GLS University

Faculty of Computer Application & IT

SY BCA

Semester - IV

2024-2025

210301404

Data Communication & Networks (DCN)

(Core Subject)

Unit 4 - OSI Model and TCP/IP IP Addressing

Supplementary Reading :

1. Forouzan, B. A. (2001). Data Communication and Networking. Tata McGraw Hill Education Private Limited.
2. Godbole, A. S. (2002). Data Communication and Computer Networks. Tata McGraw-Hill Companies.

Why IP Addresses?

- Classes of IP Addresses
  - IPV6 vs IPV4
- Introduction to CIDR
- Domain Name System (Overview)

OSI Model

- Introduction
- Functionality of OSI Layer

TCP/IP

- Introduction and its basic
- Layers and its Protocols

o Application Layer

▪ Telnet, SMTP, FTP, HTTP, TFTP, IP-RTP

o Transport Layer

▪ TCP, UDP

o Network Layer

▪ ICMP, IP, ARP, RARP

o Data Link Layer

o Physical Layer

IEEE Standards(Overview)

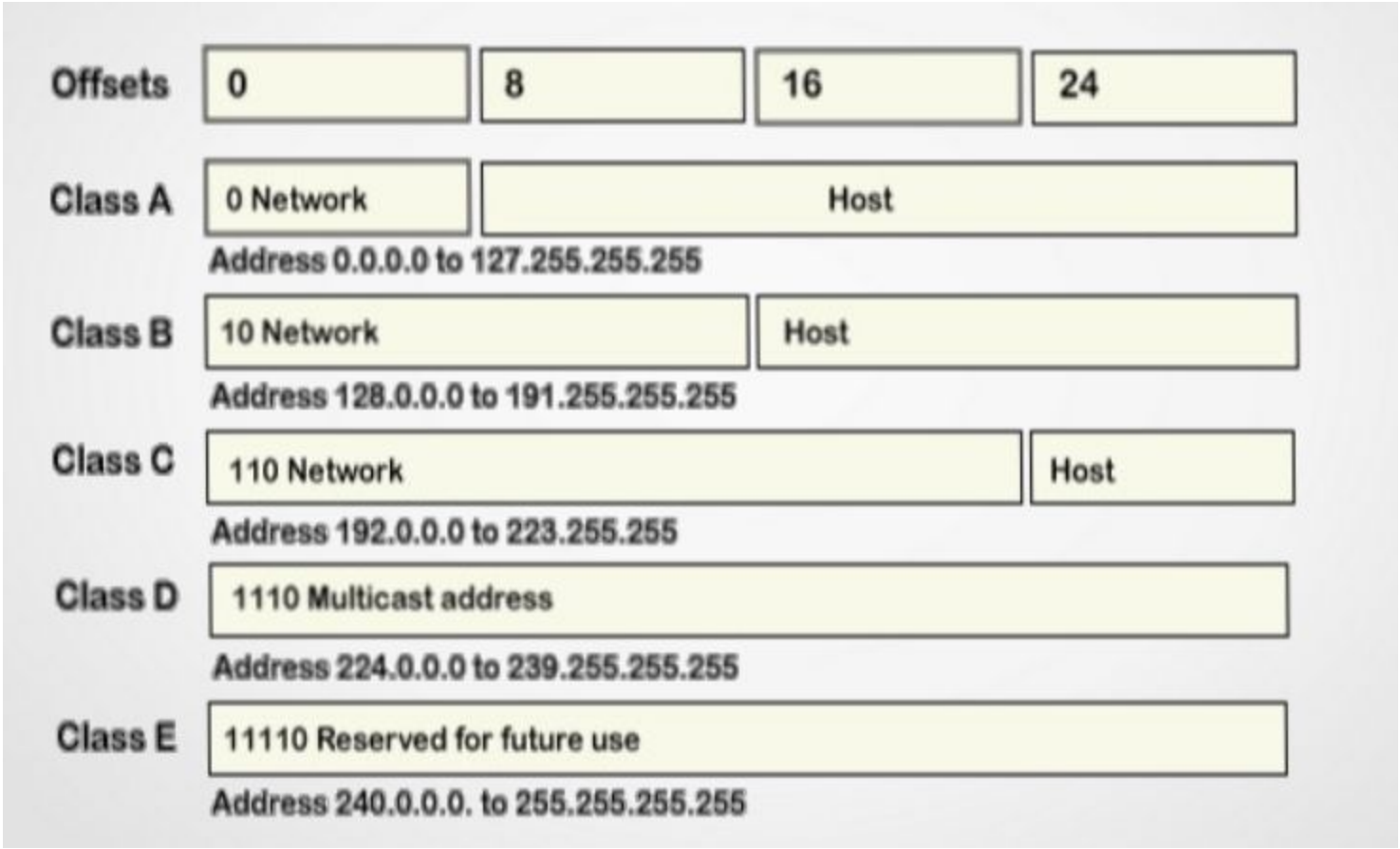
- IEEE 802.1
- IEEE 802.3
- IEEE 802.11
- IEEE 802.15
- CSMA/CD

IP address

What is an IP Address?

