1 Computer Network Basics

1.1 INTRODUCTION

Fig.1.1 Data Communication System

"Hello world", which is data here, needs to be transmitted from the Sender to Receiver, this transmission of data involves some set of protocols (will be discussed in the next chapters) and this flow of data in a system is called "Data Communication System".

Components of data communication system:
Sender:
One who sends data

Data:
It is a huge subject in itself, but we limit it to the context/information which needs to be transmitted from sender to receiver (in the above diagram **"Hello World"** is a data).

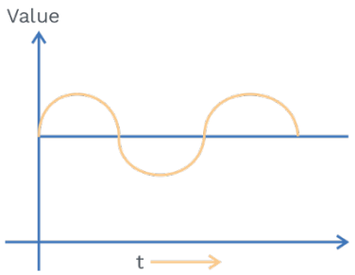
Medium:
Data passes through a medium which can be wireless or wired (Twisted pair, Coaxial cable or Optical fiber etc.)

Receiver:
One who receives data.

Protocol:
Set of rules that governs transmission of data.

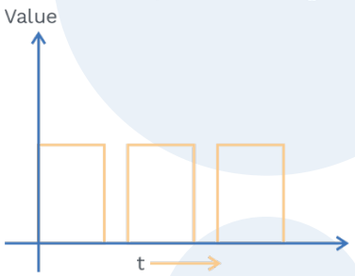
Lets understand Data and Medium a bit more:
1) Data:
For transmission of data, it must be transformed into electromagnetic signals.

Signal can be classified in analog and digital form.



Analog signal:
Data is represented in continuous waveforms.

Digital signal:
Data is represented in discrete form (0's or 1's/High or low).



Note:

Signals always varies with respect to time or frequency.

$$(\text{time} = \frac{1}{\text{frequency}}).$$

Baseband signal: Typically uses digital signals.
Broadband signal: Typically uses analog signals.

2) Medium:
Transmission medium is a channel through which data can be sent or received.

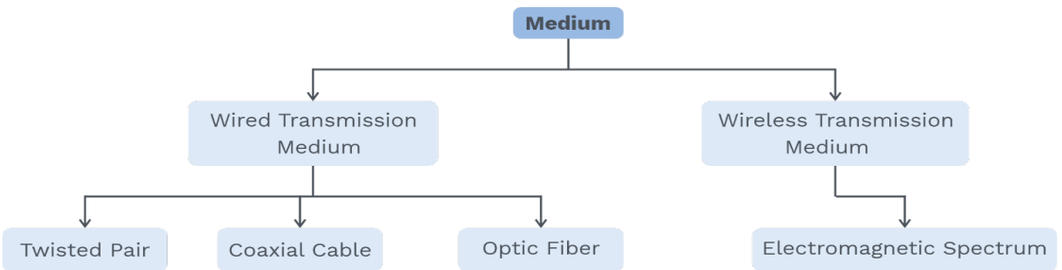


Fig. 1.2 Flow Chart Representing Types of Transmission Medium

Twisted pair:

Do you know the RJ - 45 connector?

Yes, the port on your laptop or CPU for RJ-45, it contains twisted-pair cables for Ethernet connection. It is also known as CAT 5 cables.

Fig. 1.3 Diagram of Twisted Pair

- In twisted-pair cables, two wires twisted together in a helix fashion.
- It has low cost transmission.
- It can carry both analog and digital signals.
- More the thickness of wire, more is the bandwidth.

Why twisted wires, why not normal wires !!

Normal wires will generate the magnetic field, which interferes with the signal, when the wires gets twisted, the magnetic field around the wires get disrupted.

Rack Your Brain

Where twisted wires are used !!

Coaxial cable:

It has a copper wire as a core, surrounded by insulating materials, which further surrounded by the braided outer conductor, which is further surrounded by a plastic sheath.

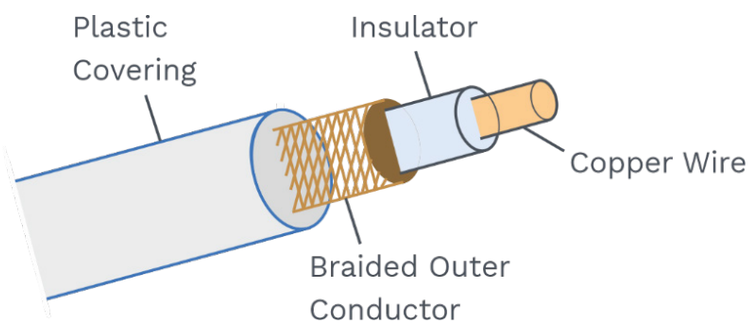


Fig. 1.4 Structure of Coaxial Cable

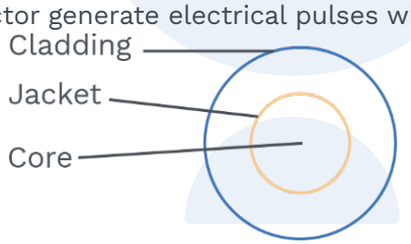
- It has better features than twisted pair because of its shielding.
- It has excellent noise immunity and high bandwidth.
- Here also, more the length of the cable, more the bandwidth.

Rack Your Brain

Why coaxial cables are used !!

Fiber Optics:

- It sends information using lights instead of electrons. Light travels from the core, a layer which surrounds the core is called cladding.
- Fiber optics consist of the light source, transmission medium and detector.
- Light pulse indicates 1 and absence of pulse indicates 0, the medium is thin, fiberglass and detector generate electrical pulses when light falls on it.



- Error rates are less because it does not affect by electromagnetic interference.
- It is thin and lightweight.
- Data rates are very high.
- They are good for security reasons because they are difficult to tap.

How many types of fibre exist !!

2 types are there – Single-mode fibre and multimode fibre.

In single-mode: Light travels in Single Path,
high cost,
can be used in 10 to 100 Km,
data rates are high (in Tb/s),

In multimode: Light travels in many paths,
low cost,
can be used in 2000 metres,
data rates are low (in Gb/s).

Rack Your Brain

If you have to run a network which ranges from 1400 metres and have a data rate as 1 Gb/s? Which fibre should you choose !!

Till now we have seen wired medium, now let us see wireless transmission medium:

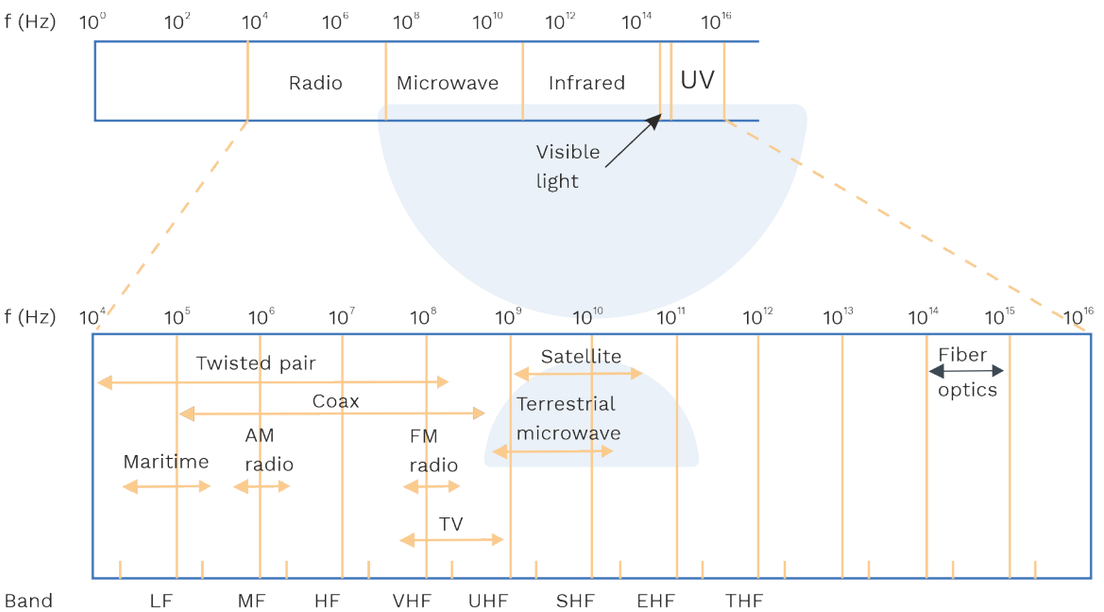


Fig. 1.5 EM Spectrum and Uses in Communication

Waves which can be used for transmitting information are radio, micro, infrared and some portion of visible light as they can be modulated and amplified easily. UV, X and gamma rays do not propagate through the buildings; hence not used for transmission frequently.

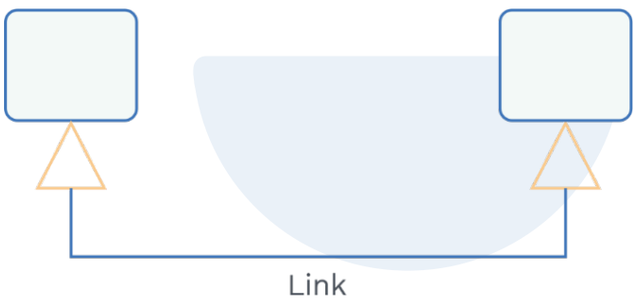
Note:

Data flow can be categorized in simplex mode, half duplex mode and full duplex mode.

Simplex mode: Only one of the two devices can send the data, hence the entire channel is used for transmission, example: radio station.

Half-Duplex mode: Any of the two devices can send or receive the data but not at the same time; here entire channel is used for transmission or receiving of data, example: Walkie Talkies.
Full-Duplex mode: Both devices can send and receive data simultaneously, hence the entire is used for two purposes simultaneously which increases the efficiency of the channel, for example: Telephone networks.

Topologies and its types:
Link:
Device connected through link



Topology:
Many links from topology, basically it is a representation of the physical and logical structure.

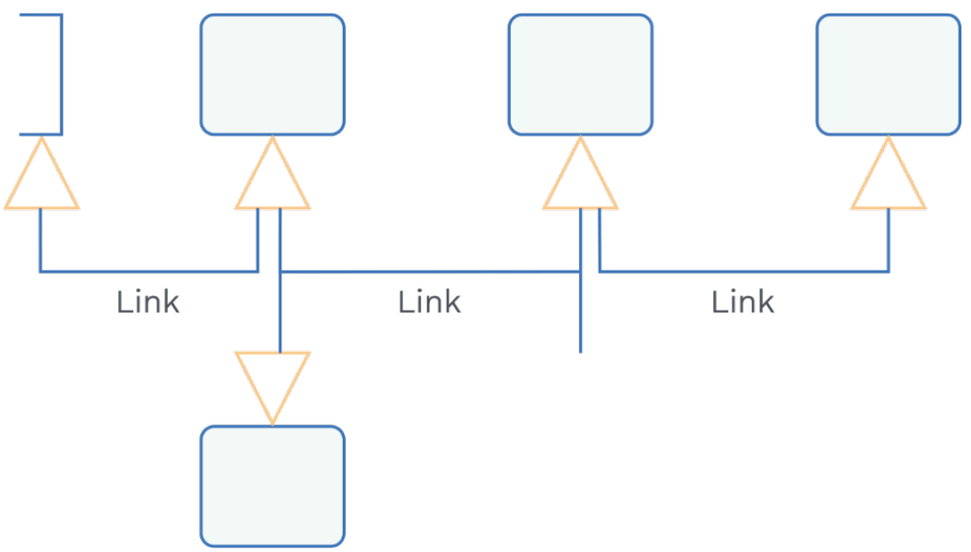


Fig. 1.6 Structure of Topology

Topology types:

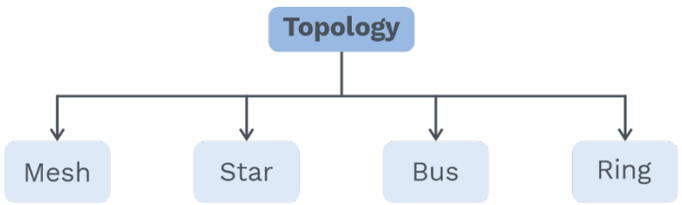


Fig. 1.7 Types of Network Topology

Bus topology:

- All the nodes are connected to a shared cable.
- There will be no central node.
- One long cable act as a back-bone of this network.
- For n devices, only 1 link is required.

Advantage:

- Installation is easy, used for small networks, fewer cables are required.

Disadvantage:

- Can be used with limited nodes; cable length is also limited.

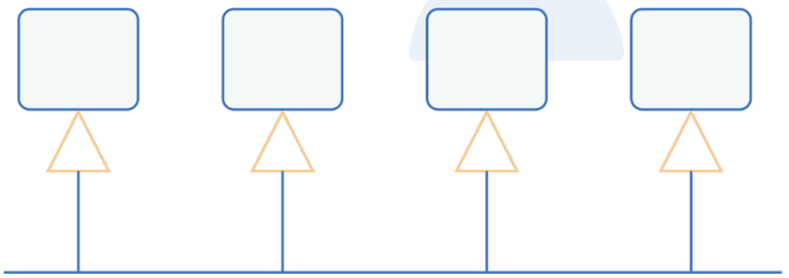


Fig. 1.8 A Bus Topology

Star topology:

- Each device has a point to point link through a central node (hub or switch) that may act as controller.
- There is a central node which acts as an exchange medium.
- Devices are not directly connected with each other.
- For n devices, n links are required.

Advantage:

- Easy to manage when faults occurs, installation is easy, easy to expand.

Disadvantage:

- Require more cable than the bus, if the central node gets down, then all nodes get down.

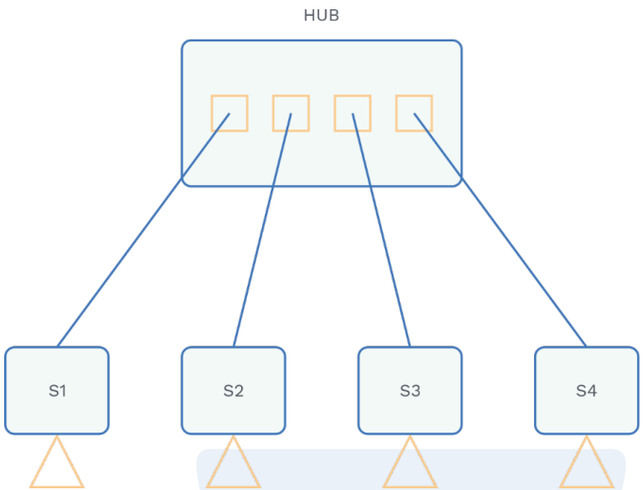


Fig. 1.9 A Star Topology

Ring Topology:

- Each device has a point to point connection only with two devices that are on either side of a device.
- If any device fails, the entire network gets down.
- Each device in a ring has a repeater.
- Message travel in a single direction.
- If n nodes are present, then n physical links.

Advantages:

- Using token, each device gets a fair chance to send a message.
- Easy to install, good for long-distance.

Disadvantage:

- If nodes get moved, it affects the performance.
- If a node gets down, entire network gets down.

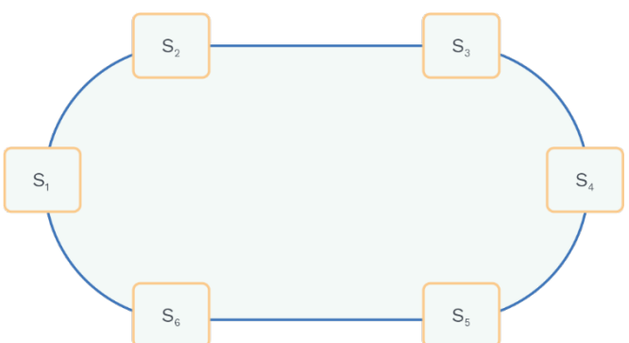


Fig. 1.10 A Ring Topology

Mesh Topology:

- Every device has a point to point link with every other device.
- Message can travel in any direction.
- If n devices are present, then (n – 1) ports must be present on each device.
- And total number of physical links is n(n–1)/2.

Advantage:

- If one node gets down, still message can flow through other paths.
- Fault detection is easy because of the dedicated link.

Disadvantage:

- Installation is not easy.
- Expensive as more number of cables is used.
- There is a possibility of a redundant path.

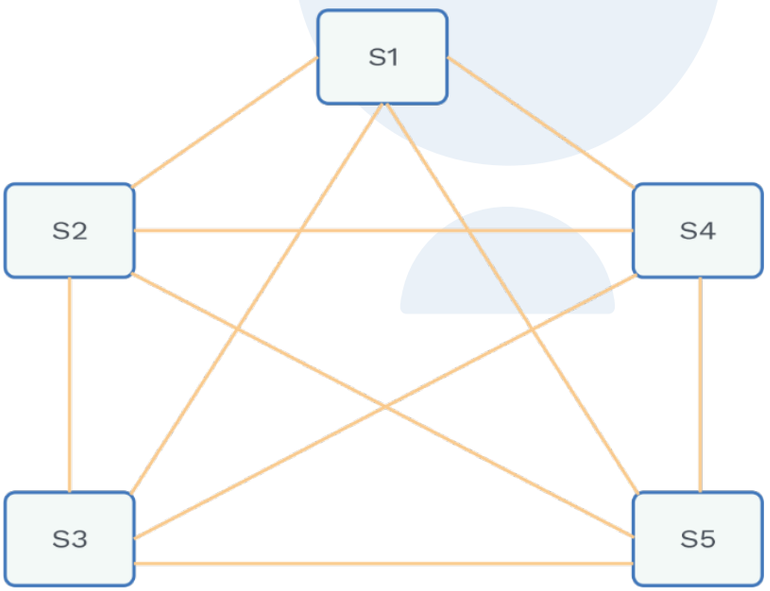


Fig. 1.11 A Mesh Topology

Rack Your Brain

a) In a mesh system, if the number of devices are 10, how many physical links must be present?

b) In a ring system, if the number of devices are 5, how many physical links must be there?

Tree Topology:

- Collection of star topology in hierarchical level.
- More devices can be added now as the network can grow by connecting one central hub to another hub.

Advantage:

- Easy to expand, Isolation of different network is possible.

Disadvantage:

- If the central hub is down, the entire network goes down.
- Cost is high because more number of cables will be required.

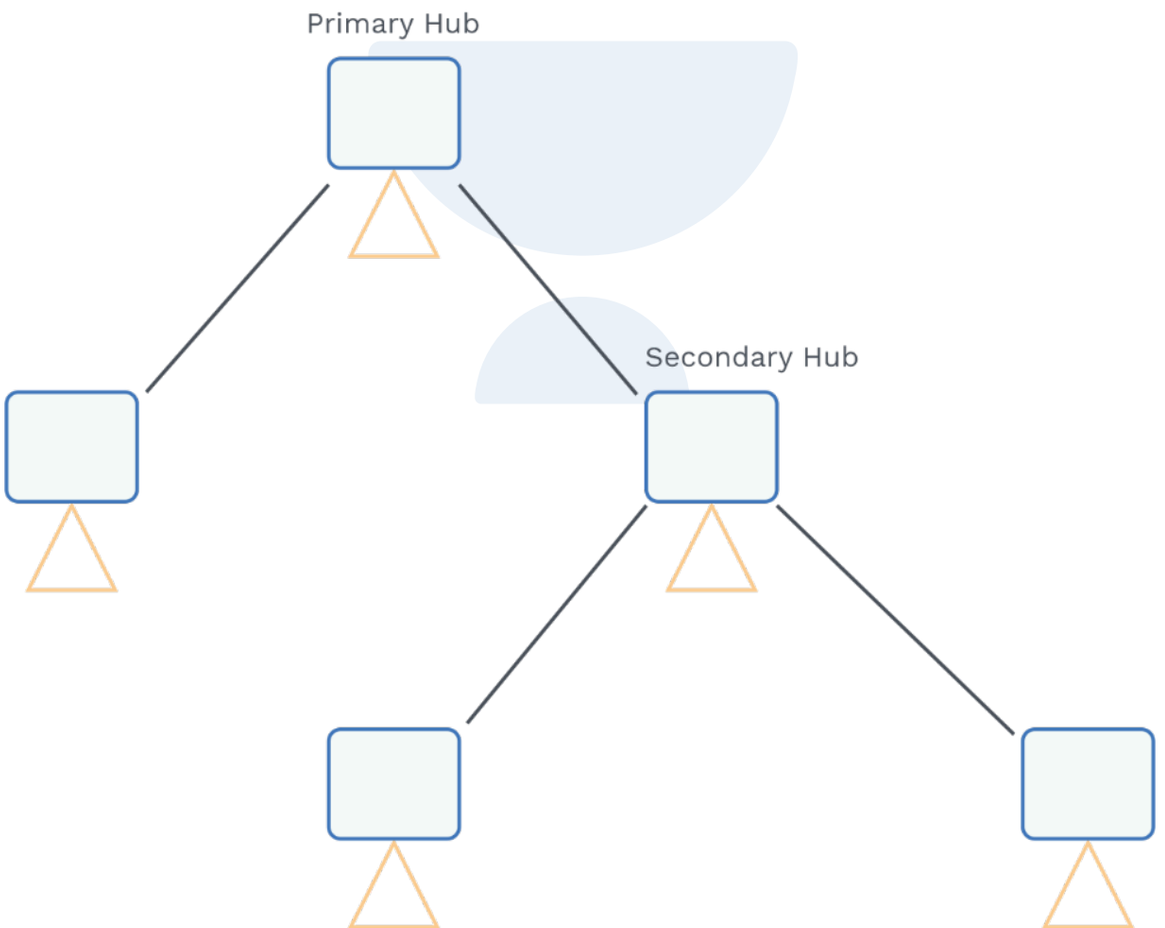


Fig. 1.12 A Tree Topology

1.2 NETWORK TYPES

Interprocessor distance	Processors located in same	Example
1m	Square meter	Personal area network
10 m	Room	Local Area Network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Fig. 1.13 Classification of Network

PAN (Personal Area Network):
- Range of Person, your bluetooth works in PAN.
- Works for short range.

LAN (Local Area Network):
- Range of buildings, privately owned networks.
- Wireless LAN such as WiFi.
- Wired LAN such as Ethernet.

MAN (Metropolitan Area Network):
- Ranges of cities, your cable television networks.
- Connection of Multiple LAN's.

WAN (Wide Area Network):
- Ranges of countries, your telephone network works in WAN.
- Works for a very large range.

OSI Model:

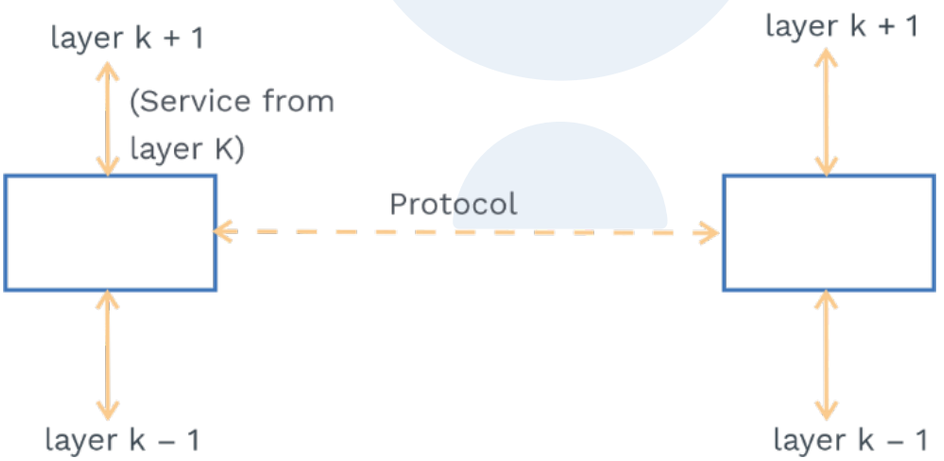
- International Organization of Standardization (ISO): proposed an open systems interconnection (OSI) model, which allows two systems to communicate irrespective of their architecture.
- The aim of the OSI model: To represent how to provide communication between the dissimilar systems without making any changes to the logic of the underlying software and hardware.
- OSI model is a 7 layered architecture.

Protocol Layering:

A list of protocols used by the system in which one protocol is used in each layer is called protocol layering or protocol stack.

Relationship between Service and Protocol:

Service and protocol both are different; one can understand service is a high-level function and protocol is a detail of a function.



Each layer's boundaries are decided in such a way that there should be a minimum flow of information between each layer.

Note:

OSI model has been widely used but the protocols "used in OSI" have been forgotten.

