header

2. Header length (HLEN) : This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).

3. Services : IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

Type of Service

TOS Bits Description	TOS Bits Description
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

IPv4 Header

4. Total length : This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes.

5. Identification : This field is used in fragmentation.

6. Flags : This field is used in fragmentation.

7. Fragmentation offset : This field is used in fragmentation.

8. Time to live : A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero.

IPv4 Header

9. Protocol : This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP.

10. Checksum : This field is an error detection mechanism **s** based on the concept of redundancy. In case of IPv4 first, the value of the checksum field is set to 0. Then the entire header is divided into 16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field. The checksum in the IPv4 packet covers only the header, not the data.

IPv4 Header

11. Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

12. Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

13. Options : The header of the IPv4 datagram is made of two parts: a fixed part and a variable part. The fixed part is 20 bytes long. The variable part comprises the options that can be a maximum of 40 bytes. Options, can be used for network testing and debugging.

IPv6 Addresses

Need of IPv6 :

IPv4 has following deficiencies (listed below) that make it unsuitable for the fast-growing Internet:

1. *Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.*
2. *The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.*
3. *The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.*

IPv6 Addresses

Need of IPv6 :

To overcome these deficiencies, IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard.

IPv6 Addresses

Advantages of IPv6 :

The next-generation IP, or IPv6, has some advantages over IPv4 that can be summarized as follows:

1. **Larger address space**. An IPv6 address is 128 bits long, as compared with the 32-bit address of IPv4, this is a huge (2^96 times) increase in the address space.

2. **Better header format**. IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

IPv6 Addresses

Advantages of IPv6 :

3. **New options**. IPv6 has new options to allow for additional functionalities.
4. **Allowance for extension**. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
5. **Support for resource allocation**. In IPv6, the type-of-service field has been removed, but a mechanism (called jlow label) has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
6. **Support for more security**. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Transport Layer

The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host. It corresponds to the transport layer of the OSI model.

The functions of this layer are :

1. It facilitates the communicating hosts to carry on a conversation.
2. It provides an interface for the users to the underlying network.
3. It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.

The protocols that this layer supports are :

1. **Transmission Control Protocol (TCP)**
2. **User Datagram Protocol (UDP)**

Transmission Control Protocol (TCP)

The Transmission Control Protocol, or TCP protocol for short, is a standard for exchanging data between different devices in a computer network.

It provides **connection-oriented transport layer service**.

The TCP protocol allows two endpoints in a shared computer network to establish a connection that enables a **two-way transmission of data**.

Any data loss is detected and automatically corrected.

Transmission Control Protocol - Features

•TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender can know about whether the data packet is reached the destination or it needs to resend it.