- An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication.
- IP address act as an identifier for a specific machine on a particular network.
- It also helps you to develop a virtual connection between a destination and a source.
- IP address is an address having information about how to reach a specific host, especially outside the LAN.
- An IP address is a 32 bit unique address.

- IP addresses were divided into five different categories called classes.
- These divided IP classes are class A, class B, class C, class D, and class E.
- classes A, B, and C are most important. Each address class defines a different number of bits for its network prefix (network address) and host number (host address).

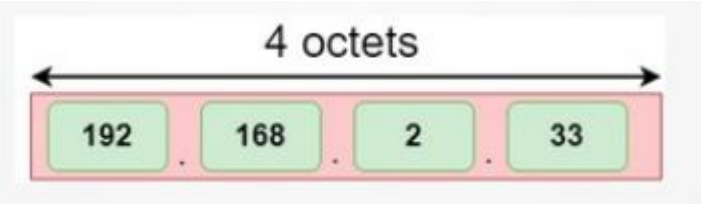

Offsets
0
8
16
24
Class A
0 Network
Host
Address 0.0.0.0 to 127.255.255.255
Class B
10 Network
Host
Address 128.0.0.0 to 191.255.255.255
Class C
110 Network
Host
Address 192.0.0.0 to 223.255.255
Class D
1110 Multicast address
Address 224.0.0.0 to 239.255.255.255
Class E
11110 Reserved for future use
Address 240.0.0.0. to 255.255.255.255

IPv4 (Internet Protocol version 4)

IPv6 (Internet Protocol version 6)

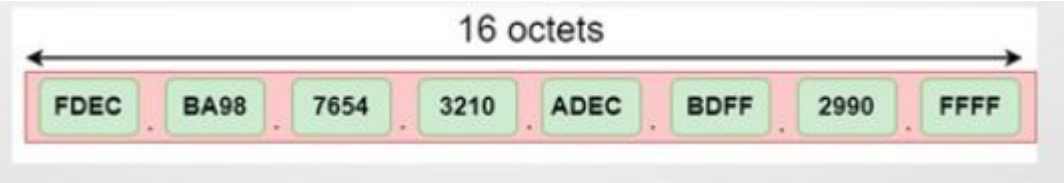
What is IPv4?

IPv4 is 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 a dot (.), i.e., periods. This address is unique for each device



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.



Introduction to CIDR

- CIDR (Classless Inter-Domain Routing or supernetting) is a method of assigning IP addresses that improves the efficiency of address distribution and replaces the previous system based on Class A, Class B and Class C networks.
- CIDR IP addresses consist of two groups of numbers, which are also referred to as groups of bits.
- The most important of these groups is the network address, and it is used to identify a network or a sub-network (subnet).
- In contrast to classful routing, which categorizes addresses into one of three blocks, CIDR allows for blocks of IP addresses to be allocated to internet service providers.

Domain Name System

The Domain Name System (DNS) is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks.

It associates various information with domain names assigned to each of the associated entities.