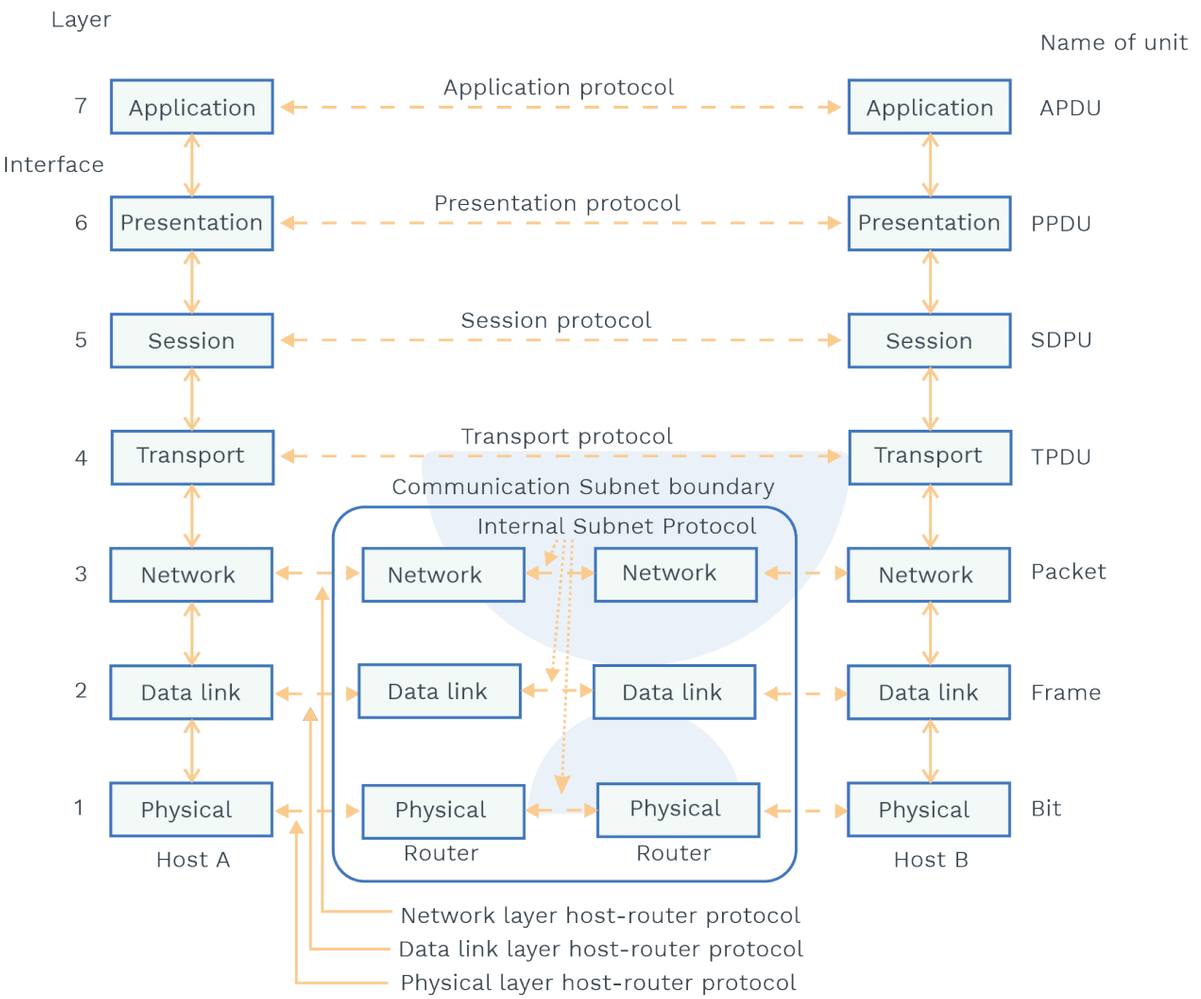
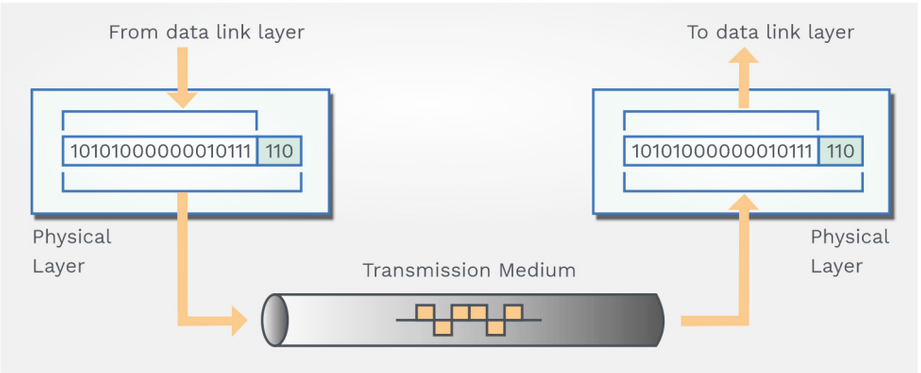


Fig. 1.14 The OSI Model

Before discussing each layer we must keep in mind that portion of the packet at stage x-1 contains the whole packet of stage x. Stage x – 1 thinks that the packet which is coming from stage x is one unit. One can say it follows the encapsulation technique.

Physical layer:

- It deals with the interface between the devices and the transmission medium.



- It deals with the transmission of raw bit through transmitting media the Sender and Receiver must send or receive bit at the same rate and must be synchronized.
- It also deals with physical topology and transmission modes.

Rack Your Brain

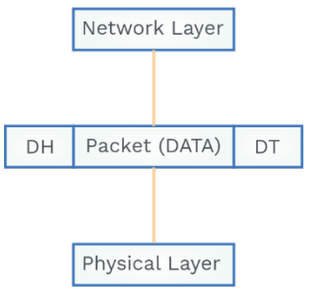
a) Name some physical topology.
b) Name some transmission mode.

Data Link Layer:
It makes a frame move from one node to the next node.

- It makes data from the physical layer error-free and sends to the network layer.
- It deals with **framing** (the process of division of data unit from network layer into manageable streams called frames).
- It deals with **physical addressing** (adding a physical address **i.e. MAC address,** so that frame could reach the destination network)
- If rates are mismatched between nodes, then the data link layer provides a flow control mechanism.
- Data link layer also see whom to give access if two or more device is connected to a link at a given time.

Rack Your Brain

Above 5 points are Error Control, Framing, Physical Addressing, Flow Control and Access Control, respectively.



Network layer:
It deals with the delivery of packets from source host to destination host.

- **Logical addressing:** Data link layer solves address issues locally, but the network layer provides a logical address (IP address) in order to reach from Source to destination when the packet reaches the destination network.
- **Network layer do routing**: Several networks is interconnected with each other through the router, and it is the responsibility of the network layer to route the packet to the destination.

Transport layer:
It is the responsibility of the transport layer to deliver the message from the source process to the destination process.

- It does **segmentation** (splitting message from application layer into segments) and **reassembly** (intact the message correctly on receiving the destination).
- It deals with port addresses in order to reach the service of the process called **port addressing.**
- Transport layer also determines service provided to the session layer, it may be connection-oriented or connectionless services.
- **Flow control:** At transport layer, flow control is done from end to end.
- **Error correction:** It is usually done by retransmission if any error occurs.

Rack Your Brain

a) You have seen how transport layers perform error control, think about how data links perform error control.
b) At the transport layer if flow control is end to end, at the data link layer, it is?

Session layer:
It is the responsibility of a session layer to establish a session (dialog control and synchronization) between sender and the receiver.

- **Dialog control:** Between a link, it keeps an eye whose turn is now on the link for sending the data.
- **Synchronization:** It adds a checkpoint if the sender is sending a huge file, **eg:** Sending a file of 1GB, it will add a checkpoint after 100KB so that if any file gets lost, it will be easily recovered.

Presentation layer:

It deals with compression, translation and encryption.

- **Translation:** It deals with the conversion of bits before sending a message.
- **Encryption:** it deals with an encoded messages before sending; encryption is done for security reason.
- **Compression:** While sending a multimedia file, it compresses the file for smooth transmission.

Application layer:

- It deals with a variety of protocols which is useful for common clients.
- The protocols are HTTP, FTP, DNS, SMTP. (We will discuss this in application layer chapter.)

TCP/IP Model:

- Protocols which are associated with the OSI model are not used in today's world, although the OSI model is still in use as it works as a framework for other models because of its generalized structure.
- If not OSI protocol, then whose protocols are we using now?
  TCP/IP model
- Below is a diagram of the TCP/IP model, which is similar to the OSI model. Have a look at the difference between the two.

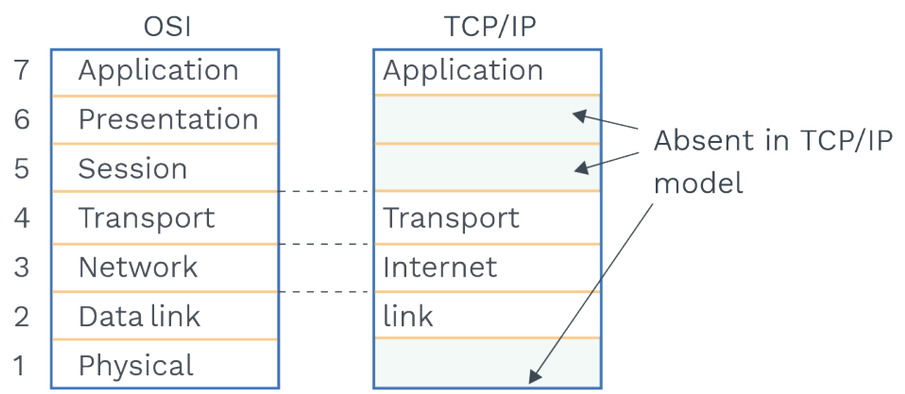


Fig. 1.15 Comparison Between OSI Model and TCP/IP Model

Have you noticed presentation, session and physical layer are absent in TCP/IP?

OSI MODEL	TCP/IP MODEL
This model is popularly used, but protocol associated with this model is now obselete	This model is not used, but protocol associated with this model is used frequently
Both model uses layered architecture Both model process data in the form of packet	

Key similarities between OSI and TCP model:

- For communication process both are using layered architecture and each layer is specific to its task in both models.
- Both models follow the encapsulation, hiding the implementation details at each layer.
- Both follow the stack independent protocol technique.
- Both model has implemented end to end communication upto the transport layer.

Key differences between OSI and TCP model:

- One major difference is between layers OSI model has 7 layers whereas TCP/IP has 4 layers.
- In the OSI model, the transport layer provides connection-oriented services, but the TCP/IP model transport layer can make choices between connection or connectionless services.

  Protocols used in TCP have been shown in the given diagram:

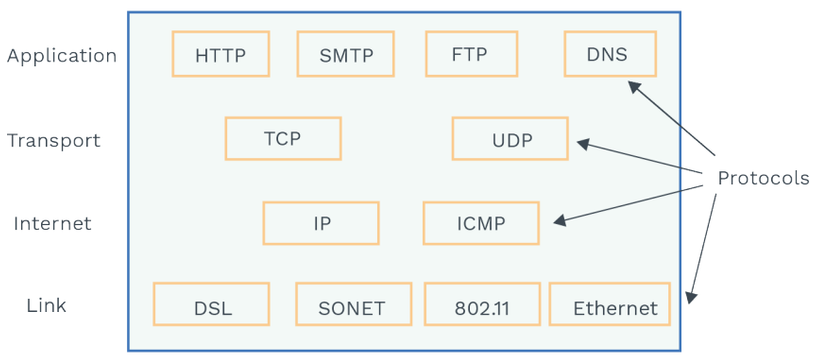
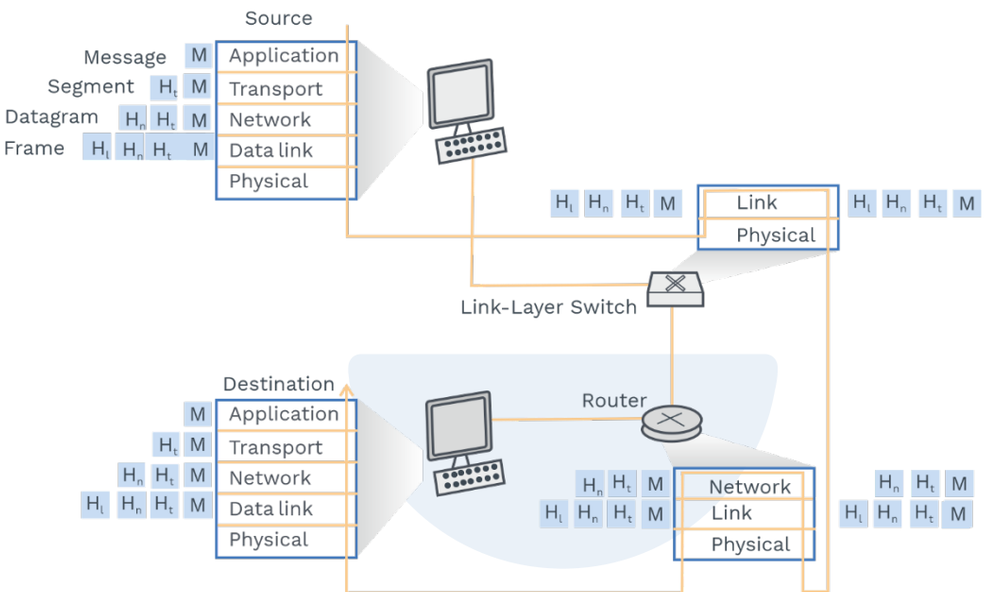


Fig. 1.16 Protocols Used in TCP Model

Let us see How these layer work in short (We will go deep of each layer later but let's have a taste)



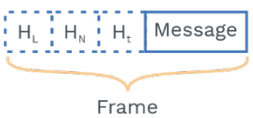
- At Source message starts travelling from the application layer.
- Transport layer receives the message and adds H_t (Transport layer header).
- The transport layer segment then passes to the network layer, and the network layer adds a network layer header to it.

Note

a) You may ask where this header gets acknowledged?
At the received side of the transport layer.

b) Is there any name given to this message at the transport layer?
Yes, we called it as segment.

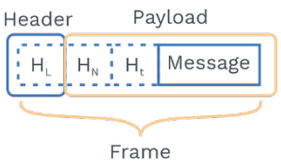
- Network layers send this datagram to the data link layer, which adds a data link layer header. Do you think there is any name at the data link layer also!! Frame



- At every layer, packet is having two fields:
  1) Header field
  2) Payload field

What is a Payload Field?

Payload field at layer k is the packet which is coming from k-1 layer !!
For example, at the data link layer, see the diagram below:

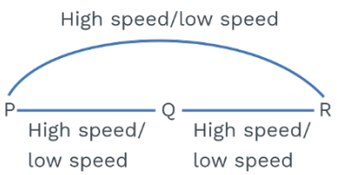


- From the link layer, it goes to the switch or bridges, which sees till the physical address (MAC) of the packet and forwards it to the destination node.
- Let us say the packet is in a different network; now packet has to pass with the router, which can see till the IP address of the packet and map to its destination address.
- Finally, packet reaches its destination host, where each layer by seeing their header and acknowledges the packet.

PRACTICE QUESTIONS

Q1 **3 routers are connected in a network, between each pair of router network, administrators can add 2 lines (high speed line or low line) If it takes 10ms to inspect each topology. How long would it take to inspect all of them?**

Sol:



No. of lines are PQ, QR, PR.
Each line is having 2 choices.
So, total number of topology possible is 2x2x2 = 8
10 ms for each to inspect; hence 0.08 sec. to inspect all.

Q2 **One advantage and one disadvantage of layered architecture?**

Sol: Advantage: Can be managed easily.

Disadvantage: Delays are more compared to single layer architecture.

Q3 **Difference between message streams and Byte streams?**

Sol: In message streams, packets have separate boundaries, but in byte streams, packets is considered as a single unit.

Q4 **Assume at in OSI model algorithms (protocol) used at layer k are changes, what will be the effect at layer K i (i = 1,2,3)?**

Sol: There will be no effect, now can you think why? Because each algorithm is associated with its layer only in OSI model, there will be no effect on other layers.

Q5 **Follow up with the question in d, what if services at layer k has changed, will it affect layer K i (i = 1,2,3)?**

Sol: We might need to modify services at upper layer because each layer is giving services to the upper layer.

Previous Years' Question

Q) In the following pairs of OSI protocol layer/sub–layer and its functionality, the INCORRECT pair is :

a) Network layer – Routing
b) Data link layer – Bit synchronization
c) Medium access control sublayer – Channel sharing
d) Transport layer – end to end sharing

Sol: b)

Physical layer – Bit synchronization

Chapter summary:

- The seven-layer OSI model provides guidelines for the development of universally compatible networking protocols:
- **Network support layers** : Physical, Data Link and Network Layer.
- **User support layers** : Session, Presentation and Application layer.
- **Physical layer** : Delivery of bit streams over physical layer.
- **Data Link layer** : Node to node delivery of data.
- **Network layer** : Source to destination delivery.
- **Transport layer** : Process to process delivery.
- **Application layer** : Enables user to access network.
- TCP/IP is a four- layer hierarchical protocol suite.
- Level of address used in TCP/IP.
- Data link layer uses physical address use in LAN or WAN.
- IP address uses logical address used to identify host.
- Port address identify a process on a host.

For N devices:

- 1 link is required for bus topology.
- N link is required for ring topology.
- N link is required for star topology.
- N(N-1)/2 link is required in mesh topology.
- Twisted air cable, coaxial cable, and optical fiber are the most popular types of guided media.
- Unguided media transport electromagnetic waves without the use of a physical conductor.

2 Physical Layer

2.1 INTRODUCTION

Physical layer:

It deals with electrical, mechanical, and functional characteristics.

Note:

Physical connectivity must be there between one hop to other hop (that connectivity may be wired or wireless).

It is responsible for the transmission of binary data through a medium.

Transmission can be analog (continuous waveform signals) or digital (discrete binary signals).

a) Do you know why a modem is used !!

Convert analog to digital and vice versa.

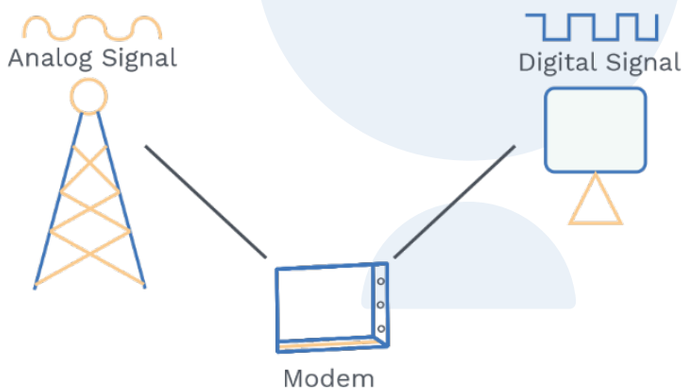


Fig. 2.1 Diagrammatic Representation of Signal Conversion

b) Do you know why multiplexers are used !!

It allows multiple signals to be carried on a single transmission line.

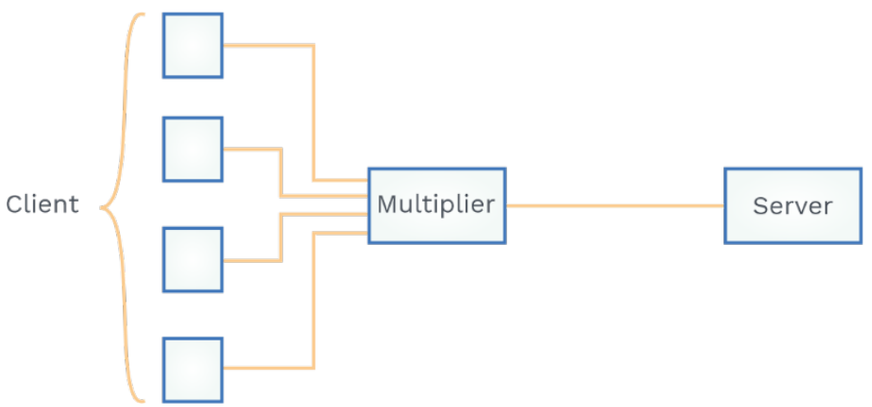


Fig. 2.2 Diagrammatic Representation of Uses of Multiplexer

Baseband transmission:

- Typically it is used in local area network (LAN)
- It uses a digital signal over a single wire.
- In a baseband transmission, the entire bandwidth of the channel is used by digital signals.

Rack Your Brain

a) Is it possible to transmit multiple signals on a single cable !!
b) Baseband signal uses which multiplexing technique !!

Broadband Transmission:

- Typically, it is used in Wide Area Network (WAN).
- It uses analog signals over multiple transmission frequencies.
- In broadband transmission, multiplexing is used using Frequency Division Technique (FDM).

Bandwidth:

- We can say maximum transmission capacity.
- It is a difference between highest and lowest frequencies contained in the composite signal.

$$\text{Bandwidth} = \text{freq}_H - \text{freq}_L$$

You may ask, what are composite signals?
Signals are the composition of many waves it may be periodic or non-periodic.

- Frequency of periodic signals has a discrete value.
- Frequency of non-periodic signals has a continuous value.

Grey Matter Alert!

5kbps vs 5hz, what is the difference !!
Both are bandwidth; these two units are two different measuring values:

5hz : A range of frequencies channel can pass
5kbps : Bandwidth on a link is 5kbps

Basically, any increase in bandwidth in hertz means an increase in bandwidth in bits per sec.

Throughput:
How fast we can send data through a network !!
One may think throughput and bandwidth are the same, but they are different. Let's say preparing 10 subjects per gate cse paper is bandwidth, but babloo is able to finish only 7 subjects in gate cse paper , So the throughput of babloo is 7.

Latency:
It is the delay, how much time it takes to travel a message from source to destination. When the first bit is sent out from the source to the destination.

Latency = Propagation delay + Transmission delay + Queueing delay + Processing delay

Propagation delay: It is the time duration for 1 bit to travel the link
T_p = distance between sender and receiver/velocity of the signal on the link.

Transmission delay: It is the time taken to push the entire packet bits onto the wire.
T_t = Frame size or packet size/Bandwidth

Queuing delay: It is the time taken for a packet to stay in the buffer.

Processing delay: Routers or switches take some time to process the packet header, which is called Processing delay.

Transmission of signal:
How information can be represented in digital signal:
1 $\rightarrow$ Positive voltage
0 $\rightarrow$ Zero voltage
The diagram below has 2 signal levels; it may have 3 or more levels, depending upon the amount of data.

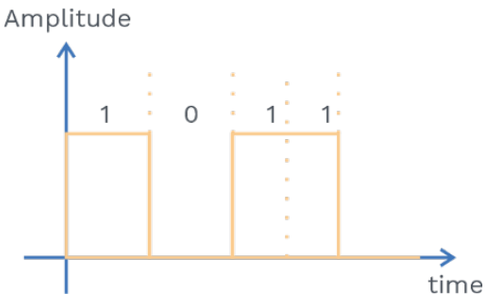


Fig. 2.3 Digital Signal Representation

Please note here for sending information at one bit per level, we need two levels.

Concept Building Exercise

a) For sending information in 2 bits per level, how many levels are needed !!
It is 4, i.e. 2^{bits}

b) What is the bit rate?
Number of bits sends in one sec.

c) What is the baud rate?
It is the number of times signal changes per second.

d) What is channel capacity?
Maximum rate at which data can be communicated.

Encoding/Decoding techniques:

- **Encoding:** Process of converting from one format into another (specified) format.
- **Decoding:** Process of converting from specified format into actual format (It is the reverse of encoding)

Terms used in encoding:

- **Unipolar:** If all the signal elements have the same sign (like all are positive or all are negative), then the signal is unipolar.

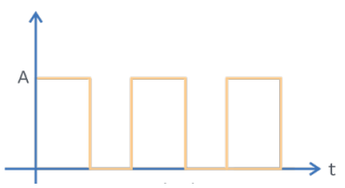


Fig. 2.4 Unipolar Scheme

- **Polar:** If the signal elements have one positive and another negative sign, then the signal is Polar.

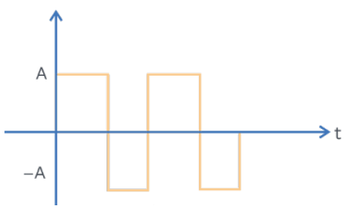


Fig. 2.5 Polar Scheme

- There are different encoding schemes, but we will limit it to Manchester and differential Manchester because it is used in IEEE 802.3.

Manchester encoding scheme:
1 → low to high transition in middle of interval.
0 → high to low transition in middle of interval.

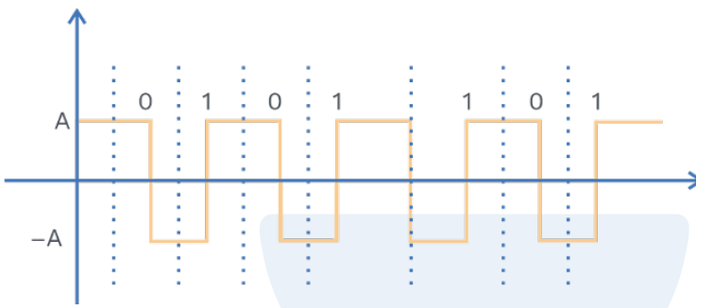


Fig. 2.6 Diagrammatic Representation of Manchester Encoding Scheme

Differential Manchester encoding scheme:
Always inversion at the middle occur,

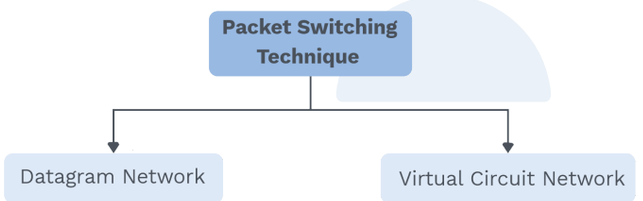
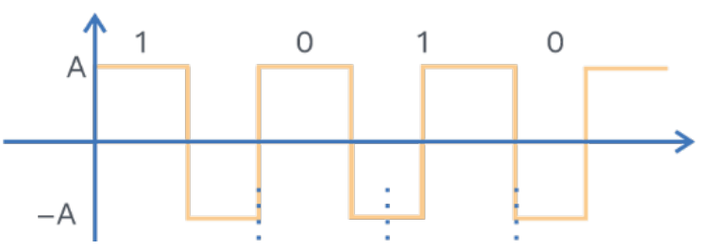


Fig. 2.7 Diagrammatical Representation of Differential Manchester Encoding Scheme



Rack Your Brain

Find the differential Manchester and Manchester encoding of the given code:

10110110

Noise:
When a signal travels, there is a high chance that unwanted signals get attached to the original signal, which creates bad results and is often termed noise. There are several types of noise: Thermal, crosstalk and impulse.