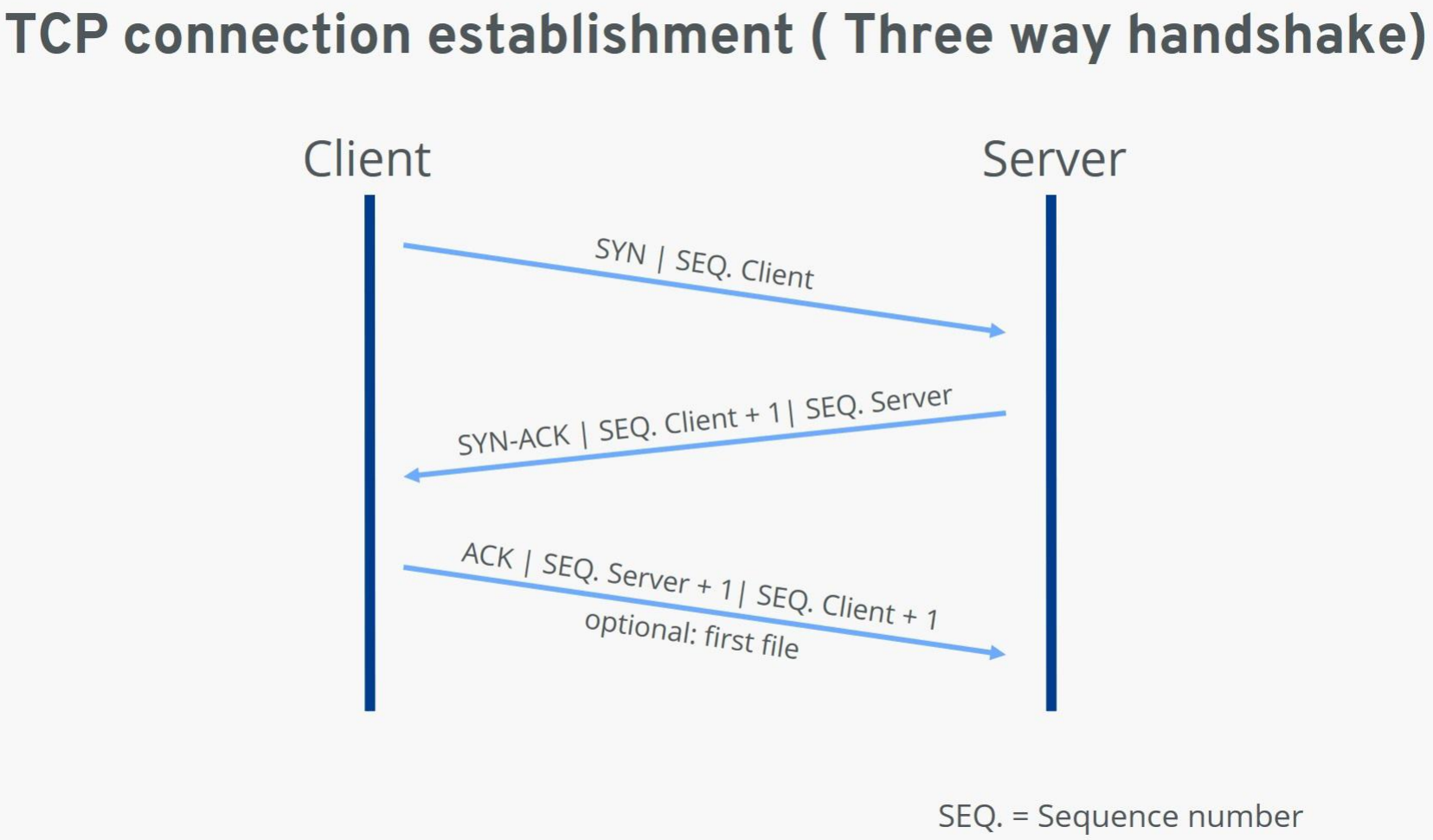
•TCP ensures that the data reaches destination in the same order it was sent.

•TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.

Transmission Control Protocol - Features

- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

TCP connection establishment(three-way handshake)



TCP connection establishment(three-way handshake)

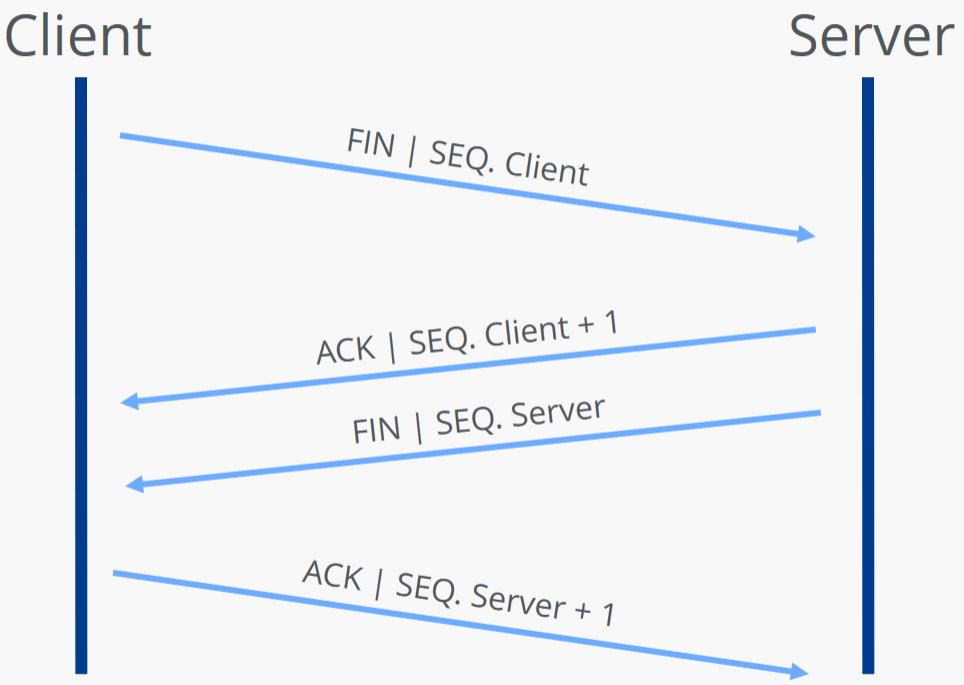
1. First, the requesting **client** sends the server a **SYN packet** or segment (SYN stands for synchronize) with a unique, random number. This number ensures full transmission in the correct order (without duplicates).