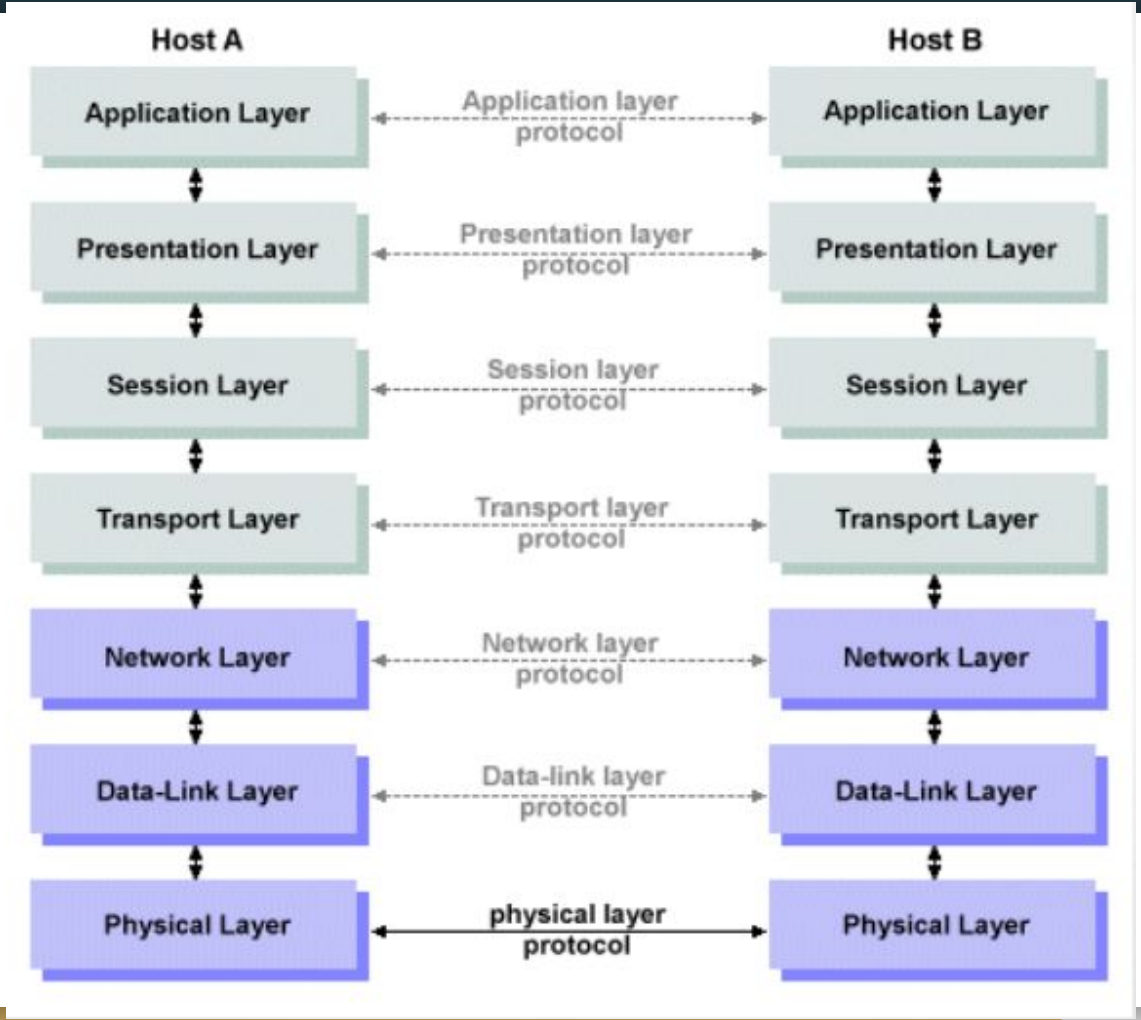
DNS is a core internet technology that translates human-friendly domain names into machine-usable IP addresses.

Example : 128.66.111.102 – Exam Moodle

The DNS operates as a distributed database, where different types of DNS servers are responsible for different parts of the DNS name space.

OSI Model

- The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.
- OSI model has seven layers.and each layer performs a particular network function.
- The layers may be listed in a top-to-bottom or bottom to top order.
- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.


Host A
Host B
Application Layer
Application layer protocol
Application Layer
Presentation Layer
Presentation layer protocol
Presentation Layer
Session Layer
Session layer protocol
Session Layer
Transport Layer
Transport layer protocol
Transport Layer
Network Layer
Network layer protocol
Network Layer
Data-Link Layer
Data-link layer protocol
Data-Link Layer
Physical Layer
physical layer protocol
Physical Layer

1) Physical Layer :

Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

2) Data Link Layer

Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames

Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.

Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

3) Network Layer

Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer.

4) Transport Layer

Segmentation : This layer accepts the message from the (session) layer, and breaks the message into smaller units.The transport layer at the destination station reassembles the message.

Service Point Addressing : In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address.

5) Session Layer

Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.

Synchronization: This layer allows a process to add checkpoints which are considered synchronization points into the data.

These synchronization points help to identify the error so that the data is re- synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

6) Presentation Layer

Encryption/ Decryption: Data encryption translates the data into another form or code.

Compression: Reduces the number of bits that need to be transmitted on the network.

7) Application Layer

Application Layer is also called Desktop Layer.