Thermal noise:
It gets created by the random motion of electrons in a wire.

Cross talk:
It is an effect of radiation which is induced on other signals because of close proximity.

Impulse:
It is spike noise which comes for a short duration due to some instant action like lightning.

Signal to noise ratio:
SNR = Average signal power/Average noise power.

Note:

High SNR means the signal is less affected by noise, and low SNR means signal is highly affected by noise:

$$\text{SNR (in db)} = 10\log_{10}\text{SNR}$$

Data rate depends on bandwidth, level of signal and level of noise.

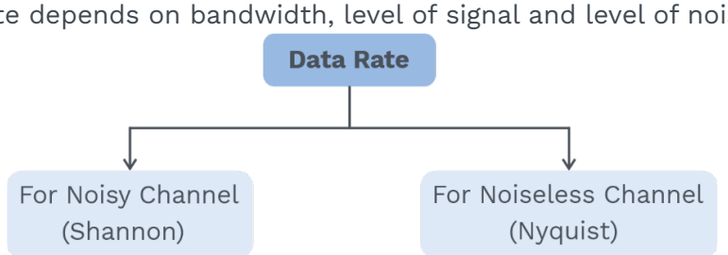


Fig. 2.8 Data Rate Based on Types of Channel

For noiseless channel:
We calculate Nyquist formula
Maximum Bit rate = 2 * Bandwidth * $\log_2 L$ (L is level of signal)

Concept Building Exercise

A channel has a bandwidth of 6000 Hz. Consider the channel is noiseless and the channel is transmitting a signal with 2 signal levels . What should be the maximum bit rate?

Maximum bit rate = 2 * Bandwidth * $\log_2 L$ (L is level of signal)
= 2 * 6000 * $\log_2 2$
= 12000 bps

For noisy channel:
We calculate the Shannon formula:
Maximum bit rate or capacity: Bandwidth * $\log_2(1+SNR)$

Concept Building Exercise

Consider a noisy channel where SNR ratio is too low, consider it as 0, What is the capacity of the channel?
Since SNR is 0, this means the signal is highly affected by noise, and it gets lost
Maximum bit rate or capacity = Bandwidth * $\log_2(1 + 0)$
= 0
Capacity of channel in this case is 0. **Have you observed bandwidth is present still the capacity of channel is zero!**

PRACTICE QUESTIONS

Q1 **If the television channels have a Bandwidth 4MHz. If 8 level digital signals are used. How many bits per second can be sent ? Assume the channel is noiseless.**

Sol: We can use Nyquist in this case:

Maximum bit rate = 2 * 4 * $\log^8_2$ (For 8 levels – 3 bits needed)
= 24 Mbps

Q2 **Can you guess rail road, oil in pipes are which types of communication!!**

Sol: Half duplex, one at a time.

Q3 **What is the effect on rate if the bandwidth gets doubled?**

Sol: The rate is doubled.

Q4 **How will the rate improve if we double the SNR?**

Sol: The rate will slightly increase.

Switching:

Why do we need switching?

When we have many devices, we can connect using point to point (as we have seen in mesh topology) or multipoint connections (as we have seen in star topology). But can we extend these methods when we have a very large network!! BIG NO

Switching helps here; there are 3 types of switching see figure below:

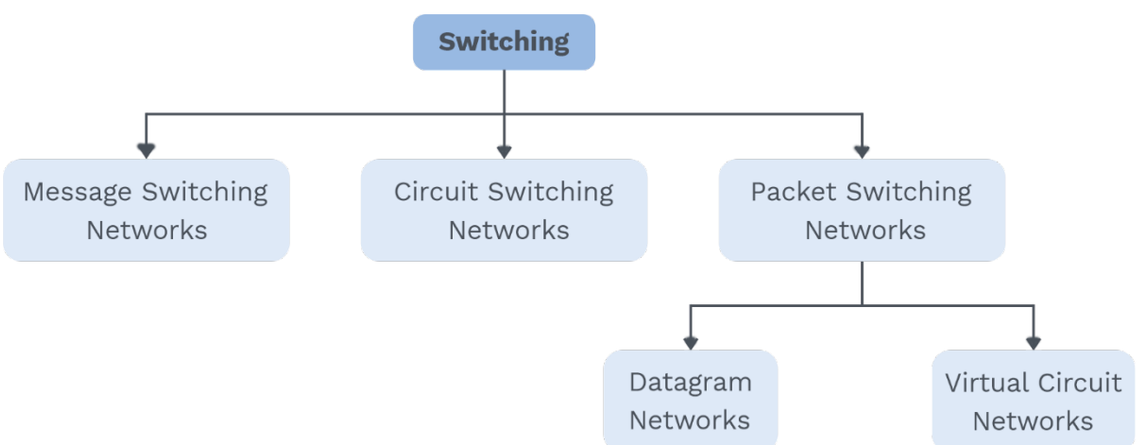


Fig. 2.9 Flow Chart Representing Types of Switching

Circuit switching networks:

Standard Definition

It is made up of a set of switches connected by physical links in which each link is divided into n channels.

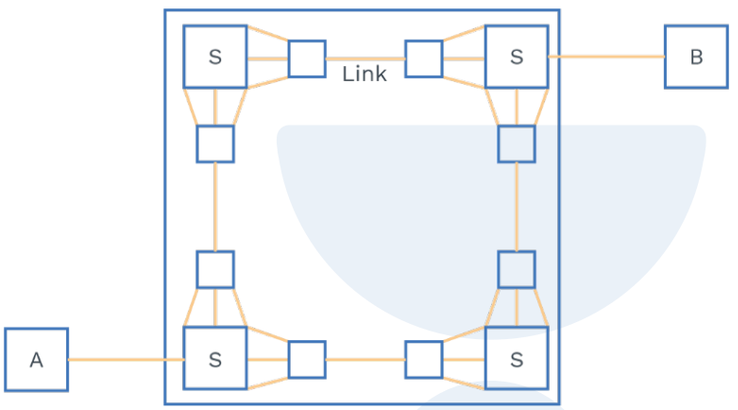


Fig. 2.10 Diagrammatic Representation of Circuit Switching

- Circuit switching needs to be handled at the Physical layer.
- There must be reservation of resources before the communication takes place
- Resources get reserved during the set-up phase, and for the entire, duration it gets fixed until there is a teardown phase.
- Communication happens in three phases:
  Set up phase: A dedicated path needed to be established before the transfer of data.
  Data transfer phase: transfer of data takes place in this phase.
  Tear down phase: A signal is sent to release the resource.
- When the path has established, there is no danger of congestion.
- Switching at the traditional telephone network uses the circuit switching.

Note:

Resource:
It is nothing but channels (bandwidth in case of FDM or time in case of TDM), buffers, ports etc.)

Packet Switching Networks:

Standard Definition

There is no resource reservation; the resource is allocated on demand.

Note:

The message is divided into packets which are fixed or variable sized networks.
There is no need to establish a dedicated path in advance but it can be allocated on demand.
The allocation of resources is done on FCFS basis.
Packet contains the user data and controlled information.

Packet switching technique:

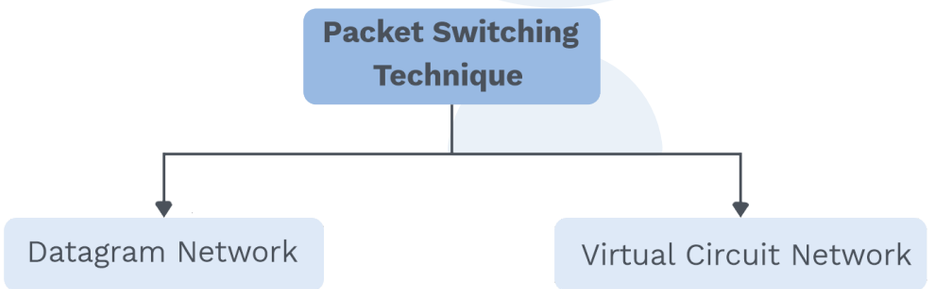


Fig. 2.12 Types of Packet Switching Technique

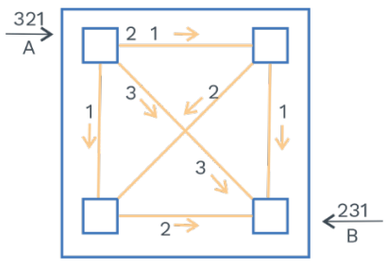
Datagram network:

In this, each packet has no relation to the other packet.

Note:

Packet in this network are called datagram.

- It is normally done at the network layer.
- A switch in the datagram network uses a routing table which is based on the destination address.
- Sometimes, it is said that these networks are connectionless, which means the switch does not keep the information about the connection state.
- The destination address in each packet remains the same.



- Packet may reach out of order as shown in the diagram.
- Switching on the internet is done using the datagram approach.

Concept Building Exercise

Is out of ordering possible in circuit switch networks?

No, since every message follows the same path.

Can you guess whose efficiency is better? And why?

Datagram network, because there is no wastage of bandwidth, resources are allocated on demand.

Virtual circuit network:

Standard Definition

In virtual circuit representation, all the packets follow the same source and destination travel the same path, but the packet may arrive with the different delays if resource allocation is on-demand.

- Packets from the single message travel along the same path.
- Resource reservations can be made during the setup phase or on-demand during the transfer phase.
- Each packet contains a Virtual Circuit Identifier (VCI).
- Again, in a virtual circuit, there are also 3 phases required to transfer the data.

Setup Phase, transfer phase, tear down phase:

- Virtual switch networks are used in switched WAN normally at the data link layer.

PRACTICE QUESTIONS

Q1 **A path in a digital circuit-switched network has a data rate of 1 Mbps. The exchange of 2000 bits is required for the setup and teardown phase. The distance between the two parties is 5000 km. The propagation speed is 2 × 10^8 m/s. What is the total delay if 1000 bits of data are exchanged during data-transfer?**

Sol: Two set up phase + 1 tear down phase, i.e 3 *(t_p + t_r)

Finally data transfer required (t_p + t_r)

So, the total delay = 4(t_p + t_r)

T_p = 5 * 10^6 / 2*10^8 = 25 msec

T_t = 2000/10^6 = 2 msec

= 4(25 + 2)

= 4*(27) msec

= 108 msec

Q2 **Tick mark where you feel end to end addressing is required:**

Sol:

	Setup Phase	Transfer Phase	Tear Down Phase
Circuit Switched Network	✓		✓
Datagram Network		✓	
Virtual Circut	✓	✓	✓

Q3 **Comparison between virtual circuit and datagram circuit:**

Sol:

Virtual circuit	Datagram circuit
The 1st packet needs a global header and for the remaining packet it just needs a local header.	Headers are required for all packets.
It is connection oriented as resources and bandwidth are reserved.	Resources are not reserved; hence datagram circuit is connectionless.
All the packets are in order as the same path is followed.	May follow a different path.
It is highly reliable.	It is not reliable.
Cost is high.	Cost is not high.
ATM uses Virtual circuits.	IP networks use datagram packet.

Previous Years' Question

Q) Which one of the following is false?

a) Packet switching leads to better utilization of bandwidth than circuit switching.

b) Packet switching results in less variation in delay than circuit switching.

c) Packet switching requires more per packet processing than circuit switching.

d) Packet switching leads to reordering, unlike circuit switching.

Sol: b) **(GATE-2004)**

Chapter summary

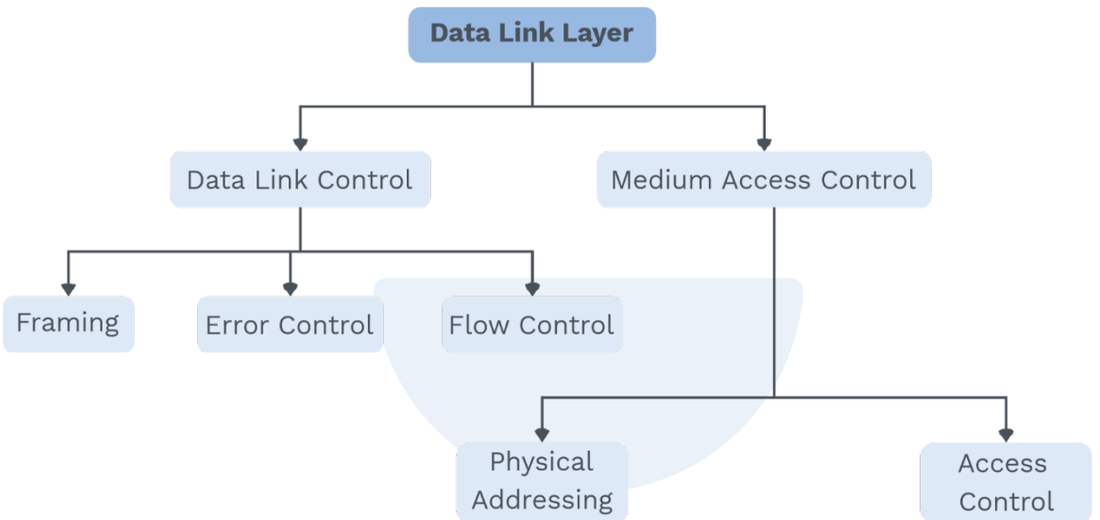
- Physical layer deals with electrical characteristics by type of link.
  Example: If the link is copper, then we use an electrical signal.
  If the link is optical, then we use a light signal.
- Physical layer deals with mechanical characteristics by type of transmission mode.
  Example: Simplex, Half duplex and Full duplex.
- Physical layer deals with various topologies like Bus, Ring, Star and Mesh.
- Physical layer deals with encoding techniques.
- Bandwidth utilization means using available BW(bandwidth) to realise the goal. and using multiplexing, we can achieve efficiency.
- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.
- Series of interlinked nodes consist of switching networks; these interconnections can be done using switches.
- Circuit-switched Network: It consists of a set of switches connected via a physical link where each link is dividing into n-channels.
- In circuit switching, there is a setup phase, data transfer phase and termination phase.
- In packet switching, there is no resource allocation for a packet, resource allocation can be done on demand.
- In a datagram network, each packet is treated independently of all others.
- A virtual–circuit network is an intermediate between a circuit–switched network and a datagram network.

3 Data Link Layer

3.1 DATA LINK LAYER

It has two major functions:

- Data link control
- Medium access control



Data link control:
It includes framing, flow control and error control.

Medium access control:
It tells about the access control.

Data link control:
1) Framing:
We already know the physical layer provides bits synchronization (sender and receiver use the same bits). Now, these bits have to pack into the frame, and this is done by data link layer.

OR

Data link layer also takes packets from the network layer, and enclose them in multiple frames and send it to the physical layer.

Frame is having 3 basic components:

- Frame header
- Payload field
- Frame trailer

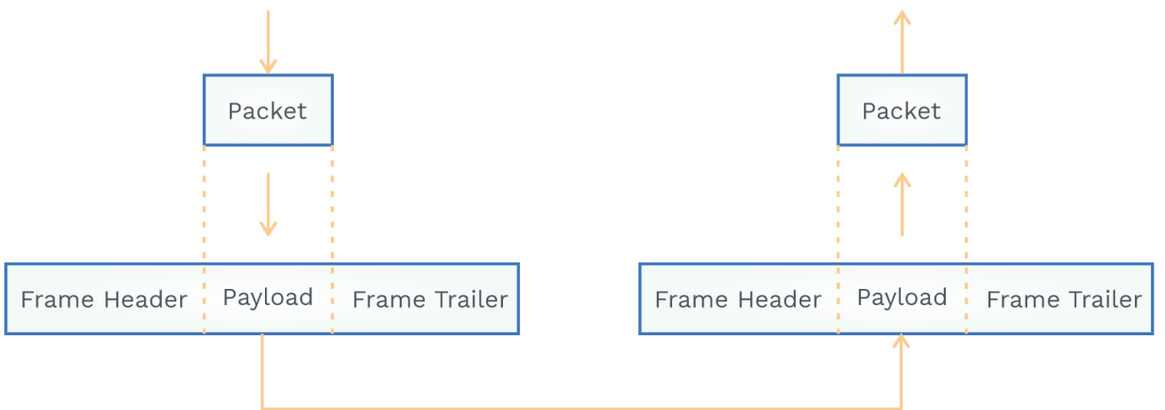


Fig. 3.1 Basic Components of Frame

Concept Building Exercise

- **Is it possible to encapsulate the entire message in a single frame? Is it efficient?**
  Yes, it is possible. But it is not efficient.
- **Why is it not efficient?**
  Because if a single bit error is there, entire frame has to retransmit.

Types of framing:
- Fixed size framing
- Variable size framing

Fixed size framing:
- As the name suggests, it is of Fixed Size.
- You need not worry about the ending of the frame.
- Since Frames are of fixed length, hence no flexibility is possible.

Variable size framing:
- We need to define an end of the frame as well as beginning of the next frame. This can be done in two ways:
  i) Character stuffing
  ii) Bit stuffing

Character stuffing:
- A flag is added at the beginning and at the ending of the frame, which tells the frame has started and ended.
- Flag size is multiple of 8 bit.
- It was used when only the character as a data was exchanged at the data link layer.

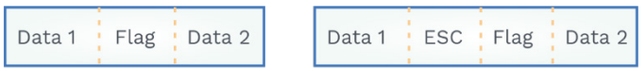
Concept Building Exercise

- **What to do when the data is having other than text, i.e. audio, video, images? Why not go with character stuffing?**
  In this case, we use byte stuffing; we cannot use character stuffing because there may be a chance when FLAG bytes get matched with the data inside the packet.
- **What would you think if you see two continuous FLAG?**
  It means ending of one frame and starting of next frame.
- **How does FLAG look like?**
  It has some special patterns like $(1111110)_2$ or $(0x7E)_{16}$ for HDLC protocol.

Byte stuffing:

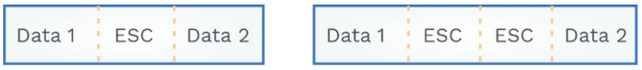
- Add 1 extra byte whenever there is a flag or ESCAPE character in the text.
- Special byte is added to the data section of the frame when the same pattern as that of flag is present inside the frame.
- Now frame has an extra byte called as ESCAPE(ESC).
- This adding of an extra byte is called Byte stuffing.
- But the problem comes when the escape pattern appears in the middle of the data. The solution is add extra ESCAPE.

See figure below!!



Original Frame — Frame after Byte Stuffing

- When there is ESC pattern in an original frame add another escape byte:



Original Frame — Frame after Byte Stuffing

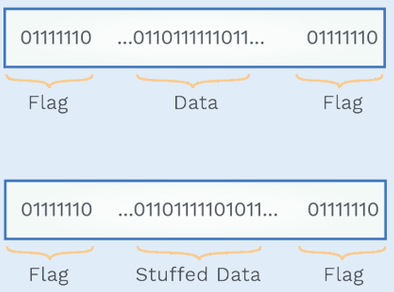
- Byte stuffing has one disadvantage, we have to use 1 byte always. So, there is always a limitation of using 8 bit.
- We can overcome this situation using bit stuffing.

Bit stuffing:

- In this, whenever flag pattern appears in the data section of the frame, to prevent it from looking like a pattern of the flag we add an extra bit to break the pattern.
- Let's say if we have taken 01111110 as Flag, so after bit stuffing, data will become 011111010.

- If we have taken 10000001 as Flag, so after bit stuffing, data will be 100000101.

- **What to do if a FLAG like a pattern appears in data?**
  If a FLAG like a pattern, say 01111110, appears in data, we need to stuff a single bit '0', at the end of 5 consecutive ones, instead of 1 byte(ESC), that we were doing in byte stuffing.



Note:

Real flag is not stuffed by the sender; hence no need to destuffing for real flag at the end of the receiver.

2) Error control:

- It manages both error connection and error detection.
- Basically, it deals with the retransmission of data, and this retransmission is based on Automatic Repeat Request (ARQ).
- There are basically two types of error: Single bit error and Burst error.

Single bit error: Single bit get changes when data reaches to receiver,

11101010 ⟶ 11111010

Burst error: When 2 or more bits gets changes,

11101010 ⟶ 11111011

Error detecting codes:
In error detection, we can only know the packet is corrupted. Redundant bits are added to detect error, and when the error is detected, retransmission is used to recover from error.

Error correcting codes:
In error detection, we can also know the bit which has been corrupted. Redundant bits are added in such a way, that it will detect and correct the errors.

Concept Building Exercise

- **What do you understand by adding redundant bits?**
  These bits are added by the sender and removed by the receiver. It is done so that errors can be detected and corrected easily.

Error detection:

- Parity checking
- Cyclic redundancy check
- Checksum

Simple parity check codes:

- It can detect an odd number of errors.
- In this k bits, data is changed into n bit code words.
- n = k + 1 (extra 1 bit is called parity bit)

In the case of even parity, if the number of 1's are even then, we add an extra bit by adding 0 else, if the number of 1's is odd, then we add an extra bit of 1 to make the Code bit an even number of 1.

Standard Definition

- A single parity check code is a single bit error detecting code in which:
- n = k + 1 with d_{min} = 2.

Concept Building Exercise

What do you understand by d_{min}?
It is called minimum Hamming distance, and it is defined as the number of bits that are changed during the transmission:

11111 ⟶ 10101

In this case $d_{min.}$ = 2

Find the hamming distance of the given coding scheme?

d(0000, 1010)

d(1100, 1111)

Sol: 2, 2

What is the minimum Hamming distance for error detection?
$d_{min.}$ = t + 1 (where t bit errors occur during transmission)

If the minimum hamming distance is 2, how many bits of error can be detected?
1 (one bit)

What is the minimum Hamming distance for an error correction?
$d_{min.}$ = 2t + 1

Let's see below diagram and understand how simple parity bits are used in error detection,

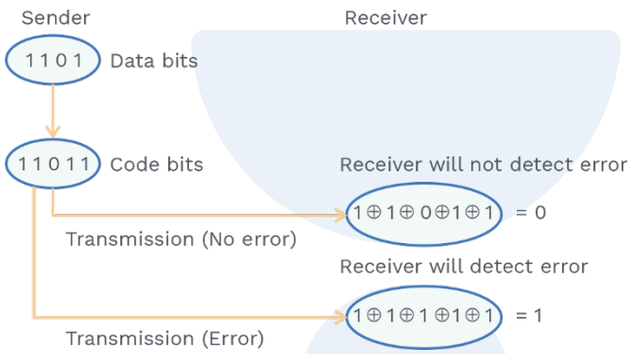


Fig. 3.6 Diagrammatic Representation of Simple Parity Bits Used in Detection

Here we are taking codebits as even parity:

- Databits are sent in the form of codebits by adding single parity.
- **You might be thinking about how to add a parity bit?**
  Add all the bits, and modulo-2 will give the parity bit.
- At the receiver side, it will do modulo-2 of the codebit, and if the result, known as syndrome, is 1, then an error is detected, and if the syndrome is 0, then there is no error.

Note:

A simple parity check code can detect odd number of errors only.

Cyclic redundancy check (CRC):
Common CRC polynomials are:
CRC–32 used in LAN, CRC–8 used in ATM header.

Some rules for generating the generator polynomial,
Rule 1: It should not be divisible by x.
This condition will ensure that all the burst error of length equal

to the length of the polynomial are detected.

Rule 2: It should be divisible by x + 1. This condition will ensure that all the burst error affecting an odd number bits are detected.

Rack Your Brain

CRC generator is $x^3 + x^2 + 1$. Convert it into binary.

CRC generator: 1101 (It is known by both sender as well as receiver)

Code: 1011011

Steps:

1) If CRC G has 4 bits then add 3 bit to the code 1011011000

2) Now mod-2 sum

And do the following at sender side,

```
1101)1011011000
     1101
      1100
      1101
        1110
        1101
          1100
          1101
          001  → Take last (n–1) CRC if CRC is having
                 n bits then append it in place of zeroes
```

The correct code which needs to be send is 1011011001.

3) Receiver will check whether the code is correct or not.

```
1101)1011011001
     1101
      1100
      1101
        1110
        1101
          1101
          1101
          0000 → All zero means code is correct
```

- CRC codes can detect the single bit errors, double errors, odd number of errors and burst error.
- Fast when implemented in hardware compared to software.
- The divisor in cyclic codes are normally called generators.