2. If the **server** has received the segment, it agrees to the connection by returning a **SYN-ACK** packet (ACK stands for acknowledgment) including the client's sequence number plus 1. It also transmits its own sequence number to the client.

3. Finally, the **client** acknowledges the receipt of the SYN-ACK segment by sending its own **ACK packet**, which in this case contains the server's sequence number plus 1. At the same time, the client can already begin transferring data to the server.

TCP connection termination

TCP connection termination (TCP Teardown)



SEQ. = Sequence number

TCP connection termination

1. The **client** sends a **FIN segment** to notify the server that it no longer wants to send data. It sends its own sequence number, just as it does when the connection is established.

2. The **server** acknowledges receipt of the package with an **ACK segment** that contains the sequence number plus 1.

3. When the **server** has finished the data transfer, it also sends a **FIN packet**, to which it adds its sequence number.

4. Now it is the **client's** turn to send an **ACK packet** including the sequence number plus 1, which officially terminates the TCP connection for the server.

Which applications use TCP?

- **Secure Shell (SSH), File Transfer Protocol (FTP), Telnet:** For peer-to-peer file sharing, and, in Telnet's case, logging into another user's computer to access a file.

- **Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP):** For sending and receiving email.

- **HTTP:** For web access.

User Datagram Protocol

The User Datagram Protocol, or UDP for short, is a protocol that allows **datagrams to be sent without connection** in IP-based networks.

UDP (User Datagram Protocol) is a connectionless protocol of the internet protocol family that operates at the transport layer.

User Datagram Protocol - Features

UDP is connectionless: Data transfer via UDP takes place without an existing connection between addressee and recipient. The respective packets are then sent to the preferred IP address, **specifying the target port**.

UDP uses ports: Like TCP, UDP uses ports so that the packets are transferred to the correct subsequent protocols or the desired applications on the target system.

UDP enables fast, delay-free communication: UDP is suitable for fast data transmission, due to the lack of connection setup. This also results from the fact that the loss of individual packets only affects the quality of the transmission. With TCP connections, on the other hand, lost packets are retransmitted.

User Datagram Protocol - Features

UDP does not guarantee the security and integrity of the data: The absence of mutual authentication between the sender and receiver ensures the excellent transmission speed of UDP – however, the protocol can neither guarantee the completeness nor the security of the data packets. The correct sequence of the sent packets is also not guaranteed.

Which applications use UDP?

"Best-effort delivery" applications: The classic deployment scenario for UDP is applications that are based on "data delivery to the best of our ability." Such programs, which use the User Datagram Protocol as a "best effort" service, transmit information unreliably because they are used to repeating this information. Examples are applications that transmit measured values or repeatedly execute the same work orders.

Lightweight applications: The low transport protocol overload provides optimal support for applications that are very simple in design. In combination with eliminating the need to establish a connection, these programs benefit from particularly high performance when processing and forwarding data packets in networks.

.

Which applications use UDP?

Applications with their own mechanisms for reliable transmission: UDP can also be interesting for applications that are actually dependent on reliable information exchange, but should have their own mechanisms for acknowledging packets.