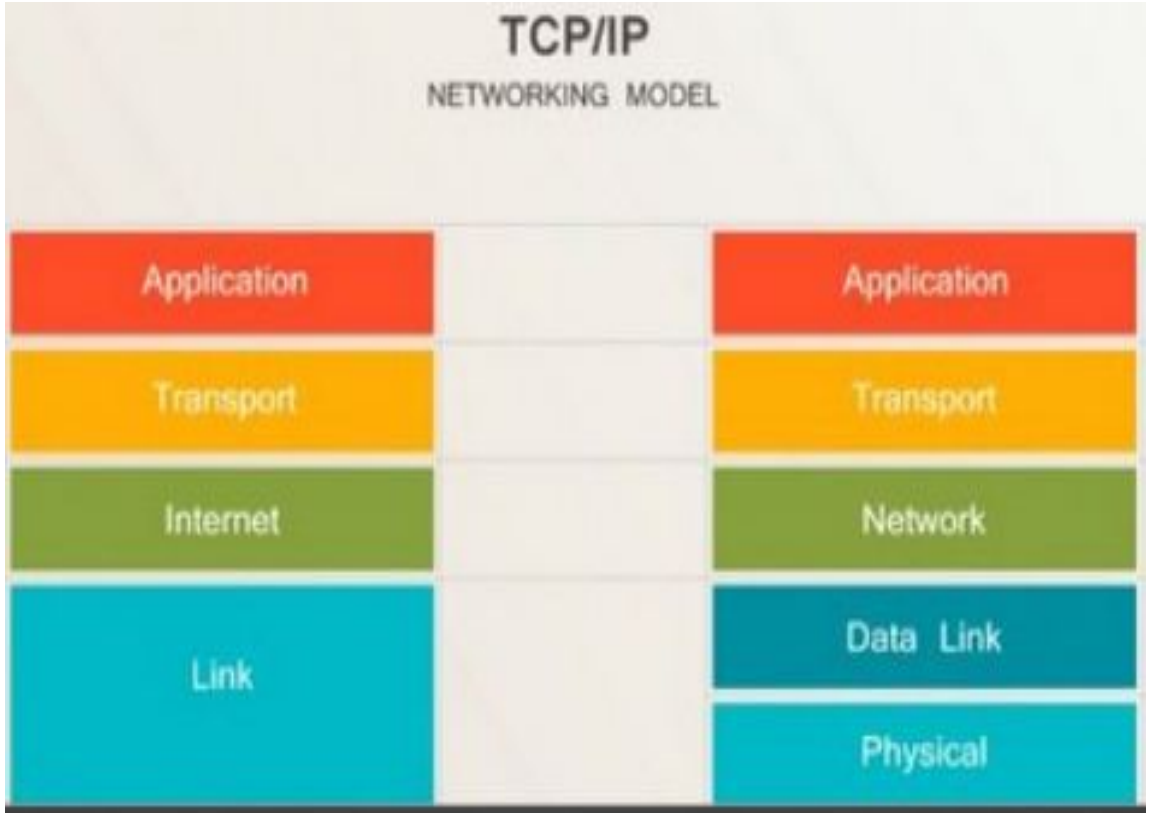
These applications produce the data, which has to be transferred over the network.

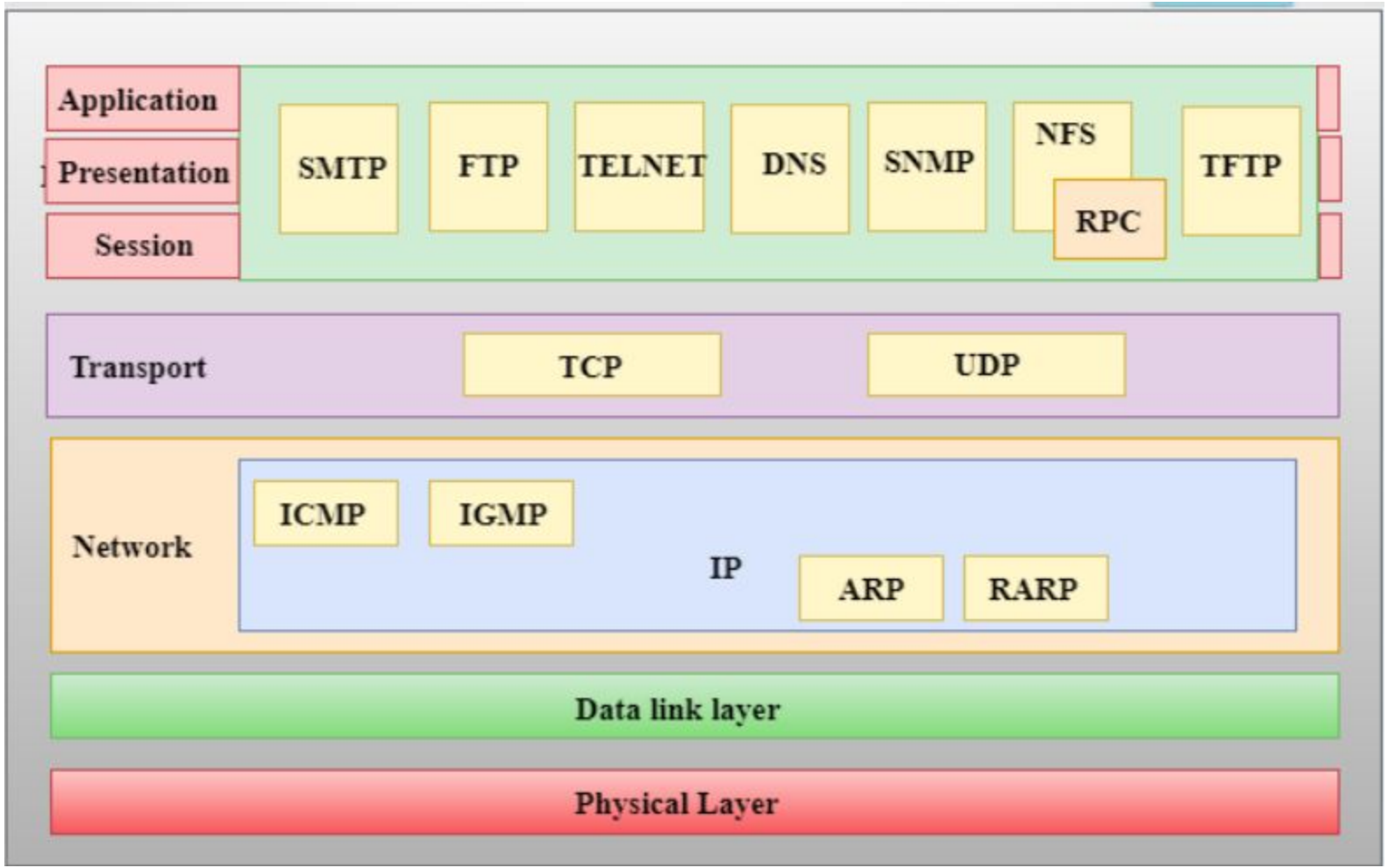
This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