Checksum:

- Checksum bits are usually placed at the end of the message with a complement to the sum function.
- It is used on the internet but not on the data link layer.

What we are using at the data link layer then!! CRC.

Let us understand by taking example,

a) Let's say a set of numbers (10, 20, 30) needs to be sent. Then the sender will send (10,20,30,-60) here -60 is the sum of all the numbers with a negative sign. Now the receiver will add all the numbers, and if the result is zero then there is no error.

b) By taking chunks of 2 bits, Explain how the checksum will work on the sender side if data is 01110001.

We have 01 11 00 01 (2 bit chunks)
Now add using 1 bit compliments 01 + 11 + 00 + 01 = 101
overflow add MSB to LSB 01 + 1 = 10
Take 1 complement of result = 01
Append to the sender data bit and send it to the receiver = 0111000101
At the receiver end we have 01 + 11 + 00 + 01 + 01 = 110
Overflow add MSB to LSB = 10 + 1 = 11
Complement of result = 00

If the result is 0; hence no error, if the result is non zero then error will be detected.

Questions:

1) In CRC, what do you think is the relationship between the size of the divisor or remainder?
Remainder is always one bit smaller than the divisor.

2) CRC generator is $x^3 + x + 1$, data bit are 1101, What will be the CRC which needs to be appended at the databit?
CRC generator $x^3 + x + 1 = 1011$, we will append 3 bit 0 to the data bit.
After doing the modulo operation, we got CRC as 010, and Codebit will become 1101001.

```
1011)1101000
     1011
      1100
      1011
       1110
       1011
        1010
        1011
         001  ⟶ This CRC needs to append
```

3) What is the checksum value which needs to be send for the following two data items:
0x4589 and 0xBA76?

```
  4 5 8 9
  B A 7 6
-------
  F F F F
  0 0 0 0  ⟵ 1's compliment
```

Checksum bit which needs to be sent is 0000

Previous Years' Question

Q. Which of the following statements is TRUE?

a) Both Ethernet frame and IP packet include checksum fields

b) Ethernet frame includes a checksum field, and IP packet includes a CRC field

c) Ethernet frame includes a CRC field, and IP packet includes a checksum field

d) Both Ethernet frame and IP packet include CRC fields

Sol: c) **(GATE-2006)**

Error correcting:

- For error detecting and correcting we will use **hamming codes.**
- Let us first understand relationship between data bits and redundant bits in hamming code.
- Let us take 'd' as data bits and 't' as a redundant bits.
- Total number of bits that has to be transmitted = d + t.
- **Think how many states can the redundant bit discover?**

Its d + t + 1

Note:

Above condition derives a relationship,
$2^t \geq d + t + 1$

Let's say the value of d (message to be transmitted) is 4 then t would be 3.
It would satisfy this equation $2^t \geq d + t + 1$
In this case, t cannot be less than 3 i.e redundant bits cannot be less than 3.

Let us understand Hamming code by taking example:
Note: We calculate here on the basis of even parity bits.

Message: 1011
Here d = 4, now we need to add parity bits for each combination in the powers of 2 as shown below:

7	6	5	4	3	2	1
1	0	1	t_4	1	t_2	t_1

t_1 will take care of 1,3,5,7,... bits
t_2 will take care of 2,3,6,7,... bits

t_4 will take care of 4,5,6,7... bits

7	6	5	4	3	2	1
1	0	1		1		1

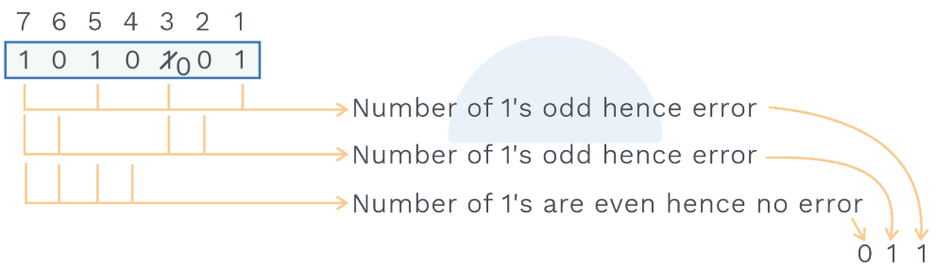
Your ultimate goal should be to make an even number of 1's for particular parity, in this case, by checking position 3,5,7 we got a number of 1's as odd, therefore we have to put $t_1 = 1$ in 1st position in order to make even parity.
Same we will do for t_2 and t_3,

7	6	5	4	3	2	1
1	0	1	0	1	0	1

Now the codebit that has to be transmitted is 1010101.
Let us assume at the receiver side one bit got corrupted, now how hamming code will detect and correct the code.

7	6	5	4	3	2	1
1	0	1	0	x_0	0	1

How receiver will detect?



How receiver will correct,
Since, we got to know which position is detected error, here it is 3rd position
Now we can change the 3rd bit and make it correct.

Previous Years' Question

Q. A computer network uses polynomials over GF(2) for error checking with 8 bits as information bits and uses $x^3 + x + 1$ as the generator polynomial to generate the check bits. In this network, the message 01011011 is transmitted as:

a) 01011011010 **b)** 01011011011
c) 01011011101 **d)** 01011011100

Sol: c) **(GATE-2017)**

Previous Years' Question

Q. A bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then the input bit-string is:

a) 0111110100 **b)** 0111110101
c) 0111111101 **d)** 0111111111

Sol: b) **(GATE-2014)**

Delays in computer network:

Transmission delay:

(t_t) Time which sender takes to transmit a frame on the link.
t_t = L/B (L = length of frame, B = bandwidth of channel).

Propagation delay:

(t_p) Time taken by 1 bit to travel from sender to receiver.
tp = d/v (d= distance between sender to receiver and v is transmission speed).

Queuing delay:

(t_q)Before processing of the frame it has to wait inside the buffer, that waiting time is called queuing delay.

Processing delay:

(t_{pr}) It is the time taken by a node or processor to process the frame. Basically it depends on the speed of the processor.

Flow control:

It deals with how much data the sender can transmit so that the receiver should not overflow.

Standard Definition

Set of procedures used to restrict the amount of data that the sender can send before waiting for an acknowledgement.

Data link layer uses error control, framing and flow control to send data from one node to another node.

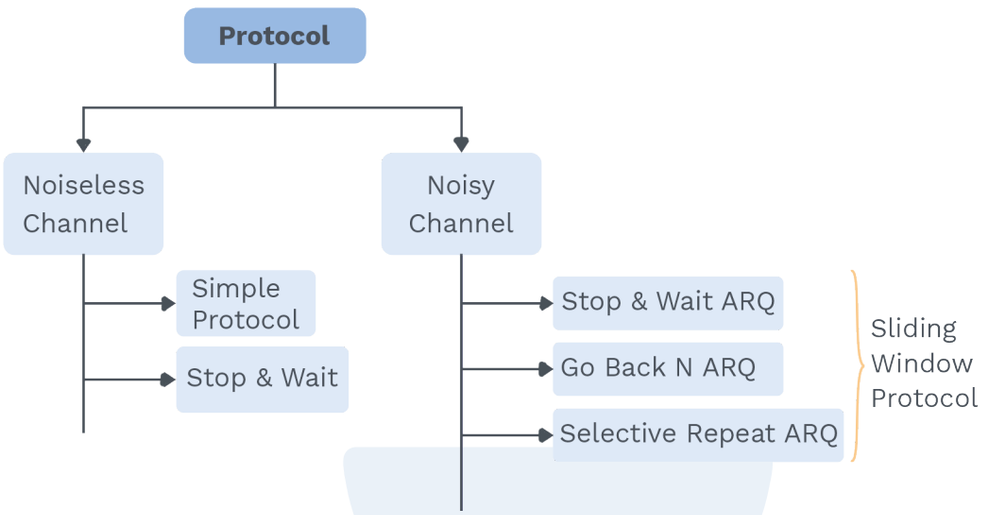


Fig. 3.2 Flow Control Protocols

For noiseless channel:

- We do not need to control errors in this channel.
- Let us assume in this channel, no packet is lost or corrupted.
- We can use simple protocol and stop and wait in this channel.

Simple protocol:

- It has no flow control and no error control.
- We assume that the direction of a packet is from sender to receiver i,e unidirectional.
- In this, the receiver can never discard the packet.
- There is no ack from the receiver.
- Both sender and receiver are constantly running because they do not know when an event is happening.

Note:

What do you understand about the events happening in the above point?
It means the sender does not know when the packet will come from the network layer; it has to constantly check, and the receiver does not know when the packet will come from the physical layer; it also has to constantly check.

Stop and Wait:

- Whenever the Receiver buffer size is full, it starts discarding the packet.
- There should be some mechanism so that sender should slow down its speed.
- **Can you guess what that mechanism is?**
  Sending ACK or acknowledgment from the receiver to sender.

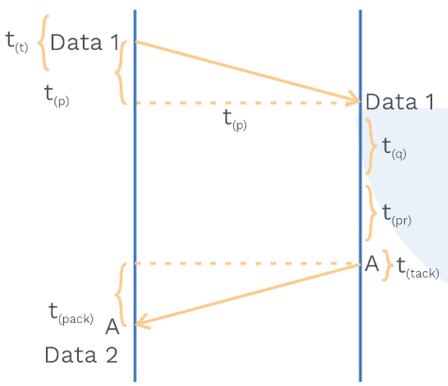
How stop and wait works:

1) Sender sends a data packet and waits for acknowledgement from the receiver.

2) Receiver receives the data packet and sends the acknowledgement to the sender.

3) After having the acknowledgment from the receiver, the sender sends the next packet.

Working:



Grey Matter Alert!

Take bandwidth in power of 10 and data in power of 2 for easy calculation.

The packet needs to be transmitted on a link by sender takes t_t time, and then it needs to propagate from sender to receiver takes t_p time and then at receiver side packet wait inside buffer which is t_q time and after that, it has to process which takes t_{pr} time. Receiver will then transmit the ack on a link, and it will take t_{tack} time.
Now receiver will send ack to sender which takes t_{pack} time.

Total time for sending 1 packet = $t_t + t_p + t_q + t_{pr} + t_{tack} + t_{pack}$

Calculation of link utilization or efficiency or sender utilization:

An assumption we made while calculating the total time of a packet.

1) Queuing delay and processing delay can be ignored.

2) Transmission delay for ack can be ignored.

Total time = $t_t + t_p + t_{pack}$

Total time = $t_t + 2t_p$ ($t_p = t_{pack}$)

Efficiency = Useful time/total time

Useful time = t_t (transmission of packet)

Total time = $t_t + 2t_p$

Efficiency = $t_t / (t_t + 2t_p)$

Efficiency = $1/ (1 + 2a)$ ($a= t_p/t_t$)

Calculation of throughput or bandwidth utilization:

Throughput is number of the bits that can be sent in a link per second

Throughput = Efficiency * Bandwidth

$= (t_t / (t_t + 2t_p)) * \text{Bandwidth}$

$[t_t = L/B]$

$= L / (t_t + 2t_p)$

Advantage of simple stop and wait:

- Receiver always acknowledges the sender by sending an ack packet.
- As the length of packet increases, efficiency increases.

Limitation of simple stop and wait:

1) Bandwidth is not efficiently utilized.

2) If the data packet gets lost receiver will wait for an infinite amount of time.

3) If ack get lost sender will wait an infinite amount of time.

For noisy channel:

We need to do error control in this channel. **Sliding window technique** is used in this channel

Sliding window protocol:

- Sender and receiver need to deal with only a part of the possible sequence number.
- Available sequence number ≥ Sender window size + Receiver window size.

Stop and wait ARQ:

- It is 1-bit sliding window protocol because Sender window size is 1, and Receiver window size is 1.
- We have seen Stop and wait in the above section, its working, advantage and disadvantage.
- Stop and wait ARQ working is the same as Stop and wait but it solves the limitation of Stop and wait for protocol by adding ARQ.

Rack Your Brain

a) Do you think any other advantage of simple stop and wait.

b) What will be the effect on efficiency if distance increases or decreases.

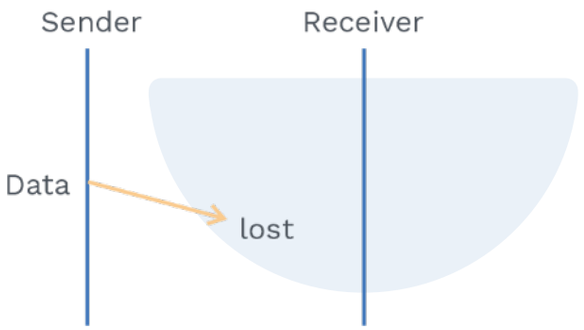
Grey Matter Alert!

ARQ: Automatic repeat request, its a request method in which receiver ask sender to retransmit the packet, if the packet is having any error.

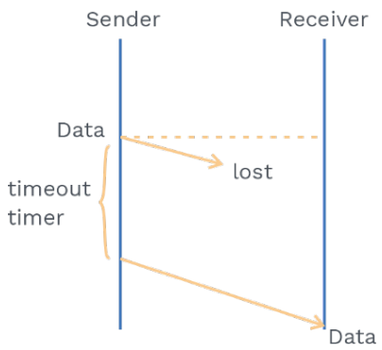
Minimum number of Sequence number required in Stop and wait ARQ?

Available Sequence number ≥ Sender window Size + Receiver window Size
Available Sequence number ≥ 1 + 1
Sequence number ≥ 2 (i.e 0,1)

Let us see how it solves the limitation of stop and wait?
a) When data packet is lost?
If the data packet is lost, both the sender and receiver may get into a deadlock.



In order to prevent this situation, after sending the data packet, the sender starts the **time out timer**, to make sure the packet is transmitted in a specified amount of time.

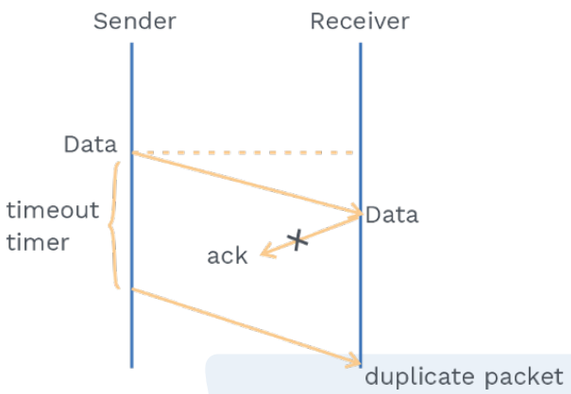


This will prevent from deadlock state.
How to prevent deadlock in Stop and wait?
Sender will add time out timer.

Note:

Stop and wait ARQ = Stop and wait + Time out timer

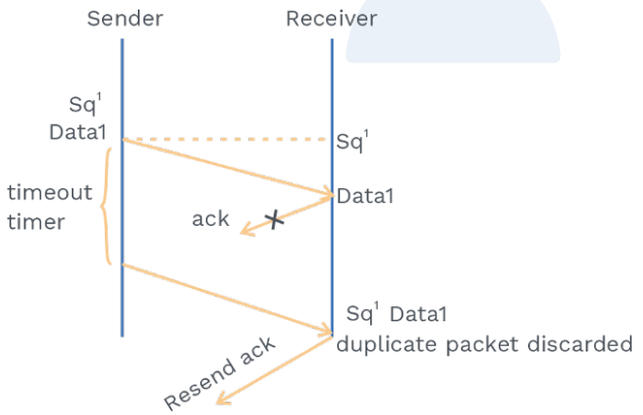
b) When ACK is lost?
Duplicate packet problem arises, see diagram.



If the timer goes timeout and sender does not receive any acknowledgement from the receiver, then the sender will retransmit the packet, but packet will be duplicated.

How to prevent duplicate packet problem in stop and wait?

Add sequence number in data packet, see, figure below.



Note:

Stop and wait, ARQ = Stop and wait + Time out timer + Sequence Number in data packet.

c) When does Ack gets delayed?
Duplicate acknowledgement problem arises.

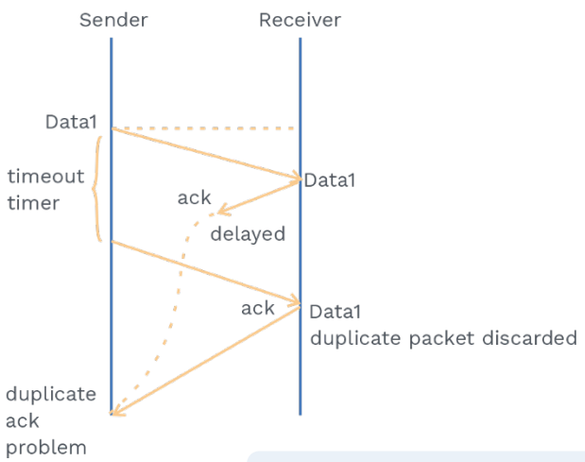


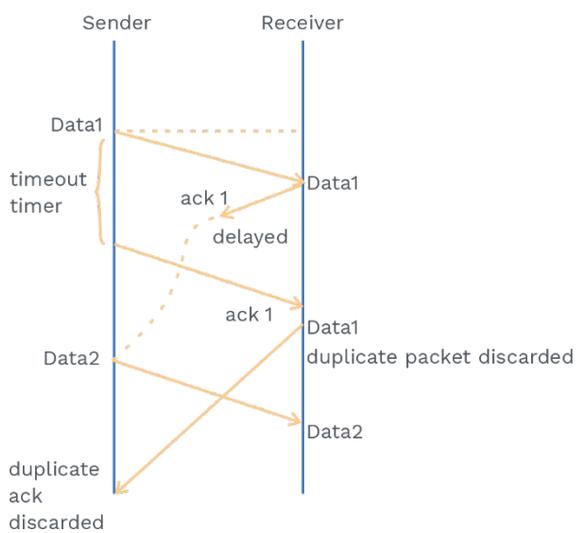
Fig. 3.3 Diagrammatic Representation of Duplicate Acknowledgement Problem

If the timer goes timeout and sender did not receive any acknowledgement from the receiver, then the sender will retransmit the packet, but packet will be duplicated this time and receiver will know that the packet is duplicated due to the sequence number attached to the packet, and it will resend the acknowledgement that will reach at the same time when the first acknowledgement reached, it will create a duplicate acknowledgement problem.

How to prevent duplicate acknowledgement problem?

Add the Sequence number to the acknowledgement.

This time if the sender sees the ack with the same sequence number, it will get to know that acknowledgement is duplicated, see diagram below.



Note:

Stop and wait ARQ = Stop and wait + Time out timer + Sequence Number in data packet + Sequence number in Ack Packet.

Let us understand the difference between “Stop and wait” and “Stop and wait ARQ.”

Stop and wait arq	Stop and wait
Since the channel is noisy there is error control mechanism.	Channel is noiseless hence no error control.
Timeout timers added after sending packet.	No concept of timeout timer.
Sequence numbers are added in data packet as well as in acknowledgement packet.	No concept of sequence number or acknowledgement number.

Rack your Brain

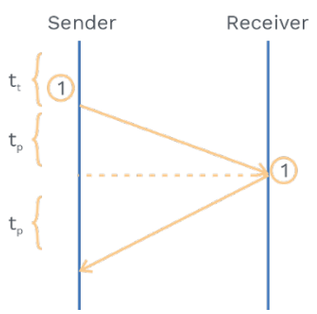
a) Why are sequence numbers added in data packets and acknowledgement packets?

b) Do you think Stop and wait ARQ is efficient?

Limitation of Stop and wait ARQ:

Sender sends data in t_t time, and then it waits for $2t_p$ time.
This $2t_p$ actually cause limited efficiency.

Let’s consider the given scenario:



- In t_t = 1 packet sends
  In 1 second = $1/t_t$ packet sends
  In a time of $(t_t + 2 * t_p) = (t_t + 2 * t_p)/t_t$ packets can be sent.
- From this we get to know we can transmit (1 + 2a) packet for full efficiency.
  But we are sending only 1 packet.
- Sender can send in $2t_p$ time also.

Grey Matter Alert!

Can you think how we can improve the efficiency of Stop and wait for ARQ?
It can be improved by increasing the window size so that sender should not wait for $2t_p$ time.

PRACTICE QUESTIONS

Q1 **In Stop and wait, 10 packets need to be sent from sender to receiver, which every 4 packets have been lost. What is the total number of the packet that needs to be sent?**

Sol:

1 2 3 (4) 5 6 7 8 9 1 0

lost (needs retransmission)

1 2 3 4 4 5 6 (7) 7 8 9 1 0

lost retransmission

1 2 3 4 4 5 6 7 7 8 9 (10) 10

lost retransmission

Total number of packet that needs to be sent is 13

Q2 **There is a channel between sender and receiver, and the channel is having a problem because of which some packets are getting lost, error probability is 0.5 (i.e while sending 100 packets, 50 packets are lost). How many total number of packets needs to be transmitted if 500 packets need to be sent?**

Sol:

error probability is 0.5 that means
50% of packet get lost

$$\underbrace{500}_{\text{Sending 500 packet}} + \underbrace{500 * (0.5)}_{\text{250 packet get lost}} + \underbrace{500 * (0.5)^2}_{\text{125 packet get lost}}.....$$

$$500\left(\frac{1}{1-0.5}\right) = \frac{500}{0.5} = 1000$$

1000 packet needs to be transmitted.

Previous Years' Question

Q. Suppose that the stop-and-wait protocol is used on a link with a bit rate of 64 kilobits per second and 20 milliseconds propagation delay. Assume that the transmission time for the acknowledgement and the processing time at nodes is negligible. Then the minimum frame size in bytes to achieve a link utilization of at least 50 % is___.

a) 160 **b)** 320 **c)** 640 **d)** 220

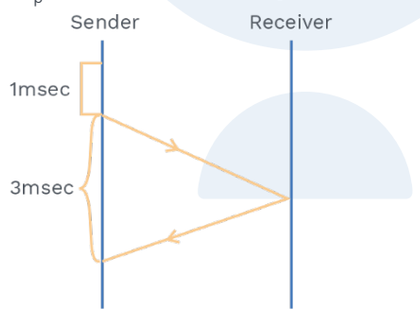
Sol: b) **(GATE-2015)**

Let us understand with example how to increase efficiency in Stop and wait ARQ,

T_t = 1msec and T_p = 1.5msec

efficiency = 1/1+2a

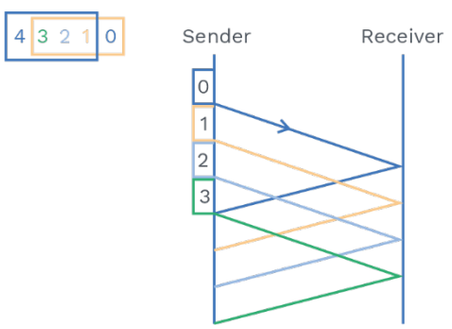
Putting values of T_t and T_p we have efficiency = 0.25



Here, sender is transmitting for 1 msec and waiting for 3 msec.

Let's send 3 more packet in 3 msec:

In the below diagram when the acknowledgement of packet (0) is received, we can send a new packet (4). At this point, the sender came to know packet(0) is received, and it makes the space for the packet (4). This is called the sliding window technique.



Note:

Until the acknowledgement of the first packet comes, sender holds the packet in buffer, that buffer is known as the sender window.

Go Back N ARQ:
What is N here ! Sender window size is N
Points:

- The size of the sender window must be less than 2^m (where m is the size of sequence number fields in bits), and the size of receiver window is always 1.
- Each time the receiver receives a new frame, it starts a new acknowledgement timer, and if the timer expires, the receiver sends the cumulative acknowledgement for all the frames which are unacknowledged at that moment and sometimes, it uses an independent frame if the receiver wants to acknowledge only one frame.
  It silently discards the frames if frames are corrupted.

Sender window:

- It is the sequence number of the data frames which can be in transmitted. The maximum size of the window is $2^m - 1$.
- The sender window will slide according to one or more valid acknowledgement comes.

Current sender window size

Window slides after sending packet (0)

Receiver window size:
In Go back N, Receiver size is always 1.