Multicast applications: While reliable transport protocols such as TCP are limited to the use of end-to-end communication, UDP also supports IP multicast connections. If an application is to be able to send IP packets efficiently and quickly to many recipients at the same time, UDP is more suitable.

Real-time applications: UDP is also suitable as a transport protocol for services that work with real-time requirements – such as audio or video transmissions. They must be able to largely control the transmission, reception, and reproduction of data streams themselves, which is easily possible with connectionless UDP transmission.

TCP vs. UDP

Transmission control protocol (TCP)	User datagram protocol (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgement of data.	UDP has only the basic error checking mechanism using checksums.

TCP vs. UDP

Transmission control protocol (TCP)	User datagram protocol (UDP)
Acknowledgement segment is present.	No acknowledgement segment.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.

TCP vs. UDP

Transmission control protocol (TCP)	User datagram protocol (UDP)
TCP is heavy-weight.	UDP is lightweight.
Uses handshakes such as SYN, ACK, SYN-ACK	It’s a connectionless protocol i.e. No handshake
TCP doesn’t support Broadcasting.	UDP supports Broadcasting.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Port Address

In TCP/IP architecture the label assigned to a process is called a port address.

A port address in TCP/IP is a 16-bit unsigned number that is used to identify a specific process on a server.

The overall range of port numbers is 0-65536.

0 to 1023 are restricted port numbers are as they are used by well-known protocol services. These port numbers called well know ports.

1024 to 49151 are registered port numbers means it can be registered to specific protocols by software corporations and in last 49152 to 65536 are used as private ports means they can be used by anybody.

Common Well Known Ports

The Internet Assigned Numbers Authority (IANA) has assigned well known port numbers to commonly used services like SSH, FTP, HTTP, HTTPS, and others.

Port Number	Usage
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH)
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web

Common Well Known Ports

Port Number	Usage
110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

Application Layer

The Application layer in the TCP/IP model is equivalent to the upper three layers(Application, Physical, and Session Layer) of the OSI model. It deals with the communication of the whole data message.

The Application layer provides an interface between the network services and the application programs. It mainly provides services to the end-users to work over the network. For Example, file transfer, web browsing, etc.

This layer uses all the higher-level protocols like HTTP, HTTPS, FTP, NFS, DHCP, FMTP, SNMP, SMTP, Telnet, etc.

Simple Mail Transfer Protocol (SMTP)

SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet.

It is a program used for sending messages to other computer users based on e-mail addresses.

It provides a mail exchange between users on the same or different computers.

Simple Mail Transfer Protocol (SMTP)