TCP/IP

- Designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.
- Transmission Control Protocol/Internet Protocol.
- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, link layer(data link layer and physical layer).


TCP/IP
NETWORKING MODEL
Application
Transport
Internet
Link
Application
Transport
Network
Data Link
Physical


Application
Presentation
Session
SMTP
FTP
TELNET
DNS
SNMP
NFS
RPC
TFTP
Transport
TCP
UDP
Network
ICMP
IGMP
IP
ARP
RARP
Data link layer
Physical Layer

Application Layer

Application Layer protocol:-

1. TELNET:

Telnet stands for the TELecommunications NETwork.

It helps in terminal emulation.

It allows Telnet client to access the resources of the Telnet server.

It is used for managing the files on the internet.

It is used for initial set up of devices like switches.

The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system.

Port number of telnet is 23.

Application Layer

Application Layer protocol:-

2. SMTP

It stands for Simple Mail Transfer Protocol.

It is a part of the TCP/IP protocol.

Using a process called “store and forward,” SMTP moves your email on and across networks.

It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

Port number for SMTP is 25.

Application Layer

Application Layer protocol:-

3. FTP

FTP stands for file transfer protocol.It is the protocol that actually lets us transfer files.

It can facilitate this between any two machines using it.But FTP is not just a protocol but it is also a program.

FTP promotes sharing of files via remote computers with reliable and efficient data transfer.

Port number for FTP is 20 for data and 21 for control.

Application Layer

Application Layer protocol:-

4. HTTP

HTTP is a protocol used mainly to access data on the www.

The Hypertext Transfer Protocol (HTTP) the Web's main application-layer protocol although current browsers can access other types of servers

A respository of information spread all over the world and linked together.

The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.

HTTP utilizes TCP connections to send client requests and server replies.

it is a synchronous protocol which works by making both persistent and non persistent connections.

Application Layer

Application Layer protocol:-

5. TFTP

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it’s the protocol of choice if you know exactly what you want and where to find it.

It’s a technology for transferring files between network devices and is a simplified version of FTP

Application Layer

Application Layer protocol:-

6. IP-RTP

The Real-time Transport Protocol is a network protocol for delivering audio and video over IP networks.

RTP is used in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications including WebRTC, television services and web-based push-to-talk features.

Transport Layer

Layer 3 or the Network layer uses IP or Internet Protocol which being a connectionless protocol treats every packet individually and separately leading to lack of reliability during a transmission.

For example, when data is sent from one host to another, each packet may take a different path even if it belongs to the same session.

This means the packets may/may not arrive in the right order.Therefore, IP relies on the higher layer protocols to provide reliability.

Transport Layer Protocols :

1) TCP (Transmission Control Protocol):

TCP is a layer 4 protocol which provides acknowledgement of the received packets and is also reliable as it resends the lost packets.

It is better than UDP but due to these features it has an additional overhead. It is used by application protocols like HTTP and FTP.

2) UDP (User Datagram Protocol):

UDP is also a layer 4 protocol but unlike TCP it doesn’t provide acknowledgement of the sent packets.

Therefore, it isn’t reliable and depends on the higher layer protocols for the same.

But on the other hand it is simple, scalable and comes with lesser overhead as compared to TCP.

It is used in video and voice streaming.

Network / Internet layer

Network/Internet Layer:

The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

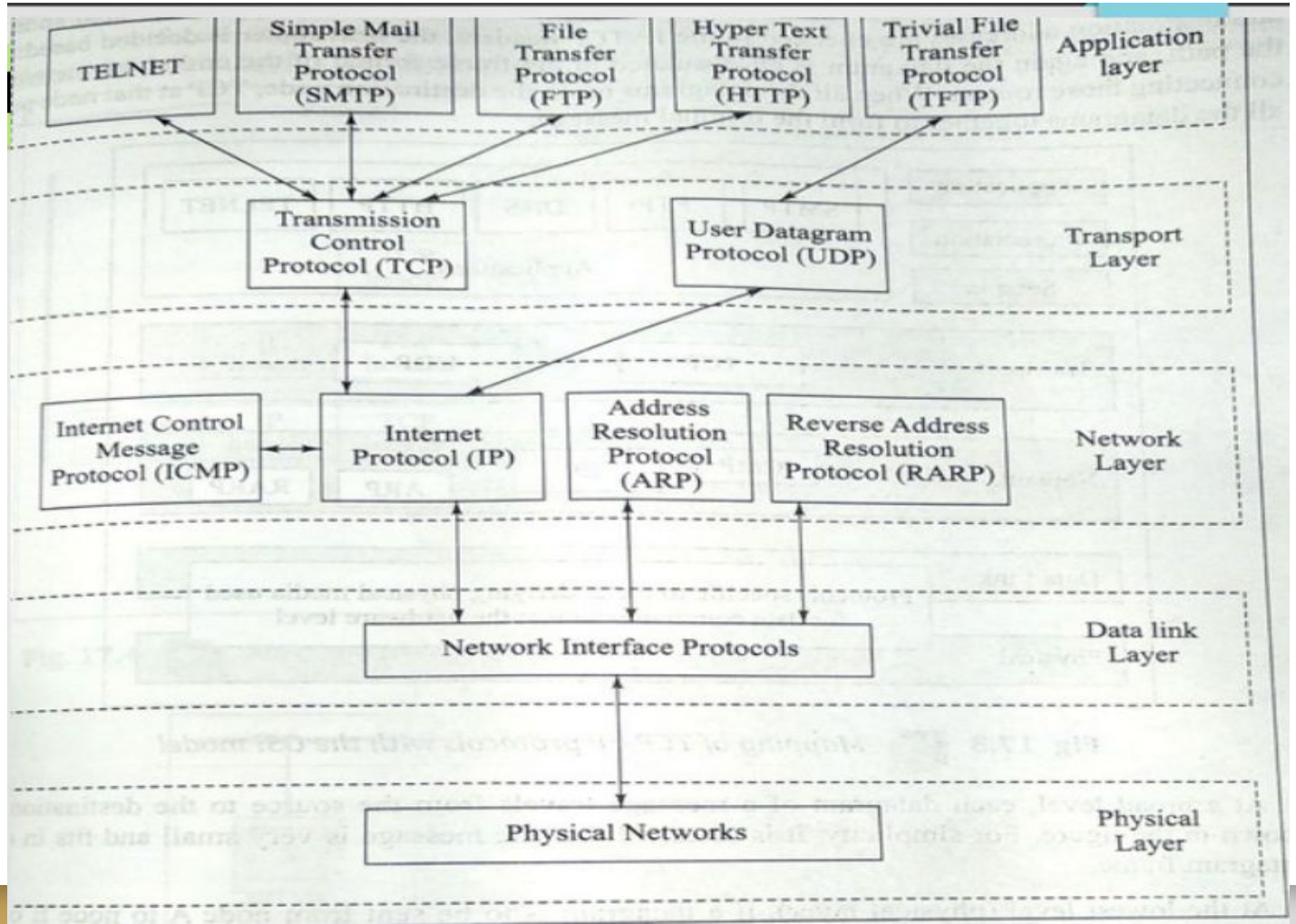
This layer is concerned with the format of datagrams as defined in the Internet Protocol(IP).

This layer is responsible for actual routing of datagrams.

The IP portion of the TCP/IP suite deals with this layer.

It routes and forward a datagrams to the next node but it is not responsible for the accurate and timely delivery of all the datagrams to the destination in a proper sequence.

Some other protocols in this layer ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol) and ICMP(Internet Control Message Protocol).


TELNET
Simple Mail Transfer Protocol (SMTP)
File Transfer Protocol (FTP)
Hyper Text Transfer Protocol (HTTP)
Trivial File Transfer Protocol (TFTP)
Application layer
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
Transport Layer
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
Network Layer
Network Interface Protocols
Data link Layer
Physical Networks
Physical Layer

Network Layer Protocol :

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.

It is an unreliable and connectionless protocol-a best-effort delivery service.

IP transports data in packets called datagrams.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address