Go Back N, does not accept the out of order packet.
Given diagram is a flow how packet travels in Go Back N,
Here, N = 4,

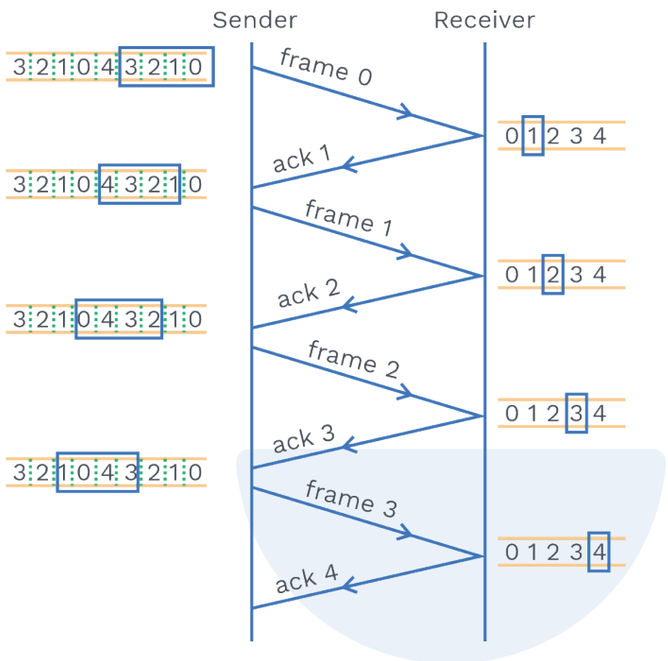
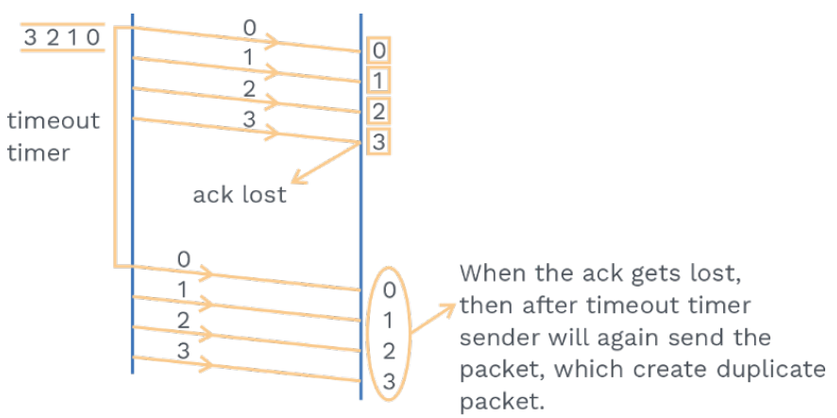


Fig. 3.4 Flow of Packets in Go Back N

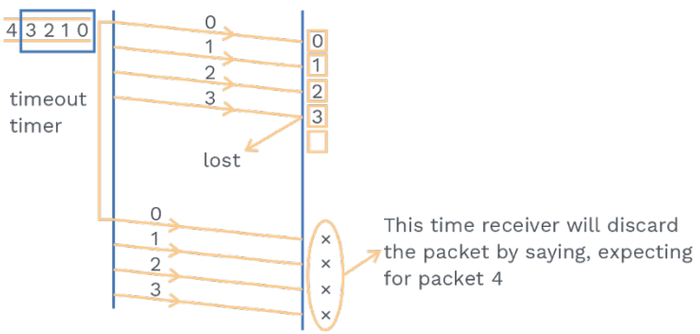
Why is there a need for taking sequence number N+1?
If you see the diagram above Window size is 4, but still, we have taken 5 sequence numbers (i.e 0,1,2,3,4).

In order to understand why we have taken the N+1 sequence number, we must understand what happens when the acknowledgement gets lost in Go Back N and when Sender window = Sequence number?
In the below diagram N = 4 and Sequence number = 4.



Here, duplicate packet problem arises.

Now, let us take a situation where N = 4 but Sequence numbers are 5.



Now you get to know why we have taken.

Note:

Maximum sequence number >= Sender window Size + Receiver window size
Maximum sequence number >= N + 1

Q3 **Sender window size = N, Receiver window size = 1, What will be the number of bits required for Sequence number?**

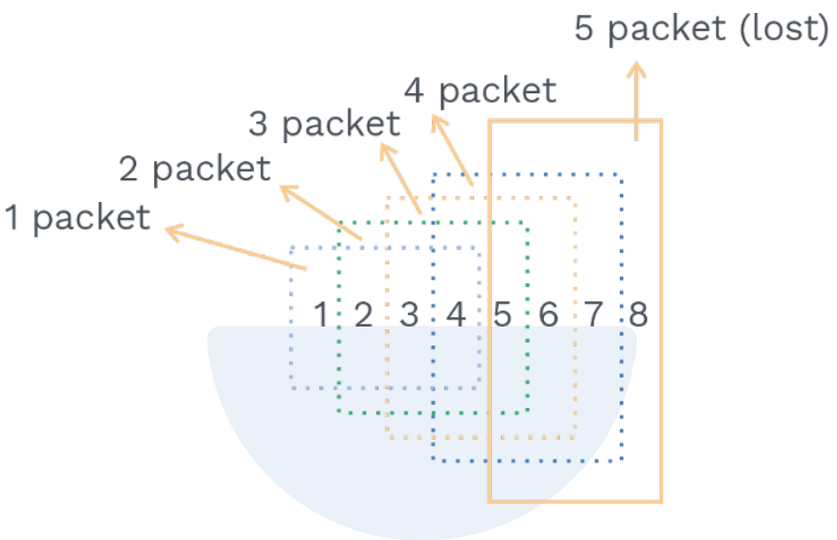
Sol: $\log_2(N+1)$

Q4 **Number of bits available in the Sequence number field is 'k', what is the possible Sequence number in GBN protocol?**

Sol: Possible sequence number are from 0 to $2^k - 1$

Q5 **In Go Back 4, assume 8 packets need to be sent from sender to the receiver in which every 5th packet has been lost. What is the total number of packets that needs to be sent?**

Sol: If N = 4, means window size is 4, if any packet gets lost we need to retransmit the entire window,



When the acknowledgement of the 5th packet does not reach the sender side, and there is a timeout timer at the sender side, it will retransmit the entire window.

Note:
The 5th packet contains Sequence numbers from 5,6,7,8. It needs to retransmit.
Now below diagram shows the scenario for remaining packet.

1 2 3 4 5 6 7 8 5 6 7 8 6 7 8 8

Total number of packet which needs to retransmit are 16.

Efficiency in Go Back N:

Efficiency = Useful time / Total time

Useful time = Sender Window Size * Transmission time (t_t)

Total time = $t_t + t_p + t_p \Rightarrow t_t + 2t_p$

Efficiency = $N * t_t / (t_t + 2t_p)$

$= N/(1 + 2a)$

Previous Years' Question

Q. A 1 Mbps satellite link connects two ground stations. The altitude of the satellite is 36,504 km, and the speed of the signal is 3×10^8 m/s. What should be the packet size for a channel utilization of 25% for a satellite link using the go-back-127 sliding window protocol? Assume that the acknowledgement packets are negligible in size, and that there are no errors during communication.

a) 120 bytes **b)** 60 bytes **c)** 240 bytes **d)** 90 bytes

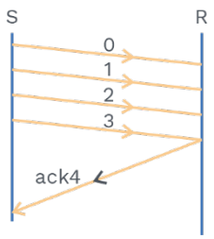
Sol: a) **(GATE IT-2008)**

Go back N uses cumulative acknowledgement (mostly) and independent acknowledgement (if required)

Let us see about these acknowledgement.

Cumulative acknowledgment:

- If Kth packet acknowledged, this implies (k-1)th packet is received successfully.
- At the receiver side, it starts the acknowledgement timer, and when it expires, the receiver will send the cumulative acknowledgement for the packet it receives in the meantime.



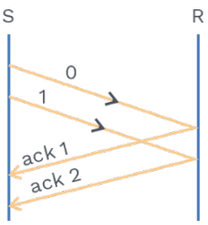
What do you understand by discarding a packet silently in Go back N?

This means it is not going to accept it; due to this, there will be time out at the other end, and entire window is sent in case of GBN.

Independent acknowledgment: Sender will receive acknowledgement for every packet

Rack Your Brain

Acknowledgement timer or timeout timer, which should be greater and why?



Selective repeat ARQ

Points:

- The size of sender window is equal to receiver window size.
- Available Sequence number = Sender window Size + Receiver window size.
  $2^n = 2^{n-1} + 2^{n-1}$ where n bits are used for sequence number
- As soon as the receiver receives the frames, it sends the acknowledgement, and uses the independent acknowledgement.

In Go back, N, out of order packets are not accepted, which means the sender has to send the entire window, which leads to consumption of bandwidth and more traffic. In noisy channels, there are more chances of corrupted packets, then we can use a mechanism called **Selective Repeat ARQ.**

In Selective repeat ARQ, only the damaged the frame needs to be sent; it makes efficient use of bandwidth in the noisy channel.

Rack Your Brain

Do you think Go back N is preferred in a noisy link !!

Note:

Receiver has to do more work in selective repeat, Think why !!

Receiver does not accept the corrupted frame and also does not discard the frame silently, but it will use negative acknowledgement.
Due to the use of negative acknowledgement, the sender need not to wait for timeout timer completion.
Receiver accepts out of order packets.
Efficiency in SR protocol: N/(1+2a).

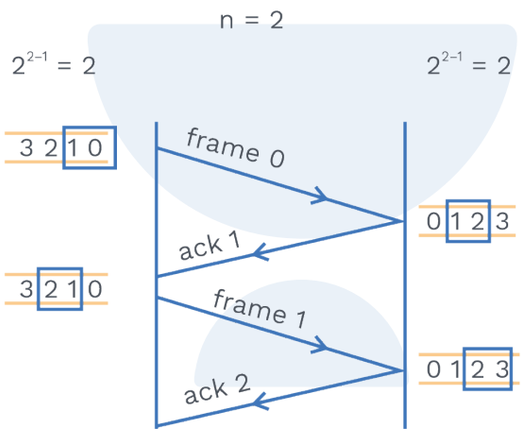
Q6 **What will be the maximum window size that is required for data transmission when SR(Selective repeat) protocol with 5 bit frame sequence number is used_____?**

Sol: Maximum window size = 2^{n-1} => which will give 16

It will be, Sender window size + receiver window size

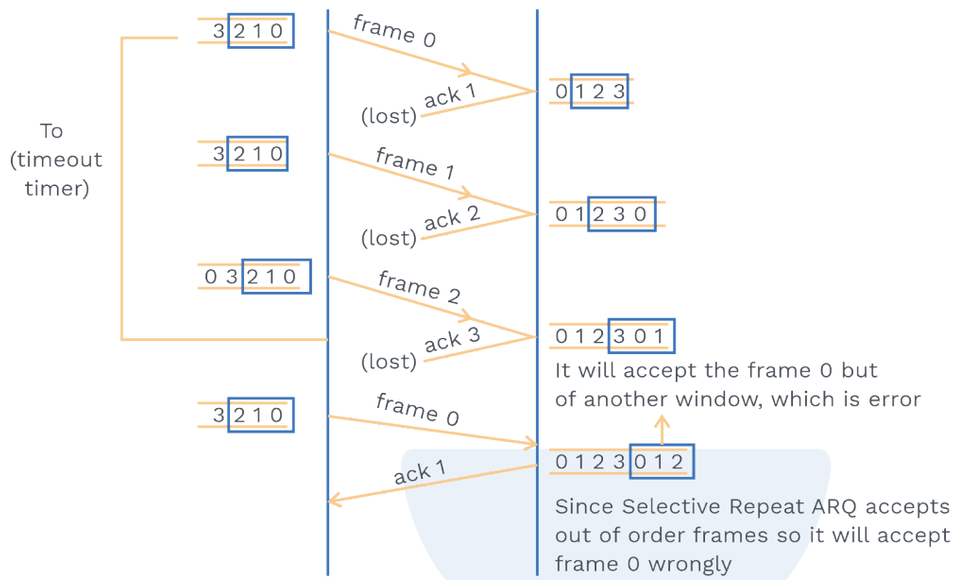
16 + 16 = 32

Lets see how selective repeat works,

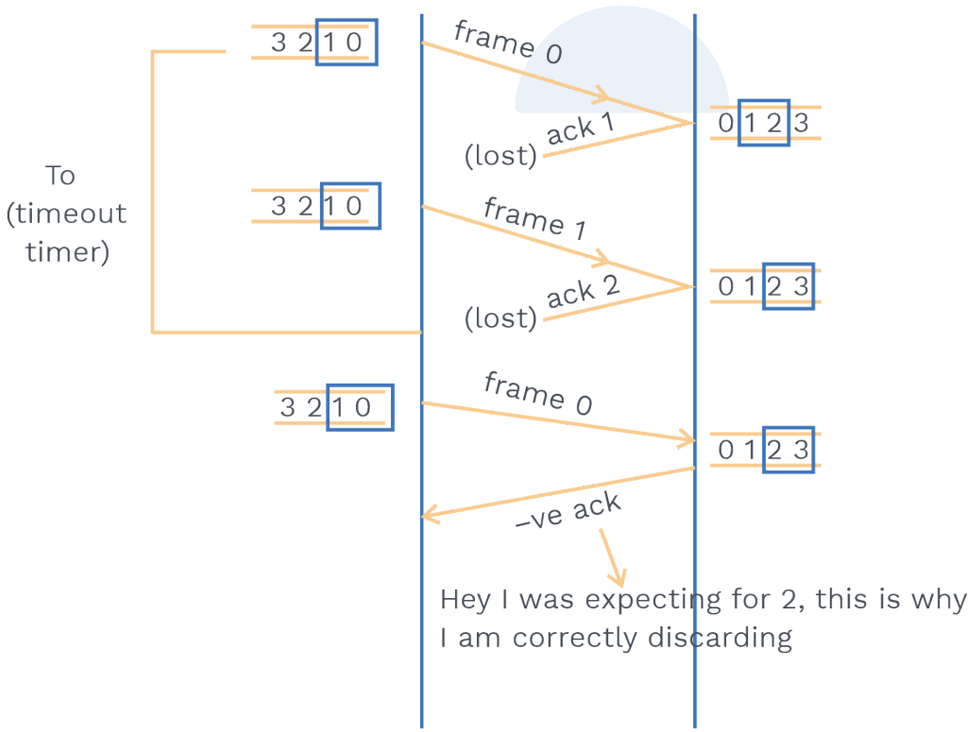


What will happen if we take window size greater than 2?
Let's take window size as 3,

In the below diagram, when all the acknowledgements are lost, the sender will send the frame again after the time out timer of that frame, and the receiver will accept the same frame, but in another window, this is an error.



Lets see if this problem will arise if we have taken window size as
Now we have taken window size as 2.



If we see the above figure, after timeout, when the sender resends the packet again, receiver will give a negative acknowledgement. This is the reason selective repeat ARQ we will use window size as 2^{n-1}.

Concept Building Exercise

Q.1 What is Piggybacking?

Sol: Piggybacking is used to improve the efficiency of bidirectional transmission. When a frame is carrying data from P to Q, it can also carry control information about frames from Q, and when a frame is carrying data from Q to P, it can also carry control information about frames from P.

Q.2 Compare Go back N and selective repeat?

Sol: In the Go-Back-N ARQ protocol, we can send several frames before receiving acknowledgement. In case a frame is damaged/lost, we need to resend all outstanding frames we have sent before. In SR(Selective repeat) protocol, we easily avoid transmission, which is not necessary by sending only those frames that are either corrupted or missing. This is possible because of negative acknowledgement.

Previous Years' Question

Q. Consider a 128×10^3 bits/ second satellite communication link with one-way propagation delay of 150 milliseconds. Selective retransmission (repeat) protocol is used on this link to send data with a frame size of 1 kilobyte. Neglect the transmission time of acknowledgement. The minimum number of bits required for the sequence number field to achieve 100% utilization is _____.

a) 2 **b)** 4 **c)** 6 **d)** 8

Sol: b) **(GATE-2016)**

Comparison of sliding window ARQ protocols:

	Stop and Wait ARQ	Go back N	Selective Repeat
Efficiency	1/(1+2a)	N/(1+2a)	N/(1+2a)
Window size	Sender Window Size = 1 Receiver window size = 1	Sender window size = N Receiver window size = 1	Sender window size = N Receiver window size = N
Sequence numbers required	2	N + 1	2 × N

In data link control, we have seen that if there is a dedicated link between sender and receiver how the protocol works, but the case will change if we do not have a dedicated link.

How to manage in case of cellular networks where channels are not dedicated?
Here comes Medium access control, which is responsible for multiple access resolution.

Lets see categories in Medium access control,

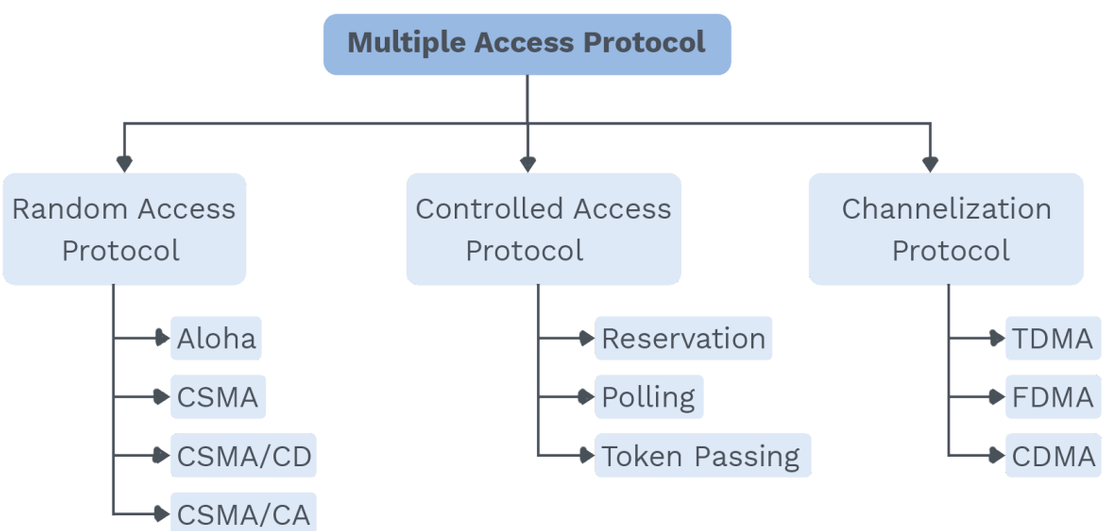


Fig. 3.5 Flow Chart Representing Multiple Access Protocol

Random access:

- It depends on the state of the medium.
- There is no proper time for the station to transmit, that is why the name is Random.
- Each station has a right to the medium without being controlled by another medium.

So, there is collision problem.

Aloha: It was designed for radio, but it can be used on any shared medium.
It can be categorized in 2 ways.

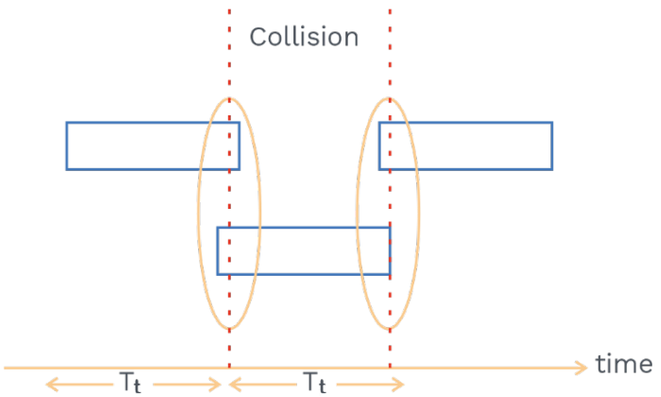
- Pure Aloha
- Slotted Aloha

Pure Aloha:

- It will allow the station to send whenever it has data.
- After sending the data, it waits for acknowledgement from the receiver.
- If it receives the acknowledgement, then the transmission is successful.
- If it doesn't receive the acknowledgement, then the transmission is unsuccessful; after the timeout timer expires, it will resend the data.

Note:

Vulnerable time: This is the time when collision is possible.



Pure aloha vulnerable time = 2 * frame transmission time(T_t)

Throughput in pure Aloha:

Let us assume G = Average number of frame generated during one frame transmitted time.
The throughput for pure ALOHA is $S = G \times e^{-2G}$

The maximum throughput S_{max} = 0.184 when G =(1/2).
G = 1/2, it means when 1/2 frame is transmitted in one T_t time or in other way 1 frame is transmitted in $2T_t$ time.

The maximum efficiency of Pure Aloha is very less due to the large number of collisions.

Q7 **Consider a 100-bits frame is transmitted by a pure Aloha network on a shared channel having, bandwidth of 100 kbps. Calculate the throughput if 250 frames/second is produced by the system(all station together)?**

Sol: Frame transmission time = 1msec

Now station is producing 250 frames in 1 sec, that means (¼) frame in 1 msec
The throughput for pure ALOHA is $S = G \times e^{-2G}$ which will give 0.152.
Now 250 * 0.152 = 38 frames will survive out of 250 frames.

Slotted Aloha:

- In slotted Aloha, data can be transmitted by any station at any given time slot, but the only condition is that a station has to begin its transmission at the start(beginning) of the time slot. A station has to wait until the starting of the next time slot in case it misses the starting of a given slot.
- In this, no station sends the data in the middle.

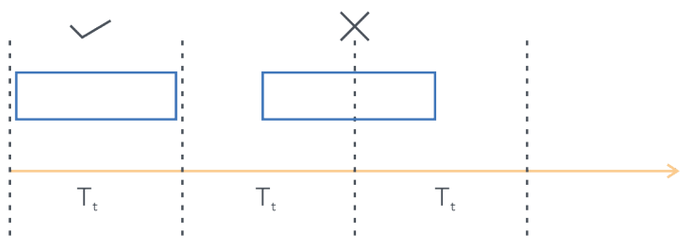


Fig. 3.42 Diagrammatic Representation of Data Transmission in Slotted Aloha

Vulnerable time = T_t

Throughput of slotted Aloha:
The average number of successful transmissions for slotted Aloha is $S = G \times e^{-G}$. The maximum throughput S_{max} is 0.368, when G = 1.

Rack Your Brain

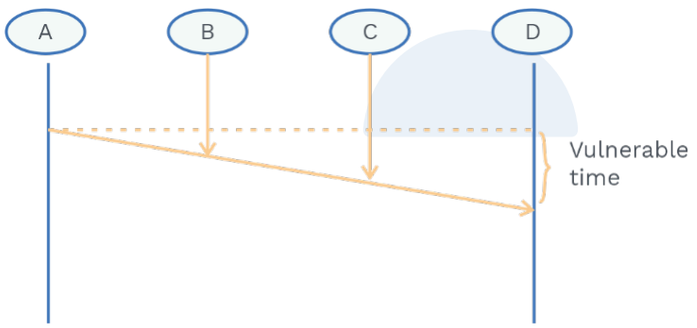
Consider a 100-bits frame is transmitted by a slotted Aloha network on a shared channel having bandwidth of 100 kbps. Calculate the throughput if the system (all stations together) produces 250 frames/second?

Comparison between slotted aloha and pure aloha:

Pure Aloha	Slotted Aloha
Station can send their data at any time	Can transmit only at the beginning of slot
Vulnerable time = $2 * T_t$	Vulnerable time = T_t
Throughput = $G \times e^{-2G}$	Throughput = $G \times e^{-G}$

Carrier sense multiple access protocols:

- It was developed to minimize the chance of collision and increase efficiency.
- It was based on the principle "Sense before transmit".
- The vulnerable time for CSMA is the propagation time Tp. This is the time needed for a signal to propagate from one end of the medium to the other.
- In the given diagram station A sends its data to station D in time T_p, when, station B wants to transmit its senses and similarly, C senses.



What should a station do when the channel is busy or idle?

There are 3 methods for this:
1-persistent method,
non persistent method,
and the p-persistent method

1-persistent method:

If the station finds the line idle, it sends its frame immediately,
If the channel is not idle, the station will continuously sense the channel.

Non persistent method:

If the station finds the channel idle, it sends its frame immediately.
Stations will wait for a random amount of time if they find the channel is busy, and when the channel is idle, it will send the frame again.

P persistent method:
In this method the station sends its frame with probability p, and it will not transmit with probability q = 1 - p. The station waits for the beginning of the next time slot and checks the line again. Now if the line is idle, it sends the frame with probability p and defers with probability q.

Carrier sense multiple access with collision detection:
Carrier sense multiple access with collision detection (CSMA/CD) elongate the CSMA to handle the collision.

Note:

Each station can sense the carrier only at its point of contact with the carrier.

Let us understand how a station senses the channel.
Station A wants to send data to station C, and station C wants to send data to station A.

It can be clearly observed that a collision is about to happen!! How to prevent this?
We need a restriction on the frame size.
Each station must transmit the data packet of size whose transmission delay is at least twice of its propagation delay.

Transmission delay >= 2 x Propagation delay
From this we can derive what will be the minimum size of the packet from 'B' to 'A'.

$$L >= 2 * T_p * B$$

Collision happens here when A is about to transmit, B can detect collision if it receives collision signal/jamming signal and it's still transmitting data.

$$T_t \geq T_{P(data)} + T_{P(jamming)}$$

$$\boxed{T_t \geq 2T_p}$$

Rack your Brain

a) What is the minimum packet length when T_p = 1msec and Bandwidth = 1Mbps
b) Guess the differences between Aloha and CSMA/CD
c) Is the throughput of CSMA/CD greater than Aloha?

Efficiency:

Useful time = Transmission delay of data packet = T_t
Total time = Time during collisions + Propagation delay of data packet + T_t
= c x 2 x T_p + T_p + T_t (where c = Number of contention slots).
Efficiency = useful time / total time
T_t /(c x 2 x T_p + T_p + T_t)
Analysis using probability gives the Average number of collisions before a successful transmission = e
Which leads to c = e
Now Efficiency = T_t /(e x 2 x T_p + T_p + T_t)

Note:

What is the average number of collisions before successful transmission?