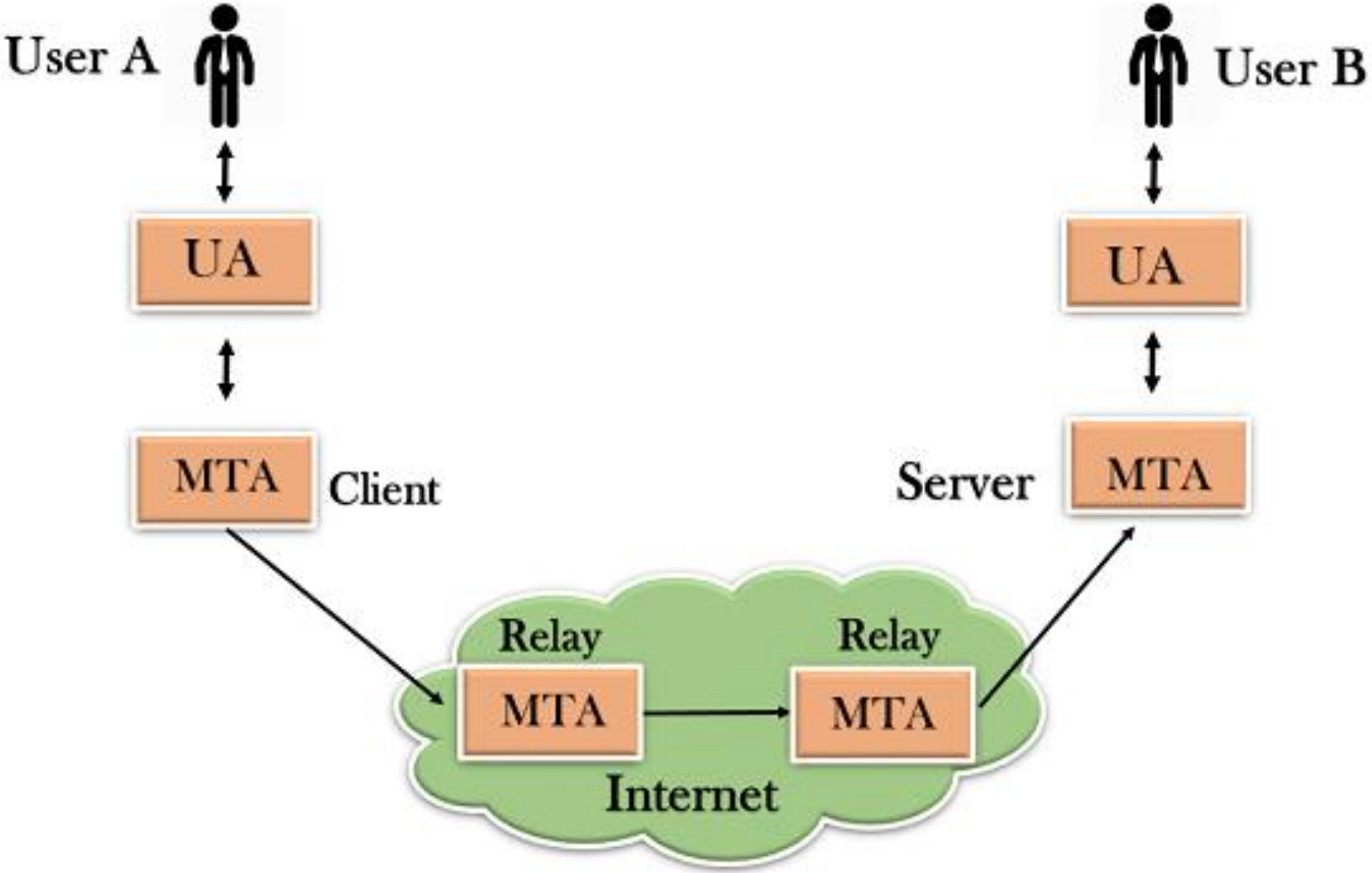
It can send a single message to one or more recipients.

Sending message can include text, voice, video or graphics.

It can also send the messages on networks outside the internet.

.

Simple Mail Transfer Protocol (SMTP)



Simple Mail Transfer Protocol (SMTP)

SMTP client and SMTP server contains two components, user agent (UA) and mail transfer agent (MTA).

The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope.

The mail transfer agent (MTA) transfers this mail across the internet.

Instead of just having one MTA there are multiple MTAs, acting either as a client or server to relay the email over the internet.

.