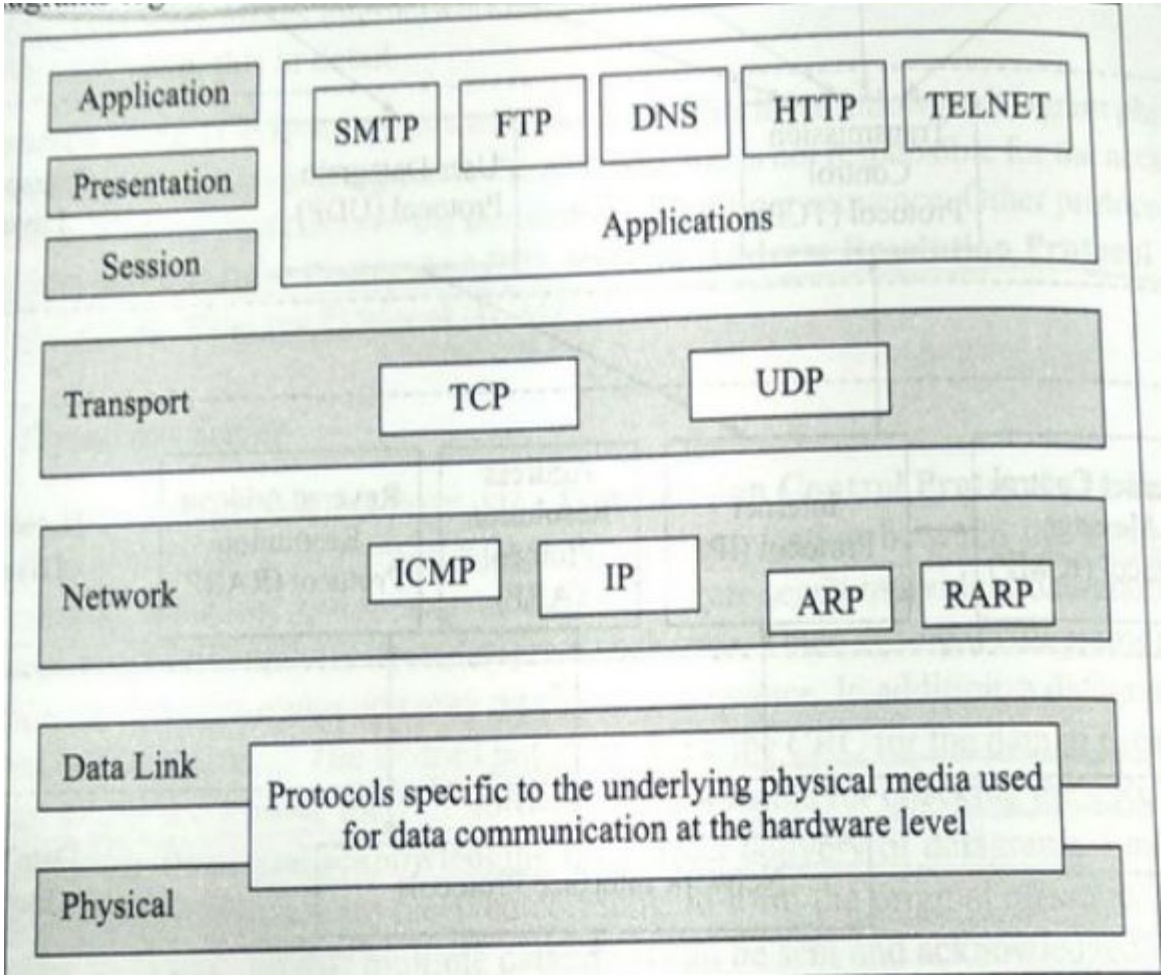
Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address

Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

ICMP sends query and error reporting messages.


Application
Presentation
Session
SMTP
FTP
DNS
HTTP
TELNET
Applications
Transport
TCP
UDP
Network
ICMP
IP
ARP
RARP
Data Link
Protocols specific to the underlying physical media used for data communication at the hardware level
Physical

Link Layer

Link Layer:(Physical layer/ Datalink layer)

A network layer is the lowest layer of the TCP/IP model.

A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

It defines how the data should be sent physically through the network.

This layer is mainly responsible for the transmission of the data between two devices on the same network.

It covers MAC(Media Access Control) i.e. who can send data and when, etc.

The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

IEEE Standards(Overview)

IEEE Standards Association (IEEE SA) is a global organization that develops standards for products and services in many industries. These standards are used to ensure that products work as intended and are safe for users and the environment.

The IEEE standards in computer networks ensure communication between various devices; it also helps to make sure that the network service, i.e., the Internet and its related technologies, must follow a set of guidelines and practices so that all the networking devices can communicate and work smoothly.

Why IEEE 802 standards are important?

There are numerous computer equipment manufacturers in the world, and they manufacture network hardware that would connect to certain computers only. Now, this is a major problem since it would be very difficult to connect various systems having different hardware.

So, the IEEE standards for computer networks developed IEEE 802 standards which ensure that various devices having different network hardware can easily connect over the network and exchange data. The IEEE 802 standards also make sure that the network connectivity and management are easier.

802.1

The IEEE 802.1 deals with the standards of LAN and MAN. Along with that, it also deals with the MAC (Media Access Control) bridging.

802.3

IEEE 802.3 is a set of standards that define the physical and data link layers of Ethernet networks. It's also known as the Ethernet standard. Defines the physical media and working characteristics of Ethernet

- Defines the media access control (MAC) for Ethernet networks
- Supports the IEEE 802.1 network architecture
- Defines a LAN access method using carrier-sense multiple access with collision detection (CSMA/CD)

802.11

IEEE 802.11 is a set of standards for wireless local area networks (WLANs) that define how devices communicate over Wi-Fi. It is developed by the Institute of Electrical and Electronics Engineers (IEEE).