P(success) = ${}^nC_1 \times p \times (1-p)^{n-1}$...1
In order to find maximum value we need to differentiate w.r.t. p
dP/dp = 0
On solving we get p = 1/n putting this value in (1) we get
Now $P(success)_{max} = (1-1/n)^{n-1}$
If there are large number of stations n –> ∞

$$= \lim_{n\to\infty}\left(1-\frac{1}{n}\right)^{n-1} = \frac{1}{e}$$

Number of times that a station request before successfully transmitting the data packet,

$$= 1/P_{max} = 1/(1/e) = e$$

Efficiency of standard ethernet = 1/ (1 + 6.44a) where a = T_p / T_t

Points:

- It is used in Wired LAN (802.3)
- Probability of successful transmission = ${}^{n}C_{1} \times p \times (1-p)^{n-1}$

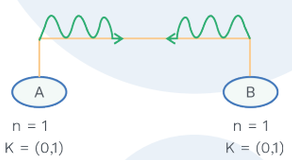
Let us understand; what is Backoff time?

In CSMA / CD protocol, after the occurrence of a collision, the station waits for some random backoff time and then retransmits, and this waiting time for which the station waits before retransmitting the data is called backoff time.

Backoff time = k * timeslot (station chooses number K and timeslot is one round trip time).

Note:

If collision is happening for nth time then station will choose a random number **k** from ($0, 2^{n} - 1$)



Possibilities:

A	B (Description)
0	0 Both station will collide
0	1 Station A will win
1	0 Station B will win
1	1 Both station will collide

Concept Building Exercise

When A = 0 and B = 1, why station A won ! How do you conclude?

Let's see scenario for A = 1 and B = 0

Backoff time for A = 1 * RTT (A has to wait for 1 RTT)

Backoff time for B = 0 *RTT (B does not have to wait)

Note:

In this algorithm, Backoff time increases exponentially
And collision probability decreases exponentially
It shows a capture effect (if the host wins the collisions for one time, it is going to win more numbers of times).

Q8 **Consider a CSMA/CD network having a bandwidth of 10 Mbps, and the minimum frame size is 512 bits for the correct operation of the collision detection process. What will be the minimum frame size when tha bandwidth is increased to 100 Mbps by keeping the propagation delay constant?**

Sol: Frame size = K * data rate

Data rate = 10 Mbps then minimum frame size = 512 bits

Data rate = 100 Mbps then minimum frame size = 5120 bits

Note:

If bandwidth increases, frame size can also increase.

Previous Years' Question

Q. A network with CSMA/CD protocol in the MAC layer is running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 2 x 10^8 m/sec. The minimum frame size for this network should be:

a) 10000 bits **b)** 10000 bytes
c) 5000 bits **d)** 5000 bytes

Sol: a) **(GATE-2005)**

Previous Years' Question

Q. Consider a network using the pure ALOHA medium access control protocol, where each frame is of length 1,000 bits. The channel transmission rate is 1 Mbps (10^6 bits per second). The aggregate number of transmissions across all the nodes (including new frame transmissions and retransmitted frames due to collisions) is modelled as a Poisson process with a rate of 1,000 frames per second. Throughput is defined as the average number of frames successfully transmitted per second. The throughput of the network (rounded to the nearest integer) is _____

Sol: 135 **(GATE-2021)**

Controlled access protocol;

Which station will send the packet ! this is done by taking the information from all other station.

In this protocol basically 3 methods are used:

- Polling
- Reservation
- Token Passing

Polling:

There is a Centralized controller which polls 'stations', and gives them an opportunity to send one packet.

All the data which needs to exchange must go through the controller.

Disadvantage in polling:

There is a high overhead of polling messages.

Stations have to depend on controller.

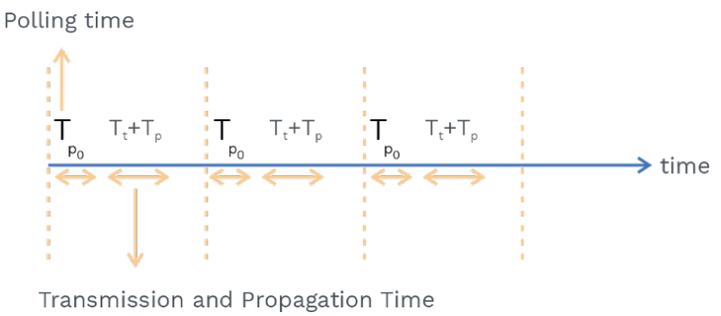


Fig. 3.6 Data Transmission in Polling

Efficiency = Useful time / total time
Useful time = T_t
Total time = $T_{po} + T_p + T_t$
$= T_t / (T_{po} + T_p + T_t)$

Reservation:
Station that wants to send data needs to make a reservation.
Time is divided into intervals.
In each interval, a reservation frame precedes the data frames sent in that interval.

In the above figure there are 3 slots made if 3 stations want to send data.
In the first interval, only station 1, and station 3 made a reservation and in the second interval.
Only station 1 made a reservation.

Token passing:
Stations are connected in the form of ring.
Access is granted through the token.
when the station receives the token, it can send a frame (if it has frame) before it passes the token to the next station; if the station does not have a frame simply, it will pass the token to the next station.

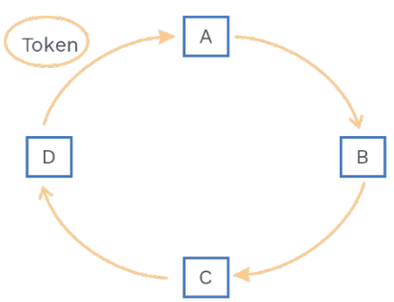


Fig. 3.7 Diagrammatic Representation of Token Ring

Early token reinsertion
Efficiency = 1/(1 + a/N) and
Delayed token reinsertion
Efficiency = 1/(1+{a(1 + 1/N)})

Channelization protocol:
Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code between different stations.

Time division multiple access:
Time of the link is divided into fixed-size intervals called time slots or time slices.
Each station can transmit the data in its time slot only.
Let's say there are 3 stations A,B and C.

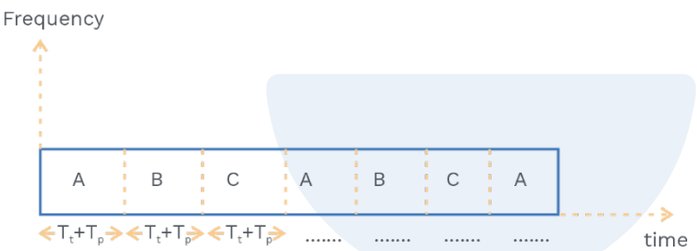


Fig. 3.8 Diagrammatic Representation of TDMA

Slots are given on the basis of Round Robin
Efficiency = Useful time/ total time

$$T_t / (T_t + T_p)$$

Disadvantage:
If the station does not want to send the frame, then also time slot has given, which eventually leads to bad efficiency.

Frequency division multiple access:
In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.
Each station has an assigned separate channel.

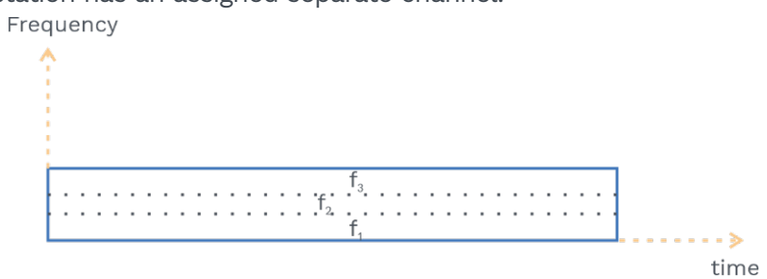


Fig. 3.9 Diagrammatic Representation of FDMA

Rack Your Brain

Give the difference between FDMA and FDM !

Wired Lan: Ethernet:
Ethernet is one of the standard LAN technologies used for wired LANs and It is defined under IEEE 802.3.
Till now we have seen Data link layer in two parts.
First one is Data Link Control, and the Second one is Medium Access Control.

But there is only one MAC sublayer in standard ethernet.
Points:

- Topology used is Bus.
- Access control method used is CSMA/CD.
- Encoding Technique used is Manchester.

Let us see Frame format of Ethernet

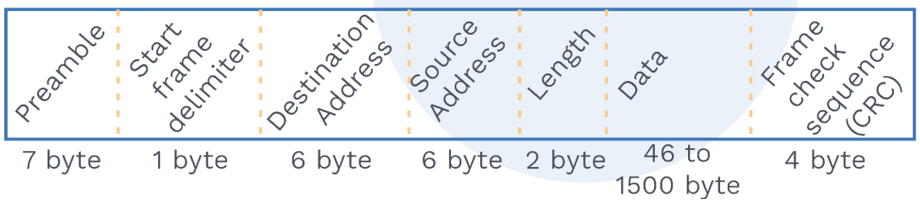


Fig. 3.10 Ethernet Frame Format

Preamble:

a) It contains 7 bytes.
b) It has 0 and 1 in alternate position.
c) It is actually added at the physical layer.
d) It enables frame to synchronize between sender and receiver.

SFD:
It contains 1 byte: 10101011.
SFD tells the station that this is the last chance for synchronization. The last 2 bits are 11 and alerts the receiver that the next field is the destination address.

Destination address: It is a 6 byte field.
It contains the MAC address (physical address) of the destination.

Source address: It is a 6 byte field.
It contains the MAC address (physical address) of the source.

Length: It is a 2 byte field.
Length field describes the number of bytes in the data field.

Note:

The maximum value that can be accommodated in this field = $2^{16} - 1 = 65535$ bytes, but the maximum amount of data that can be sent in an Ethernet frame is 1500 bytes.

Note:

Minimum frame length = 64 bytes
Maximum frame length = 1518 bytes

Data: This field contains actual data also called payload field.
Minimum bytes in data field = 46 bytes.
Maximum bytes in data field = 1500 bytes.

CRC: It has 4 bytes.
This field is used for error detection.

Rack Your Brain

Why 65535 bytes is not allowed in ethernet frame?

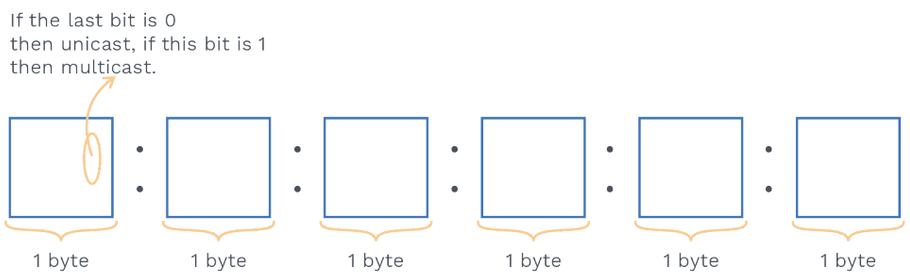
Addressing in ethernet:
Each station has NIC (Network interface card) which has its own physical address.

We already know physical address has 6 bytes.
It is written in hexadecimal code with colon between bytes.
There are 3 types of addresses:

- Unicast
- Multicast
- Broadcast address

Note:

The least significant bit of the first byte defines the type of address. If the bit is 0, the address is unicast; otherwise, it is multicast.



Source address is always unicast.
Destination address can be unicast, multicast or broadcast
The broadcast destination address is a special case of the multicast address in which all bits are 1.

Rack your Brain

Q.1 Define the type of the following destination addresses:
- **a)** 5A:40:20:31:2O:2A
- **b)** 46:60:6B:7E:78:8E
- **c)** FF:FF:FF:FF:FF:FF

Q.2 Why source address cannot be multicast or broadcast?

SOLVED EXAMPLES

Q9 **Compare the data rates for Standard Ethernet, Fast Ethernet, Gigabit Ethernet,
and Ten-Gigabit Ethernet?**

Sol: Standard Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1 Gbps, Ten-Gigabit Ethernet: 10 Gbps

Q10 **If an Ethernet destination address is 09:02:02:03:04:05, what is the type of the address (unicast, multicast, or broadcast)? Can this address be a source address?**

Sol: The first byte; i.e 09 => 00001001, the last bit is 1; therefore it is a multicast. No, this address cannot be a source address because a source address cannot be a multicast.

Q11 **The efficiency of Ethernet increases when propagation delay is low, and transmission delay is high. The following statement is true/false.**

Sol: This statement is true because, $E = 1/(1 + 6.44a)$

Where, $a = T_p/T_t$

Q12 **Determine the ratio of the smallest useful data that a frame can carry through ethernet to the largest ethernet frame size?**

Sol: Smallest data size in ethernet frame = 46

Largest frame size = 1518

46/1518

Q13 **Which of the following is/are false about CSMA/CD? (MSQ)**

a) IEEE 802.11 wireless LAN runs CSMA/CD protocol.
b) CSMA/CD is useful for system like ATM
c) Ethernet is based on CSMA/CD protocol
d) CSMA/CD is not suitable for high propagation delay network

Sol: **a,b**

a) IEEE 802.11 wireless LAN runs CSMA/CA protocol.
b) CSMA/CD is not useful for system like ATM because ATM uses interactive methods

Connecting devices:

- Operate at physical layer: Active Hub or repeater
- Operate at physical and data link layer: bridges or 2 layer switches
- Operate at physical, data link layer and etwork layer: Routers or 3 layer switches
  Operate at all five layer: Gateways

Repeater:

- It receives the signal at physical layer and before the signal becomes too weak it regenerates the original bit pattern
- A repeater regenerates the signal. It does not amplify signal.

Previous Years' Question

Q) Suppose the round trip propagation delay for a 10 Mbps Ethernet having 48-bit jamming signal is 46.4 μs. The minimum frame size is:

a) 94 **b)** 416
c) 464 **d)** 512

Sol: d) **(GATE-2005)**

- A repeater connects two **segments** of LAN.
- A repeater forwards every frame, it has no filtering capability (Collision domain remain).

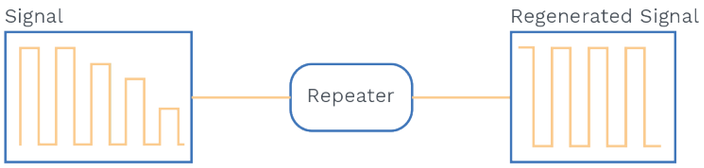


fig 3.11 Regeneration of Signal Using Repeater

Rack your Brain

Difference between repeater and amplifier.

Note:

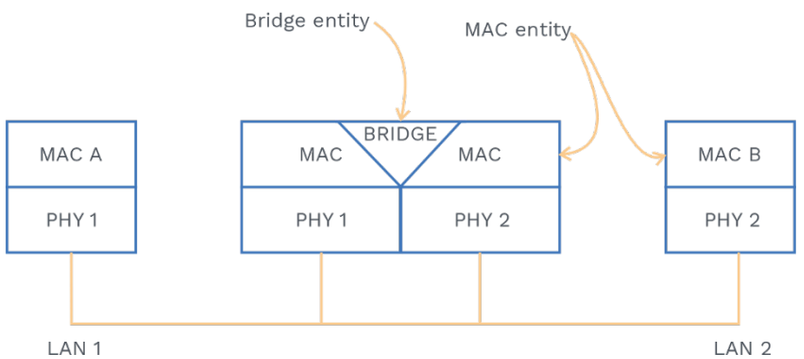
A repeater is not used for connecting two LANs of different protocols.

Active hub:

It is a multiport repeater.
Hubs can also be used to create multiple levels of hierarchy.
Hubs cannot filter data (collision domain remain same).

Bridges:

It works at the physical layer and data link layer.
At the physical layer, it regenerates the signal.
At the data link layer, it can check the MAC address contained in the frame.
It has filtering capability (because it can check the destination MAC address and decide whether the frame has to forward or drop).



Transparent bridge:

- A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. It implies that no reconfiguration is required if a bridge is added/deleted from the system.

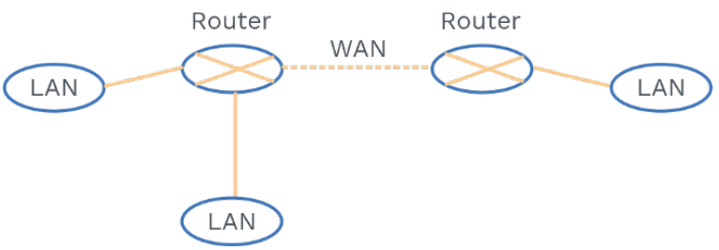
- It works on transparent and learning process.
- Transparent bridges work fine until there is a redundant bridge which causes a **looping problem.**

Solution of looping problem:
Spanning tree: To prevent the loop path and proper working of forwarding and learning process, there must be only one path between any pair of bridges and that path is maintained using the **Spanning tree algorithm.**

Source routing bridges:
- Here the routing is performed by the source host.
- The frame contains not only the source and destination addresses but also the addresses of all bridges to be visited.
- Source gets these bridge addresses through the exchange of special frames.

Two layer switches:
- It performs at the physical and data link layer.
- A two-layer switch is a bridge having many ports, and it is designed such that it gives a faster(better) performance.
- It takes filtering decisions on the basis of the MAC address of the frame it received. (Each port has a separate collision domain).
- Here, the ports are provided with a buffer.

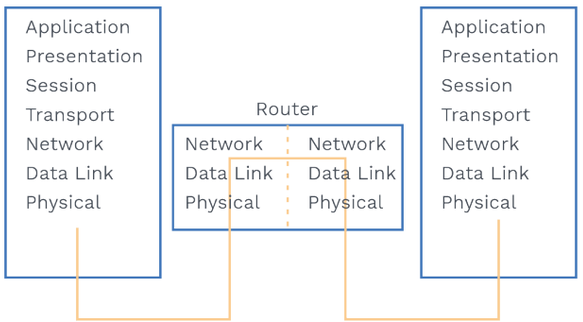
Router:
- It is used to link two dissimilar LAN.
- It is a 3 layer device which routes the packets based on logical address.
- Routing table is dynamic and updated using a routing protocol.



Three layer switch:
- A three-layer switch is a router, which is faster and more sophisticated.
- The switching fabric in a three-layer switch allows faster table lookup and forwarding.
- It can separate broadcast domain.

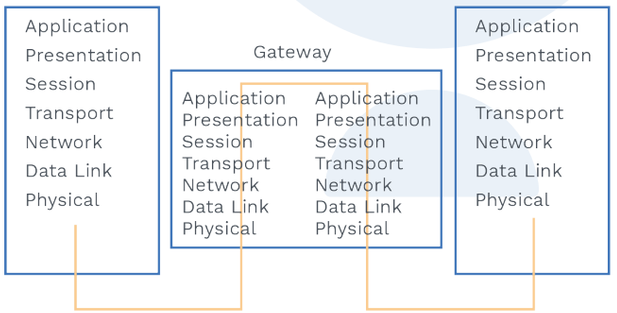
How does a communication through a router happens?

Router can inspect through network layer:



Gateway:

- A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model.
- Gateways can provide security.
- It is used to filter unwanted application-layer messages.



Concept Building Exercise

Q. Which of the following statements are not correct differences between a switch and a hub? *[MSQ]*

a) Switch transmits a signal to all the devices connected to it, hub transmits a signal only to the intended port.

b) Switch works in the physical layer, the hub works at data-link layer

c) Switch works at layer 2 while hub works at layer 1

d) Switch is a smart device, whereas hub is a dumb device

Sol: a) and b)

Hub Transmits a signal to all the devices connected to it; switch transmits a signal only to the intended port

Hub works in the physical layer; Switch works at data-link layer

Previous Years' Question

Q. Which of the following is NOT true with respect to a transparent bridge and a router?

a) Both bridge and router selectively forward data packets

b) A bridge uses IP addresses while a router uses MAC addresses

c) A bridge builds up its routing table by inspecting incoming packets

d) A router can connect between a LAN and a WAN

Sol: b) **(GATE-2004)**

Chapter summary:

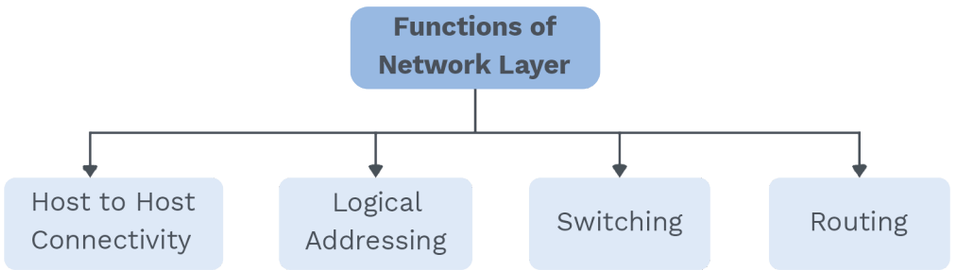
- **Data link layer:** Two major function
  1) Data Link Control
  2) Medium Access Control
- Data Link Control performs Framing, Error Control, Flow Control.
- Medium Access Control performs Access Control and Physical Addressing.
- There are two types of framing
  1) Fixed Size Framing
  2) Variable Size Framing
- Error detection can be done by Parity checking, CRC and Checksum.
- Some rules for generating the generator polynomial
  Rule 1: It should not be divisible by x.
  Rule 2: It should be divisible by x+1.
- **Flow control:**
  Set of procedures used to restrict the amount of data that the sender can send before waiting for an acknowledgement.
  Flow control can be done in Noiseless channels and noisy channel.
  In Noiseless channel: Stop and Wait
  In Noisy channel: Stop and Wait ARQ
  Go back N ARQ
  Selective repeat ARQ
- Available Sequence number >= Sender window Size + Receiver window Size

- Stop and Wait ARQ = Stop and Wait + Time Out Timer + Sequence number in Data Packet + Sequence number in ACK Packet.
- Maximum Available Sequence Number in GBN >= N+1.
- Maximum Available Sequence Number in SR >= N+N.
- Maximum throughput of pure Aloha is 18.4%.
- Maximum throughput of slotted Aloha is 36.8%.
- Frame transmission delay in CSMA/CD must be twice than propagation delay.
- Minimum frame length = 64 bytes
- Maximum frame length = 1518 bytes

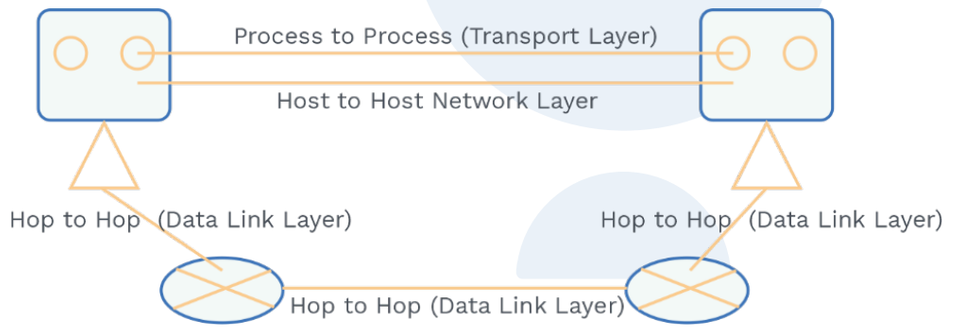
4 Network Layer

4.1 NETWORK LAYER

Across multiple links, the network layer is responsible for source to destination delivery. Is the data link layer not enough? No, as it works on the same links.



Host to Host Connectivity



Logical addressing:

Now for implementation, logical address is IP addresses having 32 bit number which is globally unique, and physical address are MAC address having 48 bit which is also globally unique.

Let's talk about IPV4 address:

It is 32 bit long and unique

What do you understand by unique here!

This means two devices on the internet can never have the same address at the same time.

Rack Your Brain

a) Can IP be used as Physical Address?
b) Can MAC be used as Logical Address?

Note:

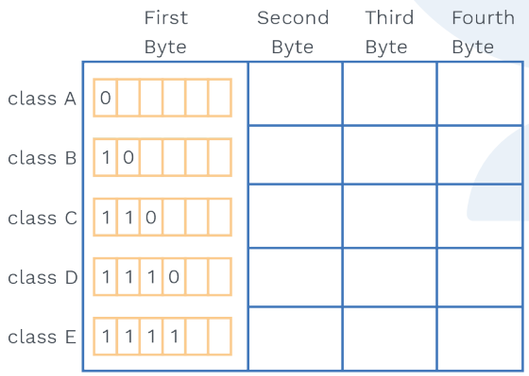
For N bit, there can be 2^N values.

For 32 bit address, we have 2^{32} address space (4,294,967,296).