TELNET

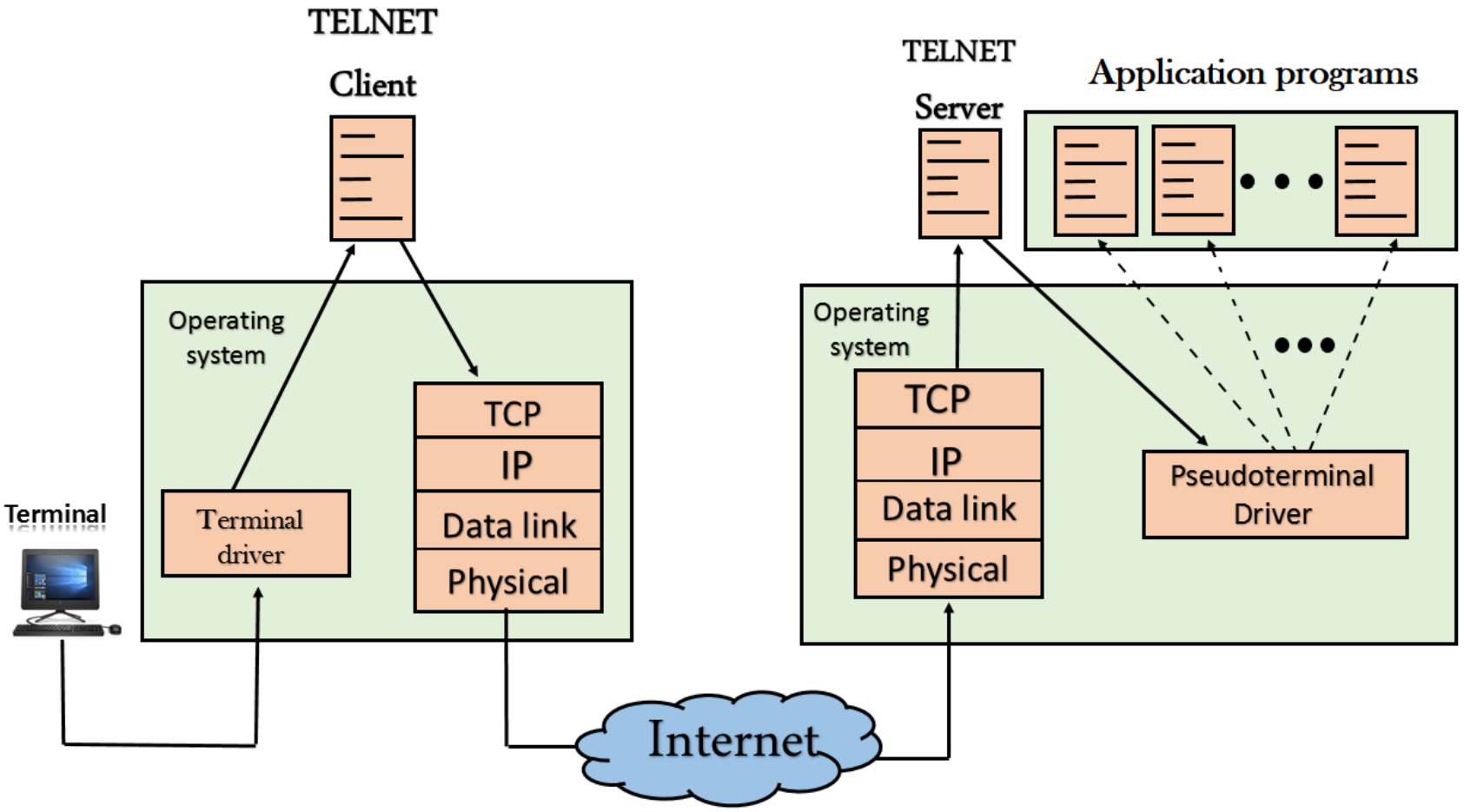
TELNET is a terminal emulation program for TCP/IP networks such as the Internet.

Telnet is a program that allows a user to log on to a remote computer.

The Telnet program runs on your computer and connects your PC to a telnet server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the remote system console.

To start a Telnet session, you must log in to a server by entering a valid username and password

TELNET : Remote Login



TELNET : Remote Login

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client delivers them to the local TCP/IP stack.

The commands are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer.