- Defines the physical layer (PHY) and media access control (MAC) protocols for WLANs
- Allows devices like laptops, smartphones, and printers to communicate with each other and access the internet
- Enables the use of WLANs instead of wired networks

802.15

IEEE 802.15 is a working group of the Institute of Electrical and Electronics Engineers (IEEE) that develops standards for wireless specialty networks (WSN). WSNs include wireless personal area networks (WPANs), Bluetooth, and Internet of Things (IoT) networks.

- Develops standards for wireless networking
- Creates recommended practices and guides for interoperability with other wireless and wired networks
- Publishes standards for WSNs used in IoT, wearables, and autonomous vehicles

CSMA/CD

Carrier Sense Multiple Access with Collision Detection Multiple host can access the Ethernet bus at a time through their transceiver and determine for the absence/presence of a carrier wave on the bus.

If a host wants to send the data , first check the cable is ideal or not -sensing It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.

The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.

CSMA/CD- Binary Exponential Policy

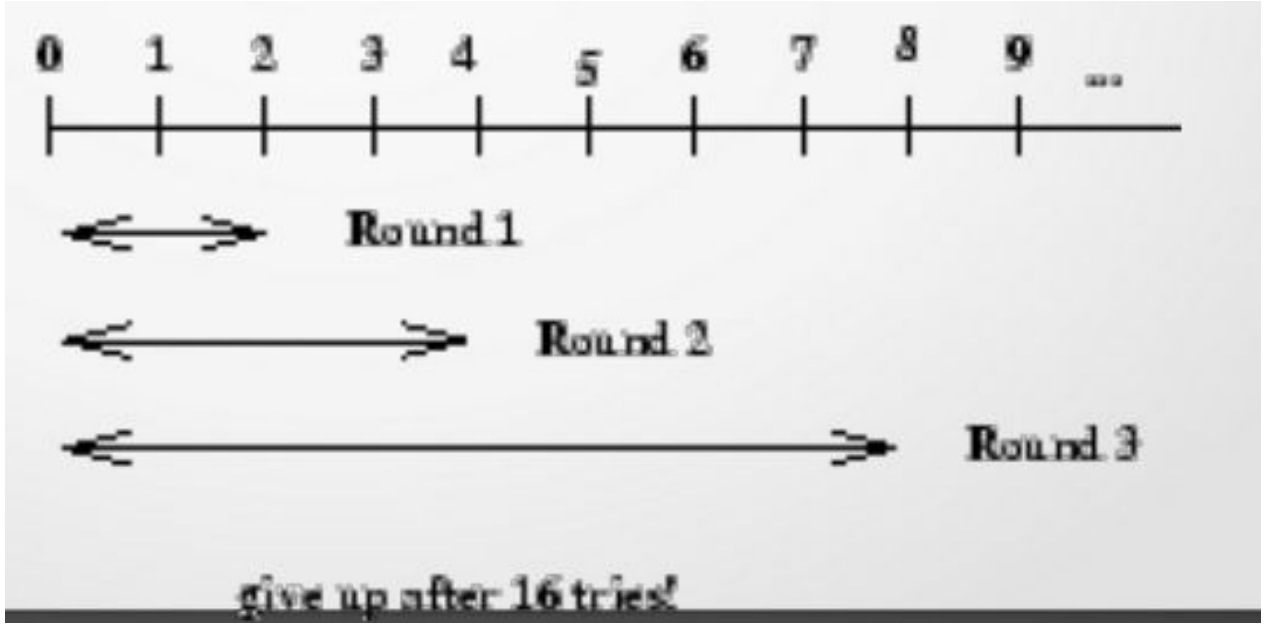
The Ethernet standard specifies a binary exponential back-off policy, where in a sender waits for a random time after a first collision, twice a long if retransmission also results into collision, four times as long if the retransmission also results in a collision and so on.

Wi-Fi as an example. Two Wi-Fi stations A and B want to send data to C at the same time. When two stations access the channel at the same time, we say that it's a collision. Stations whose packets have just collided will initiate a backoff procedure. Every station maintains a number called Contention Window (CW). The station will choose a random value within this window. This value, which is really the number of idle transmission slots that the station has to wait, is called the Backoff Period. During this period, these stations (A and B) cannot transmit.

CSMA/CD- Binary Exponential Policy

The essence of BEB is that the backoff period is randomly selected within the CW. Each station will potentially have a different waiting time. They can't transmit until the backoff period has passed. Moreover, when another station gains access, backoff timer is paused. It's resumed only when the channel becomes idle again as determined by Distributed Interframe Space (DIFS).

With every collision, the station will double its CW. This is why the prefix "binary exponential" is used. It's common to have minimum and maximum values for CW.


0 1 2 3 4 5 6 7 8 9 ...
Round 1
Round 2
Round 3
give up after 16 tries!

Thank You.