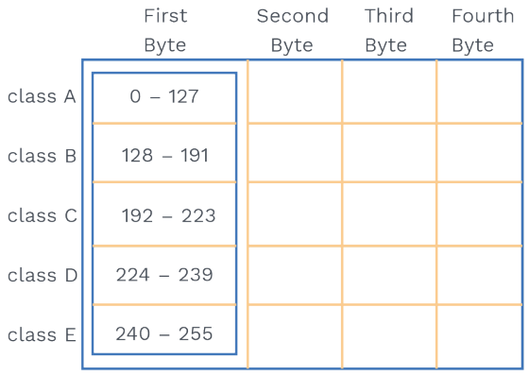
Notation:
Binary notation – 10000001.10000011.10000010.00000010
Dotted decimal notation – 129 . 131 . 130 . 2

Classful addressing:
In classful addressing, the address space is divided into five classes: A, B, C, D and E.

a) How each class is distributed when it is represented in Binary?
When the address is given in binary notation, the first few bits can signify the class of the address.
Let's say if the starting bits are 110... then it is of class C, and if the address starts from 1110... then it is of class D.
Have a deep look at the below diagram:



b) How each class distributed when it is represented in dotted decimal?
When the address is given in decimal–dotted notation, the first byte defines the class.



Rack Your Brain

a) Change the following binary notation into dotted decimal. 0000 0001.00000011.00001011.10101101
b) Change the following dotted decimal into binary notation. 1.3.11.173

Rack Your Brain

Identify, below IP address is of which class? 00000001.00000011.00001011.10101101

Rack Your Brain

The IP address below is of which class? 25.27.129.15

Now we will see what Net ID and Host ID are!
In IP address, each of 4 bytes is called octets, where each octet has 8 bits. The octets are divided into 2 components – Net ID and Host ID.

Class A, B and C have Net ID and Host ID, class D, and; class E does not have Net ID and Host ID.

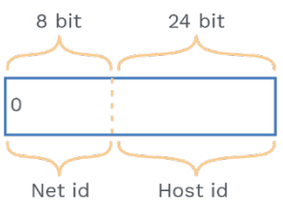
Note:

Net ID: Network IDs are IP addresses of the network and are used to identify the network.

Host ID: Host IDs are the IP address of the host and is used to identify the host within the network.

In Class A, 1 byte denotes Net ID and remaining 3 bytes are Host IDs.
In Class B, 2 bytes denote Net ID and remaining 2 bytes are Host IDs.
In Class C, 3 bytes denote Net ID and remaining 1 bytes are Host IDs.
In Class D, there is no Net ID and Host ID.
In Class E, there is no Net ID and Host ID.
Let's take a look at individual class.

Class A:



Rack Your Brain

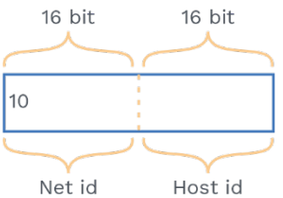
Why 31 bit is taken, why not 32 bit?

- Total number of possible IP addresses available in this class is number of networks * possible number of address in single network.
  $126 * (2^{24}) = 2113929216$
- Total number of networks available in this class is 2^7-2.
- Total number of hosts available in each network in this class is $2^{24}-2$.

Why did we subtract 2 from 2^7?

IP address 0.0.0.0 is reserved for broadcasting requirements and IP address 127.0.0.1 is reserved for loopback address used for software testing.

Class B:

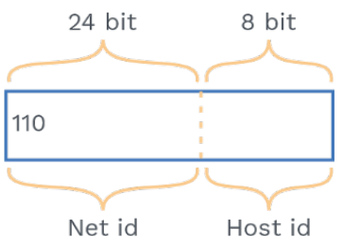


Rack Your Brain

Why 30 bit is taken, why not 32 bit?

- Total number of possible IP addresses available in this class is 2^{30}.
- Total number of networks available in this class is 2^{14}.
- Total number of hosts available in each network in this class is $2^{16}-2$.

Class C:



- Total number of possible IP addresses available in this class is 2^{29}.
- Total number of networks available in this class is 2^{21}.
- Total number of hosts available in each network in this class is $2^{8}-2$.

Class D:

- Total number of possible IP addresses available in this class is 2^{28}.
- Class D is reserved for multicasting and there is no need to extract the host address from the IP address in multicasting.

Class E:

- Total number of possible IP addresses available in this class is 2^{28}.
- Class E is reserved for future purposes.

Mask:
It is a 32 bit number made of contiguous 1 followed by contiguous 0. It will help to find the Net ID and Host ID.

Let's say the mask for a class A address has eight 1's, which means the first 8 bits of any address in class A define the Net ID, and the next 24 bits define the Host ID.

Default masks for classes A, B and C are given in table.

Summary of what we have read till now is given in table below:

Class of IP Address	Total Number of IP Addresses	Number of Networks Available	Host Per Network	Default Subnet Mask
Class A	126 * (2^{24})	2^7–2	2^{24}–2	255.0.0.0
Class B	2^{30}	2^{14}	2^{16}–2	255.255.0.0
Class C	2^{29}	2^{21}	2^8–2	255.255.255.0
Class D	2^{28}			
Class E	2^{28}			

Note:
Blank spaces are not defined.

Concept Building Exercise

Q.1 Why are we subtracting 2 in Hosts per network?
Sol: The reason is when all Host ID bits are 0, it represents the Network ID for the network, and when all Host ID bits are 1, it represents the broadcast address.

Q.2 How can we obtain the IP address of the network?
Sol: For any IP address, its network ID can be obtained by making all the Host bit 0.

Q.3 For any Given IP address, How can we obtain Direct broadcast address and Limited broadcast address?
Sol: Direct Broadcast address -> make all the Host bit 1
Limited broadcast address -> make all the bit (Net ID and Host ID) as 1

Q.4 For the given IP address 4.5.6.7, what will be the Class, Network IP address, DBA and LBA?
Sol: Class is A because it is in the range (1–126)
Network IP address is 4.0.0.0
Direct Broadcast address is 4.255.255.255
Limited Broadcast address is 255.255.255.255

Concept Building Exercise

Q.5 In performing a Loopback address, if the given Ip address is 4.5.6.7, then what will be the source and destination IP?

Sol: Source address 4.5.6.7
Destination address 127.0.0.1

Q.6 What is the default mask for 171.10.55.10?

Sol: Given IP address belongs to B, hence default subnet mask is 255.255.0.0.

Q.7 Which of the following can be used as both Source as well as destination IP?

a) 191.2.255.255 **b)** 127.0.0.1
c) 255.255.255.255 **d)** 18.18.18.18

Ans. d)

Sol: **a)** 191.2.255.255 is DBA
b) 127.0.0.1 is Loopback address
c) 255.255.255.255 is Limited broadcast address
d) 18.18.18.18 can be used as Source as well as destination IP

Note:
In classful addressing, class A, B and C are used for reserved addresses, class D is used for multicast, and class E is used for future purpose addresses.

Limitation of classful addressing:
In classful addressing, we are using fixed classes for special purposes which is not efficient in today's scenario like Class C is used for the midsize organization, but it is not effective as the only Host available per network is 2^8.

Rack Your Brain

For the given IP address 191.5.26.7 what will be the Class, Network IP address, Direct broadcast address and Limited broadcast address?

Classless addressing:

- Classless addressing is used now, and classful has become obsolete.
- In classless addressing, ISP (Internet service provider) grants IP addresses based on requirement on the number of customers needed.
- It is an improved version of classful addressing and is also known as CIDR (classless interdomain routing).

How ISP grants IP addresses?
There are 3 rules for CIDR block creation:
Rule 1: All the IP addresses must be contiguous in a block.
Rule 2: A block must be in power of 2 (1,2,4,8....).
Rule 3: The first address is evenly divisible with number of address.

PRACTICE QUESTIONS

Q1 **Block of 4 addresses can be assigned to an organisation having an IP 205.26.24.8 Is it possible?**

Sol: According to CIDR,
Rule 1: All the IP addresses must be contiguous in a block.

205.26.24.8, 205.26.24.9, 205.26.24.10, 205.26.24.11

Rule 2: A block must be in the power of 2.
Yes, 4 is power of 2
Rule 3: The first address is evenly divisible by a number of address.
First address is 205.26.24.8 which is divisible by 4 (block size).

Q2 **What does a CIDR IP address look like?**

Sol: p.q.r.s/t
t is used as identifier for network bits.
32-t bits used as identifier for Host bits.

Rack Your Brain

Q) What is the block address of 2.2.3.4/5?

Q3 **What do you understand by 192.4.5.6/16?**

Sol: Let's first write it in binary.

11000000. 00000100. 00000101. 00000110/16

First 16 bits represents network id.
11000000. 00000100. 0. 0 (Network ID)
As you see, we got the network address by keeping 16 bits as it is and making 32 - 16 bits 0.
Remaining 16 bits are used for the identification of the Host id, in which one of the host is given IP address i.e 192.4.5.6.

Q4 **Given a CIDR representation 122.10.5.8 / 29. Find the range of an IP addresses in CIDR representation?**

Sol: Range means the block which is provided in CIDR.
Octet having decimal value, in binary address will be 122.10.5.00001000 / 29.
Make 29 bits as network address 122.10.5.00001000 (First address of block).
Make remaining bits 32-29 as 1.122.10.5.00001111 (Last address of block).

Q5 **Following IP addresses are given, can you apply CIDR aggregation?**
188.67.4.0/24, 188.67.5.0/24, 188.67.6.0/24, 188.67.7.0/24

Sol: 188.67.00000100.0 / 24
188.67.4.0 Number of hosts possible in one network is 2^8
Rule 1: Is the given block contiguous ! Yes.
Rule 2: Is the size of the block is in power of 2 !! yes.
Total number of host possible is $2^8 + 2^8 + 2^8 + 2^8 = 2^{10}$
Which is in the power of 10
Rule 3: The address of the first block is evenly divisible by the size of the block !!!
188 .67.00000100.0 when divided by 2^{10} last 10 significant bits are 0.
Hence yes given block can follow CIDR aggregation.

Rack Your Brain

Q) Is the following range of IP addresses following CIDR rules 188.67.3.0/24, 188.67.5.0/24, 188.67.6.0/24, 188.67.7.0/24?

Note:
The first address in a block is normally not assigned to any device, it is used as the network address that represents the organization to the rest of the world.

Subnetting:
An organisation that is generated a large block of address may need to break into small networks (Subnets) On a higher level i.e. from outside the organisation, it works as a signal network, but internally, it may have many networks.

Subnetting is the process of dividing a network into multiple sub networks.

We can divide subnetting into two parts:

Classful Subnetting (Fixed length subnetting)

Classless Subnetting (Variable length subnetting)

Lets see the difference between Classful subnetting and classless subnetting.

Rack Your Brain

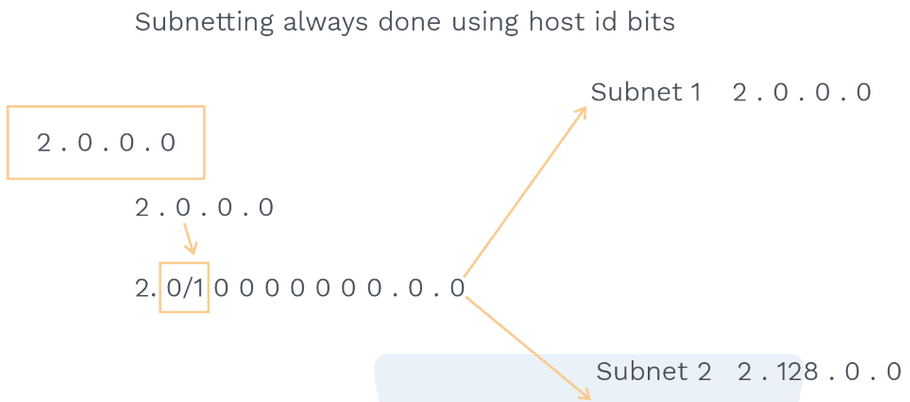
Q) Can you guess the advantages of subnetting.

Classful Subnetting	Classless Subnetting
Same size subnets	Different size subnet
Subnets have equal number of host	Unequal number of host
All the subnet have same mask	Each subnet have different mask

Table 4.1 Classful Subnetting vs Classless Subnetting

Lets say we have a single big network having IP 2.0.0.0.

We have to make 2 subnet?
Take one bit from the host id, from one bit we can make two subnet.



- Lets see inside First Subnet i.e Subnet 1.
  Subnet Id of Subnet 1 = 2.0.0.0, this is the Net ID of the Big network also.
  DBA of subnet 1 = 2.127.255.255
  LBA of subnet 1 = 255.255.255.255
- Total number of IP addresses possible in Subnet 1 = 2^{23}. Why have we taken 23 not 24 bits? one bit is used for subnetting from host part.
- Total number of hosts that can be configured = $2^{23} - 2$.
- Subnet Mask of this subnet = 255.128.0.0
- Range of subnet 1 = 2.0.0.0 to 2.127.255.255 !! Why have we stopped at 127 not 255.
- Since subnet 1 as taken 0 bit on MSB see binary notation of last octet.
  00000010.0000000.0000000.0000000 to 00000010.01111111.11111111.11111111

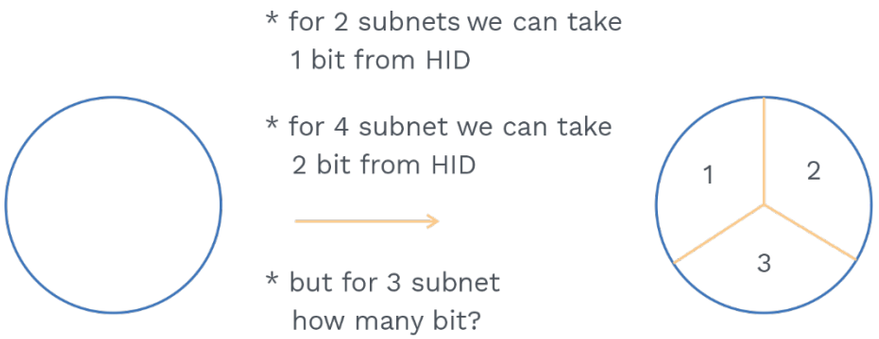
Lets see inside Subnet 2.

- Subnet Id of Subnet 2 = 2.128.0.0
- DBA of subnet 2 = 2.255.255.255. this is the DBA of entire network also.
  LBA of subnet 2 = 255.255.255.255
- Total number of IP addresses possible in Subnet 2 = 2^{23}. Why have we taken 23 not 24 bits? One bit is used for subnetting from host part.
- Total number of hosts that can be configured = 2^{23} - 2.
- Subnet Mask of this subnet = 255.128.0.0
- Range of subnet 2 = 2.128.0.0 to 2.255.255.255.
- Since subnet 2 as taken 1 bit on MSB see binary notation of last octet.
  00000010.1000000.0000000.0000000 to 0000010.1111111.11111111.11111111

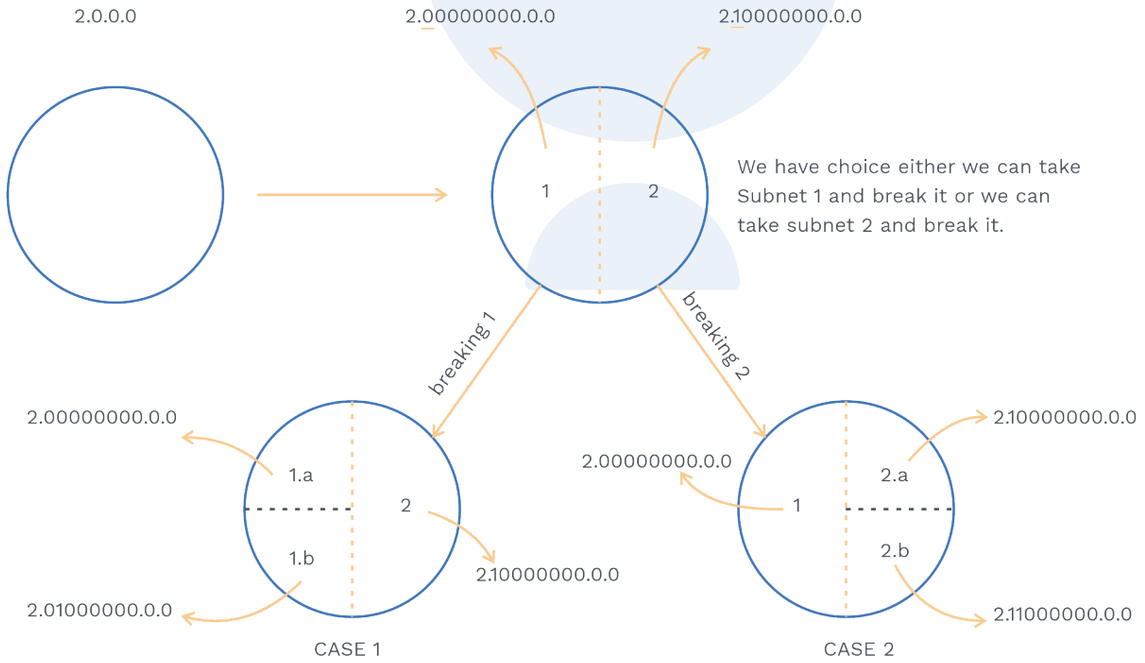
Rack Your Brain

Can you divide the network having IP address 2.0.0.0 into 4 Subnet?

We want, to divide this big network having IP address into 3 small networks!
Lets see



For 3 subnet also we have to take 2 bits; see the figure below



3 Subnet having Possible IP address using,

Case 1:

2.0.0.0

2.64.0.0

2.128.0.0

Case 2:

2.0.0.0

2.128.0.0

2.192.0.0

Previous Years' Question

Q) An organization requires a range of IP address to assign one to each of its 1500 computers. The organization has approached an Internet Service Provider (ISP) for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17. The ISP wants to assign an address space to the organization, which will minimize the number of routing entries in the ISP's router using route aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one of the organization?

i) 202.61.84.0/21 **ii)** (202.61.104.0/21

iii) 202.61.64.0/21 **iv)** 202.61.144.0/21

a) I and II only **b)** II and III only

c) III and IV only **d)** I and IV only

Sol: b) **(GATE-2020)**

Let's see how address allocation is done?

Responsibility of address allocation is taken care by ICANA (Internet Corporation for Assigned Names and Addresses). ICANA gives a block of addresses to ISP; Now it is the responsibility of ISP to divide the block of address into sub-blocks;

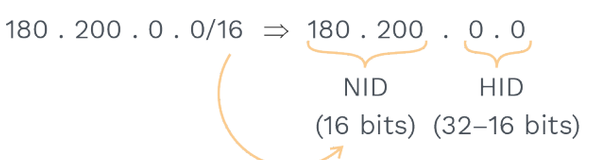
Standard example of subnetting in CIDR

Example 1: Suppose ISP grants a block of address starting with 180.200.0.0/16 to Unacademy. Now Unacademy wants to distribute this address into two teams, the names of the teams are NEET. GATE.

I) NEET has 32 teams and each team needs 128 address.

II) GATE has 64 teams and each team needs 64 address.

Sol:



Q6 **How many possible Host addresses does the Unacademy block have?**

Sol: 16 bits are available for address; therefore, 2^{16} addresses are possible but first and the last IP should not be assigned to any host therefore 2^{16} - 2 Hosts can be configured.

Since the NEET team wants 2^{12} and the GATE team wants 2^{12}.

combinedly need 2^{13} address. i.e 8192 address.

Total Available address are 2^{16}

S0, Available can satisfy the Needs of two teams.

given,

180.200.0.0/16

make, two subnets by borrowing a single bit from HID part 16 bits.

180.200.0/1 0000000.00000000

Suppose NEET team

180.200.00000000.00000000/17 → start

180.200.01111111.11111111/17 → end

it has 32 teams each with 128 address requirements.

for 32 teams take 5 bits.

180.200.0xxxxx00.00000000/22

180.200.00000000.00000000/22 -starts

180.200.01111100.00000000/22 -End

suppose GATE team.

180.200.10000000.00000000/17 -- start

180.200.11111111.11111111/17 --end

it has 64 teams with each 64-address requirement.

for 64 teams take 6 bits.

180.200.1xxxxxx0.00000000/23

180.200.10000000.00000000/23 –starts

180.200.11111110.00000000/23 --ends

Rack Your Brain

How many total addresses are present in the NEET team?

Example 2: A subnet mask 255.255.192.0.0 belongs to class B.
How to find the number of subnets in this subnet mask.

NID

11111111 . 11111111 . 11 000000 . 00000000

SID

No. of bits in Subnet = 2

Total number of subnet possible = $2^2 = 4$

How to find the number of hosts in each Subnet?

NID

11111111 . 11111111 . 11 000000 . 00000000

SID HID

14 Host id bits → 2^{14} address for each subnet

Since 1st and last address are not used

$\therefore 2^{14} - 2$ address possible

Example 3: A subnet mask 255.255.0.0 belongs to class A.
How to find number of subnets in this subnet mask.
Class A net id has 8 bits.
Given Subnet mask has 16 nits.
Number of subnet bit = 16 - 8 = 8 bits (see below figure for more information).

11111111 . 11111111 . 00000000 . 00000000

for class A → 11111111 . 00000000 . 00000000 . 00000000 (NID)

No. of subnet bit = $16 - 8 \Rightarrow 8$

Possible no. of subnet $\Rightarrow 2^8 \Rightarrow 256$

How to find the number of subnets if subnet mask 255.255.0.0 belongs to class B.

for class B → 11111111 . 11111111 . 00000000 . 00000000

No. of subnet bit = $16 - 16 \Rightarrow 0$

Possible no. of subnet $\Rightarrow 2^0 \Rightarrow 1$

How to find the number of subnets if subnet mask 255.255.0.0 belongs to class C.

for class C ⟶ 11111111 . 11111111 . 00000000 . 00000000

No. of subnet bit = Not possible

Why is the subnet not possible in the above case!!
For Subnet Mask for class C (255.255.255.0), all 1's cover the given subnet mask (255.255.0.0). Hence there are no extra 1's which can be used in subnetting therefore, subnet is not possible.

Supernetting:
Combination of multiple networks into one single network by following some rules is Supernetting.
Rules for Supernetting:
Rule 1: All the IP addresses must be contiguous in a block.
Rule 2: A block must be in power of 2 (1,2,4,8....)
Rule 3: The first address is evenly divisible with number of address.

Concept Building Exercise

Q.8 Can we come up with a bigger network of given sub networks?
200.100.10.0
200.100.12.0
200.100.15.0
200.100.17.0

Sol: In this Even first rule is not followed, therefore we cannot perform supernetting.

Q.9 Let's make above subnetworks contiguous.
200.100.10.0
200.100.11.0
200.100.12.0
200.100.13.0

Sol: In this first and second rule is followed but third rule is not followed.
First address i.e 11001000.01100100.00001010.00000000.
Block size is 2^{10}
But first address is not divisible by 2^{10}; therefore cannot perform supernetting.

Network address translation:

a) With a shortage of available IP, there is a need for translation of addresses. NAT comes as a solution for this problem.

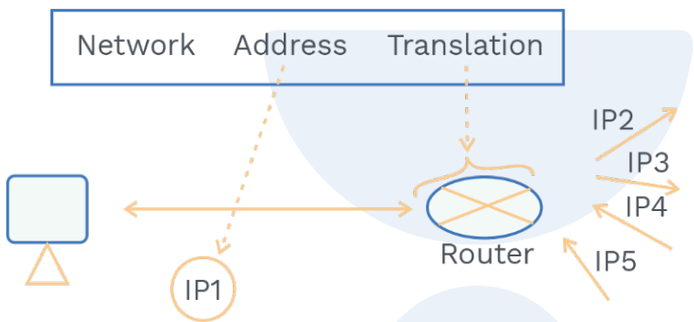
b) In the given diagram, IP_1 is used inside the organisation, while outside the organization it can be treated as IP_2, IP_3 depending upon the situation.

c) Inside the organization, IP_1 is called as Private IP.

d) Outside the organization, IP_2, IP_3, IP_4 and IP_5 are called public IP.

Rack Your Brain

Can prepladder distribute IP addresses to UPSC groups, in this UPSC group there are 511 teams, and each team needs 512 addresses.



How does a host get to know that a particular IP coming from the internet is it's or not?

Answer: It is the NAT table. A NAT table is responsible for mapping each private IP to its corresponding public IP.

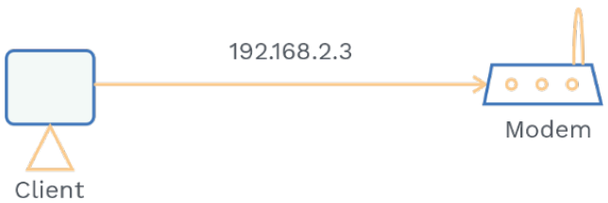
The Internet authorities have reserved three sets of addresses as private addresses.