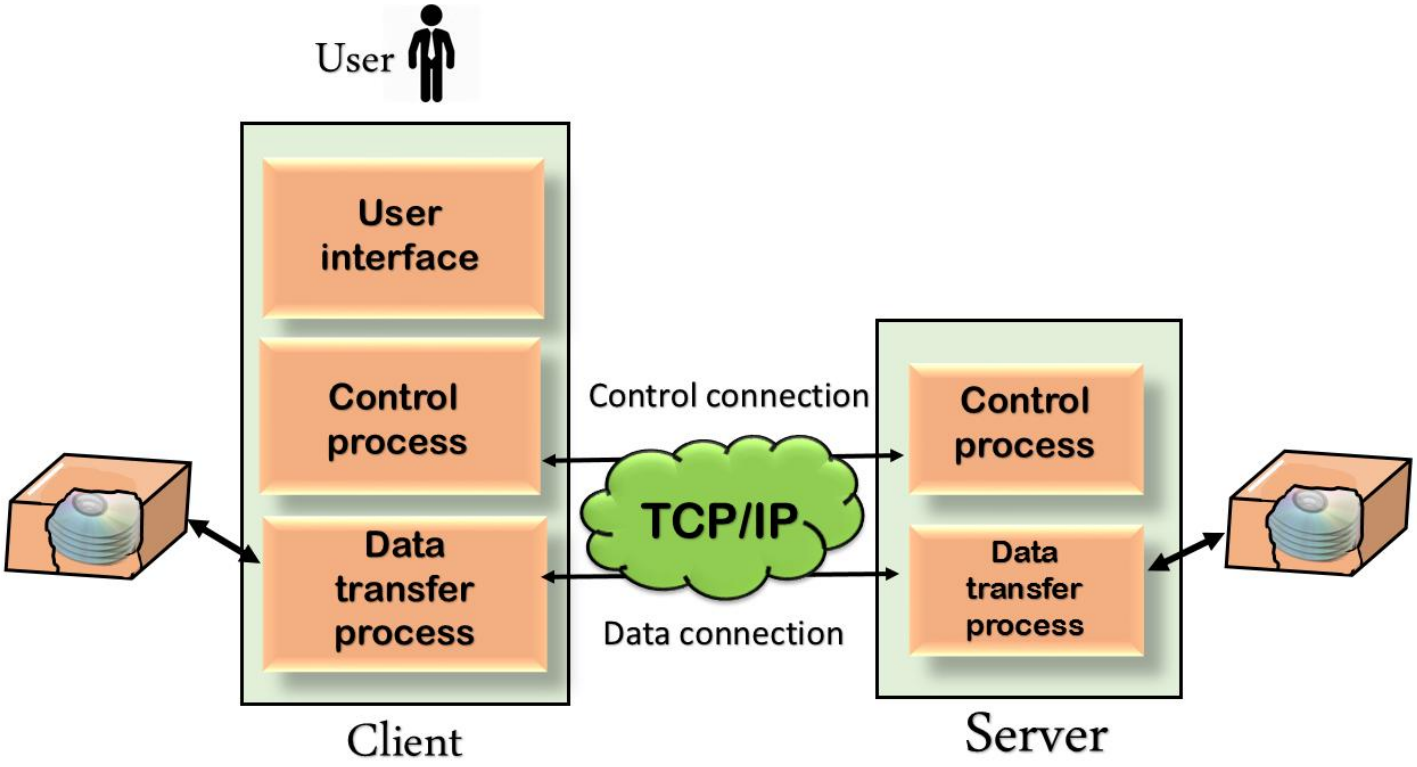
File Transfer Protocol (FTP)

File Transfer Protocol is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet.

FTP is built on client-server architecture and utilizes separate control and data connections between the client and server applications.

FTP is used with user-based password authentication or with anonymous user access.

File Transfer Protocol (FTP)

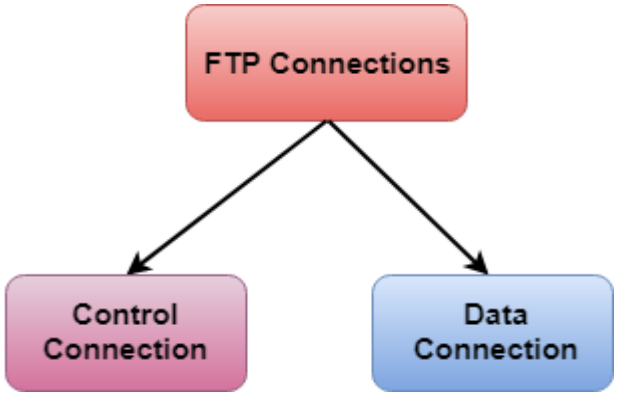


The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

FTP : Connections

Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.



FTP : Servers

Anonymous Server: Anonymous server is the most common use of FTP, the Internet file transfer protocol. FTP sites that allow anonymous FTP do not require a password for access. You only have to log in as anonymous and enter your e-mail address as password (for their records).

Non-anonymous Server: If you use a non-anonymous server, then you will log in as yourself and give your password.

FTP : Common commands

FTP hostname: This command written at the DOS prompt and it opens an interactive FTP session.

GET : get command is used to download a file from FTP server.
Syntax: ftp> get filename

PUT : get command is used to upload a file to the FTP Server.
Syntax: ftp> put <LocalFile> [<remoteFile>]

Dynamic Host Control Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that automatically assigns an IP address (as well as other related configurations) **to a device** .

Dynamic Host Control Protocol (DHCP)

Every computer on a network must have an IP address to communicate with other devices. **An IP address is an identifier for a computer or device on a network**.

There are two ways an IP address is assigned to a computer – **static and dynamic**. A static IP is where a user assigns an IP address manually to a computer. However, this process is tedious and error-prone as it requires manual intervention every time a device joins the network. Dynamic IP assignment resolves this issue.

A dynamic IP is where a computer receives an IP address from a DHCP server. Moreover, a DHCP server also assigns a device a subnet mask, default gateway, and the Domain Name System (DNS) server in addition.

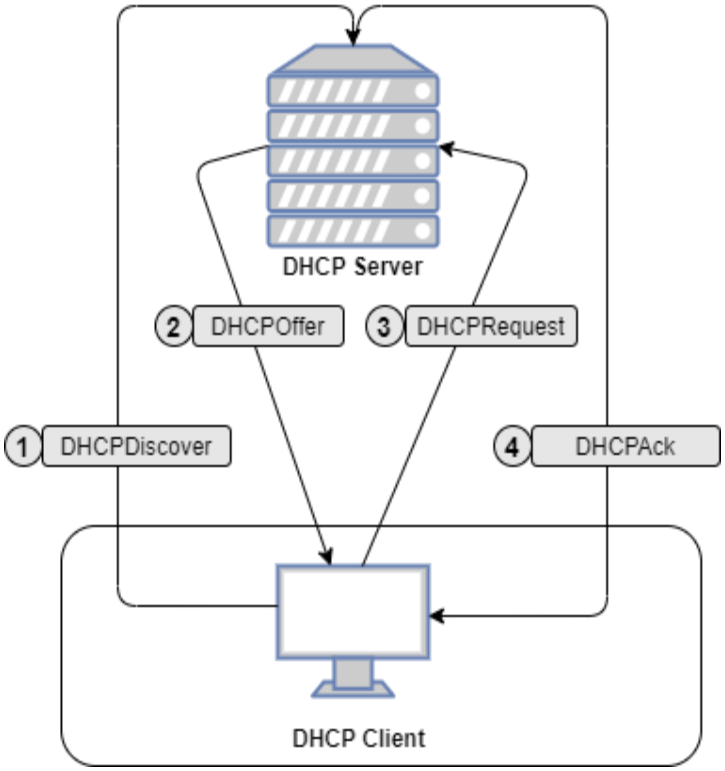
How does DHCP work?

1. ***Server Discovery**:* Once a device joins a network and requires an IP address, it broadcasts a message to the network asking for it. The DHCP server will process this request and all other devices in the network will ignore this message.

2. ***DHCP Offer**:* The DHCP server looks for an available IP address from its pool of addresses and offers one to the requesting device.

3. ***DHCP Request**:* The device responds to the DHCP server by confirming the provided IP address.

4. ***Acknowledgment:*** The DHPC server provides the IP address, subnet mask, default gateway and the DNS server details to the device.



DHCP Lease Time Management

The IP address information assigned by DHCP is only valid for a limited period of time and is known as a DHCP lease and the period of validity is called the DHCP lease time.

When the lease expires, the client can no longer use the IP address and has to stop all communication with the IP network unless it requests to extend the lease via the DHCP lease renewal cycle.

To avoid impacts of the DHCP server not being available at the end of the lease time, clients generally start renewing their lease halfway through the lease period. This renewal process ensures robust IP address allocation to devices.

Benefits of DHCP

DHCP offers several benefits over static IP configuration:

1. *Reliable IP address management:* **DHCP minimizes configuration errors caused by manual IP address configuration**, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time

2. *Reduced Manual Intervention:* DHCP lets network administrators **centralize and automate the IP address configuration process**. DHCP lets efficient management of IP addresses. For example, if a device leaves the network or moves to a different location, the assigned IP address is removed and assigned to another device

Thank You