Range	Total
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

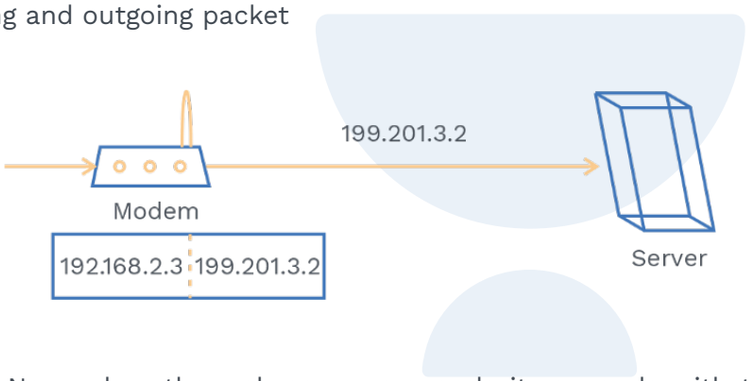
Table 4.2 Range of Private IP Addresses

Lets understand the NAT working:

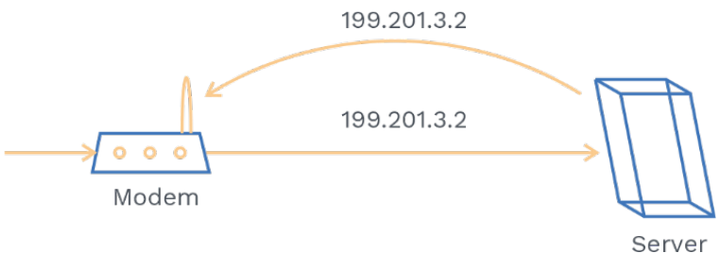
Step 1: Client send an IP packet to access point:



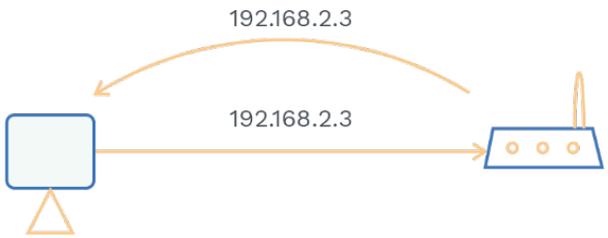
Step 2: Now the modem or access point sends the IP packet with a different IP address to the server. In addition to this, it records the mapping of the incoming and outgoing packet



Step 3: Now, when the web server responds it responds with the same public IP address.



Step 4: Access point gives back packet to the client.



Concept Building Exercise

Q.10 How will NAT use this mapping when the packet has source IP 192.168.22.1 returns from the server?
NAT Table:

Source IP	Destination IP	Source Port	Destination Port	NAT Port
192.168.22.1	200.200.1.1	2456	80	4000
192.168.11.2	201.102.1.1	1245	21	5000

Sol: It will look like this.
Source IP 200.200.1.1
Destination IP 192.168.22.1

Q.11 What types of devices can do NATing?
Sol: It can be Routers, Switch, even some servers also.

Note:

Despite having NAT, the depletion of IP address is not yet solved.
IPv4 does not provide better security features on its own.
By maintaining the basic functionality of IP addressing, IPV6 comes into the picture.
Let's discuss IPv6 addressing.

Points:

1) It is 128 bit long, hence a larger address space (IPV4 is 32 bit long).
2) IPv6 can be written in hexadecimal and binary notation.

Rack Your Brain

Q) Is NATing always preferable? If yes, then What will happen if some protocol changes the position of the IP address inside the IP packet? Do you still think it's always good!!

a) In Binary we denote IPv6 something like this

$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13}\ b_{14}\ b_{15}\ b_{16}.$
$b_{17}\ b_{18}$ ..... b_{32} .
$b_{33}\ b_{34}$ ..... b_{48} .
$b_{49}\ b_{50}$ ..... b_{64} .
$b_{65}\ b_{66}$ ..... b_{80} .
$b_{81}\ b_{82}$ ..... b_{96} .
$b_{97}\ b_{98}$ ..... b_{112} .
$b_{113}\ b_{114}$ ..... b_{128} .

Now if write IPv6 in binary every time, it would be long, hence we can use hexadecimal notation also.

b) In hexagonal notation, IPv6 looks like:

$h_1\ h_2\ h_3\ h_4 : h_5\ h_6\ h_7\ h_8 : h_9\ h_{10}\ h_{11}\ h_{12} : h_{13}\ h_{14}\ h_{15}\ h_{16} :$
$h_{17}\ h_{18}\ h_{19}\ h_{20} : h_{21}\ h_{22}\ h_{23}\ h_{24} : h_{25}\ h_{26}\ h_{27}\ h_{28} : h_{29}\ h_{30}\ h_{31}\ h_{32}$

There are 8 octets in hexadecimal notation, each octets is having 2 byte in length

1) Abbreviations in IPv6:

The need for abbreviations in IPv6 is that if we write in hexadecimals, then also there are some zeros which can be shortened. Hence we come up with rules which can reduce the size of hexadecimal notation illustrated below.

FDAB : 0017 : 000F : 0000 : 0000 : 0000 : A123 : 4567

Refined → FDAB : 17 : F : 0 : 0 : 0 : A123 : 4567

More Refined → FDAB : 17 : F : : A123 : 4567

Points from above illustration:

a) Leading zeros can be eliminated.
b) Lets say 0017 can be written as 17.
c) If there are consecutive zeros that can be replaced by a double colon.
d) Only leading zeros can be removed not the trailing zeros like 4120 cannot be written as 412.

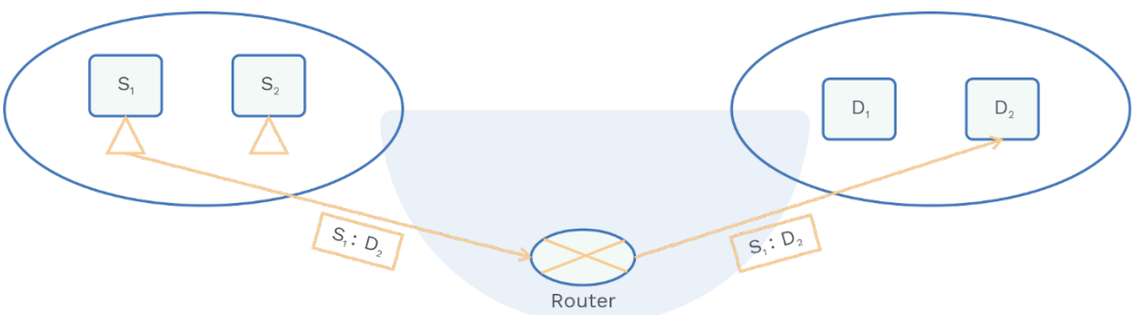
Rack Your Brain

Expand: 13:: 123: FFFF: ABCD: 1AC0

e) With a larger number of IP addresses, end to end connectivity can be easily done.
f) No broadcasting in IPv6, though multicast is there to communicate multiple host.
g) IPv6 has different types of addressing modes UNICAST, MULTICAST and ANYCAST.

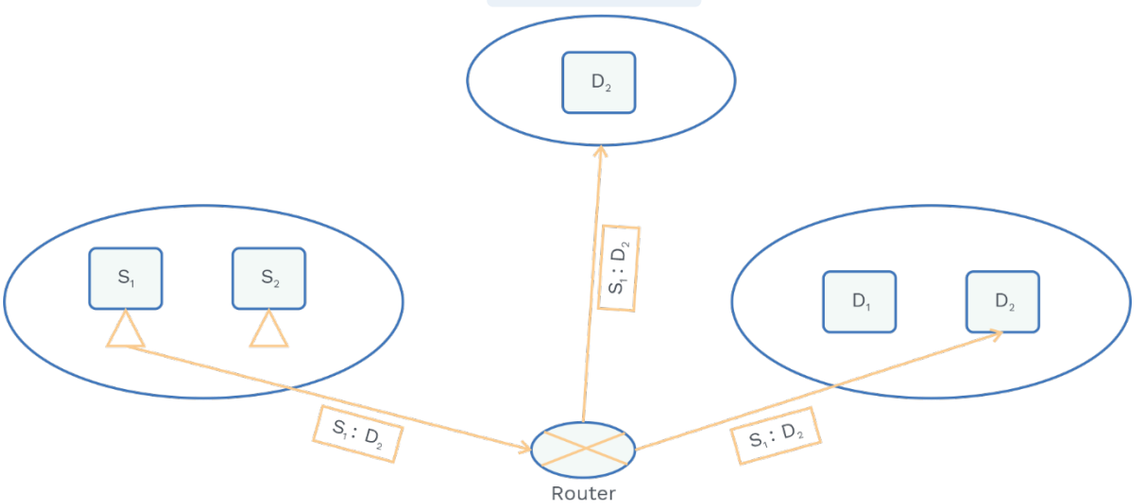
UNICAST:

- It is based on one source and one destination.
- In unicasting, the router forwards the received packet through only one of its interfaces.
- Forwarding a packet is done only one of its interfaces.
- Its a type of one one communication.



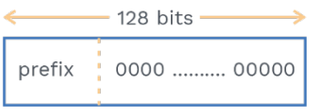
MULTICAST:

- There is one source and one group of destinations.
- In this source is unicast, but the group of destinations is multicast.



A multicast packet starts from S1 and sends it to groups D2 at all interfaces.
In multicasting, the router may forward the received packet through several of its interfaces.

ANYCAST:
Standard point from cisco: Assigning a unicast address to more than one interface makes a unicast address an anycast address.
Host which is closest to the Sender will receive the unicast message.



Concept Building Exercise:

Q.12 01000011.... patterns come as IPv4 packets, Can you tell if it is a valid pattern?
Sol: NO,
First 4 bit are version 0100
Next four bit are header length i.e 0011 it comes out as 3 * 4 = 12
Header length at least should be 20.

Q.13 Hogwarts has the block 15.0.0.0/8. Albus Dumbledore wants to create 400 fixed-length subnets.
a) Find the subnet mask.
b) Find the number of addresses in each subnet that can be assigned.
c) Find the first and last addresses in subnet.

Sol: **a)** Subnet mask:
Albus Dumbledore wants fixed length Subnet.
He needs 9 bits for 400 fixed length subnets.
Subnet mask will have 8+9 = 17 bits
It will look like 15.0.0.0/17
b) Number of possible address in each subnet that can be assigned.
2^{32-17} - 2 addresses will be assigned as a host in each subnet
c) First and last possible addresses in subnet 1 that can be assigned.
Assuming 15.0.0.0 is subnet 1
Now first possible address would be 15.0.0.1
Last possible address would be 15.0.127.254

Note:

1) In order to find the Subnet ID or number of Subnet, We have to know class ID or NID.
2) Even without knowing the class of network, we can find HID.

Example 1: Subnet mask = 255.255.255.128 and it is from class A.

Sol:
We know NID + SID = Total number of 1
HID = No of Zeros

Number of 1's is 25
NID in class A = 8 bits
SID = 17
Number of Subnet = 2^{17}

Number of 0's = 6
IP address = 2^6
Possible Host = 2^6 - 2

Example 2: What should be the value of n in a.b.c.d/n, when we want a block size as 2^{15}?

Sol: It should be 32 - 15 = 17
NID = 17 bits

Example 3: Can you mention all the IP addresses present in 10.1.5.0/30 block ?

Sol: It has 4 IP addresses

10.1.5.0/30

10.1.5.1/30

10.1.5.2/30

10.1.5.3/30

Note:
In above solution only 2 IP can be used as Host ID.

Previous Years' Question

Q) Every host in an IPv4 network has a 1–second resolution real–time clock with battery backup. Each host needs to generate up to 1000 unique identifiers per second. Assume that each host has a globally unique IPv4 address. Design a 50–bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around?

Sol: 256 **(GATE-2014)**

Special IP address chart and their meaning:

NID	HID	Description
✓	✓	Valid IP Address
✓	0'S	Network IP
✓	1'S	Directed Broadcast
1'S	1'S	LImited Broadcast
1'S	0'S	Subnet Mask
0'S	✓	Host within N/w
0'S	0'S	Host dont know IP
127	✓	Loop Back address

Need for network layer:
Since the data link layer was responsible for Hop to Hop delivery, there needs a mechanism which will take care of host to host delivery through routers.

You may think Host to Host delivery can also be done through a data link layer! yes, possible only when these two hosts share a single network. What if they share a different network? Network layer takes care of this situation.

Note:
Internet uses datagram approach in packet switching.

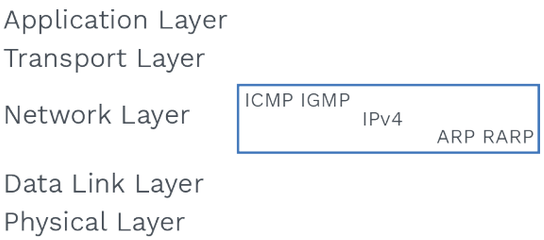
Internet protocol version 4 is used by TCP/IP model.
Look where IPv4 is placed at TCP/IP suite.

Grey Matter Alert!

Internet uses datagram approach, ATM and frame relay uses virtual circuit approach.

Rack Your Brain

Is the Internet connection-oriented or connectionless since we know it uses datagram services?



IPv4 has no error control and no flow control, IP relies on TCP in order to take care of error and flow control.

What are we called packets at IPv4? Datagram packets.
IPv4 datagram format:

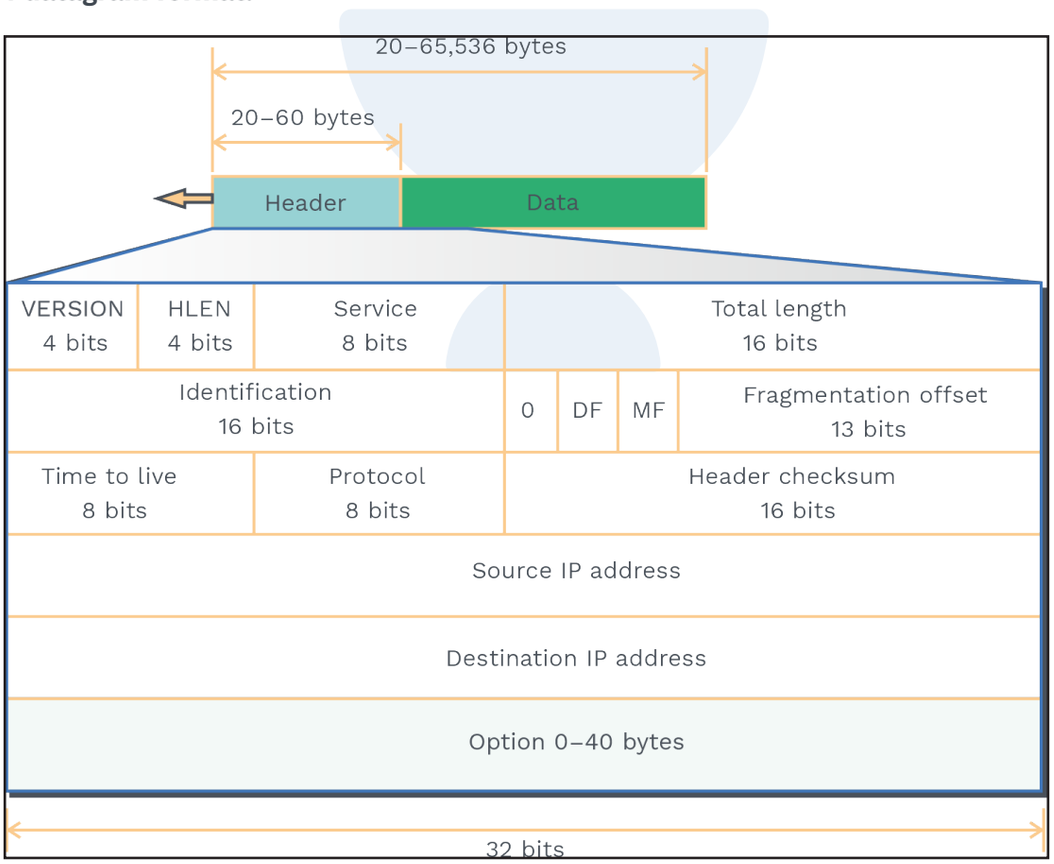


Fig. 4.1 IPV4 Header Format

Version: It has 4 bit,

- IPv4 uses version 4 whereas IPv6 uses version 6.

- Binary 0100 can be written in this field.

Header length:
- It has 4 bit.
- It defines length of IP header.

Note:
What is the minimum and maximum length of the IP header?
Minimum length = 20 Bytes, How? number of essential rows * size of each rows i.e 5 * 4 bytes.
Maximum length = 60 bytes, How? Maximum size of options are 40 bytes
20 + 40 = 60 bytes.

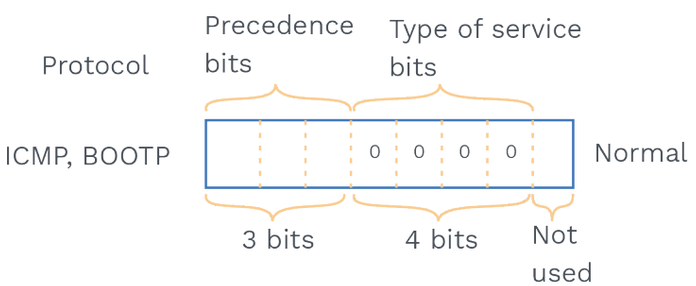
Example: If IPv4 has a binary pattern starting with 0100010.. What does this mean?
This means packet has version 4 and header length is 2 * 4 = 8 bytes.

Example: If IPv4 has a binary pattern starting with 01001111.. What does this mean?
This means packet has version 4 and header length is 15 * 4 = 60 bytes.

Grey Matter Alert!

- We have minimum and maximum length as 20 and 60 bytes respectively.
- But at header length we have only 4 bits i.e using 4 bits maximum we can go upto 15 bytes.
- It leads to the concept of scaling factor in this case it is 4 bytes.
- Header length = Header length field value * 4 bytes. If header length field contains decimal value 6 (represented as 0110), then-Header length = 6 x 4 = 24 bytes.

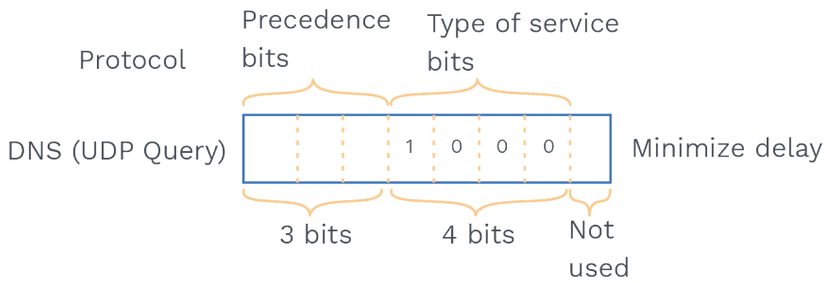
Service: It has 8 bit fields.



- Precedence bits are never used.
- Types of bits are used for various purposes depending on the protocol for ICMP and BOOTP it uses 0000 bits at Type of services.

Rack Your Brain

What is the range of Header length and Header length field?



Total length: It has 16 bit fields.
What is the minimum and maximum total length?
Minimum total length = Header length + Payload length

$$20 + 0 = 20 \text{ bytes}$$

Maximum total length = > with 16 bits we can go upto $(2^{16} - 1)$ bytes = 65535 bytes.

Example: In IPV4 packet HLEN is 7, value of total length field is 0x0033, How many
bytes of data are being carried?
HLEN = 7, number of bytes in header = 28 bytes (1 byte from the option)
Total length = 51 bytes
Packet carrying data = 51 - 28 = 23 bytes

Identification: It has a 16 bit field.

- From datagram packets, this field is responsible for the identification of fragments.
- Let's say there are n fragments; then each fragment are assigned the same identification number.
- Why is the identification number given to each fragment? So that during reassembly router can identify which IP datagram the fragments belong to.

Flags:
There are 3 bits, one bit uses do not fragment bit; one bit uses more fragment bits, and one bit is reserved.

Do not fragment bit: The value of this field can be 0 (do fragment if required) or 1 (do not fragment).
More fragment bit: It may be 0 (last fragment or only fragment) or 1 (more fragments are present behind this packet).

Fragment offset: It is has 13 bit.
It is equal to number of bytes ahead of it.

Note:
total length field = 16 bits = > 65535 Bytes.
Fragment offset = > 13 bits which will give 2^{13} - 1 bytes = 8191 Bytes.
Scaling is done because fragment offset cannot represent sequence of bytes greater than 8191.
Scaling factor in fragment offset = 2^{16} / 2^{13} = 2^{3}
Fragment offset field value = fragment offset/8

Time to live: It is a 8 bit field.

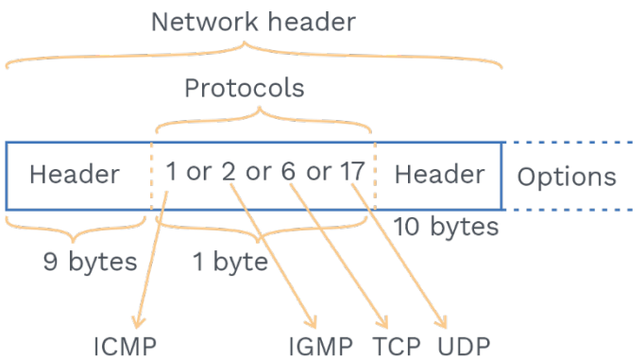
- Purpose of TTL is to prevent from looping.
- Devices which is having network layer decreases TTL by 1.
- At destination, value of TTL must be 0 or greater than 0 then the datagram packet will be accepted.
- At, the intermediate the value of TTL must be greater than 0; otherwise packet will be discarded.

Protocol: It is a 8 bit field.

Protocol values

Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Which protocol IP datagram belongs depending on the value inside the protocol field.



These numbers will eventually decide the router when the traffic becomes heavy which packet to discard.

The sequence of discarding the packet at routers is ICMP > IGMP > UDP >TCP

Means, TCP is the least discarded.

Header checksum: It is a 16 bit field
Checksum value stored in this field

At every router, checksum is calculated if it is not matched with the value present in the header, then the packet is discarded.

What are the fields that may be modified at every router?
TTL, Fragment offset, Header length, Datagram length, Options

Rack Your Brain

Why is checksum used at the Network layer?

Source IP address:
- It is a 32 bit fields.
- It is having IPv4 address of the source.

Note:
IPv4 address must not change until packet reaches destination.

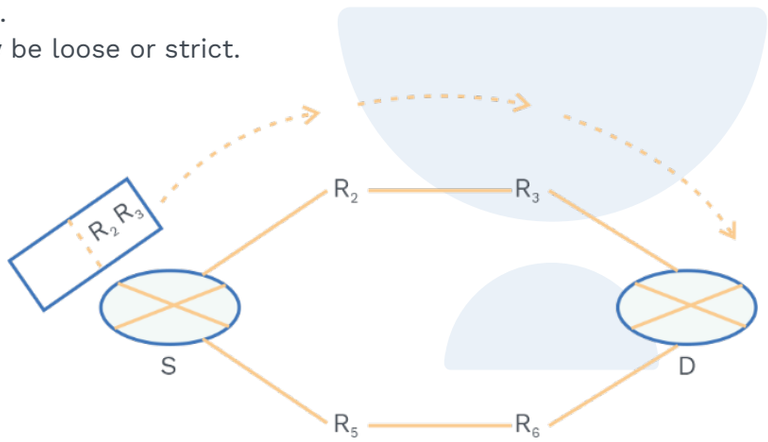
Destination IP address:
- It is a 32 bit fields.
- It is having IPv4 address of the destination.

Note:
IPv4 address must not change until packet reaches source.

Options: It has 0 to 40 bytes
- They are not mandatory but can be used for testing.
- Mainly it is used for source routing, record route and padding.

Record route:
When this option is set in the options field, the IP address of the router gets recorded in the options field.

Source routing: This field is used in order to check if the path is working or not.
It may be loose or strict.



Padding: Addition of dummy data to fill up space and make it a standard size is called padding, usually done through options only.
Options are actually used for testing and debugging.
Let us understand fragmentation through example.

Example: A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Give your view about fragmented packets?

Sol: Since M bit = 0,
This may be the last fragment but since we don't know about the fragmentation offset, we cannot say about the fragmented packet is the first, last or middle.

MF	Fragment Offset	Description
0	0	Invalid
0	!0	Last packet
1	0	First packet
1	!0	Intermediate packet

Previous Years' Question

Q. In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400, and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively, are:

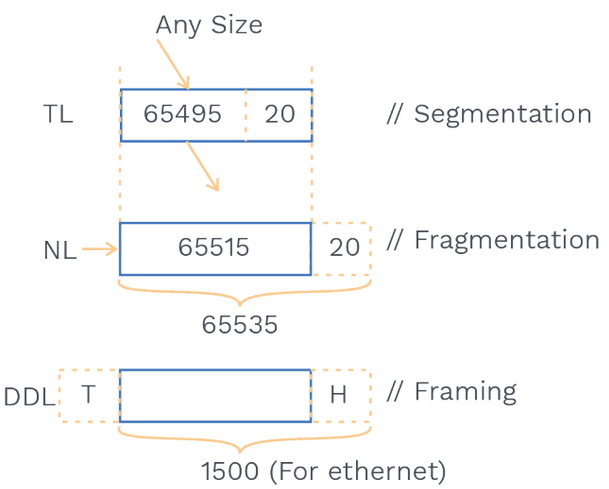
a) Last fragment, 2400 and 2789
b) First fragment, 2400 and 2759
c) Last fragment 2400 and 2750
d) Middle fragment 300 and 689

Sol: c) **(GATE - 2013)**

Fragmentation:

When the datagram is divided inorder to pass through other networks, this is called fragmentation.

Let us see the below scenario,



How we can limit fragmentation at the sender side!!

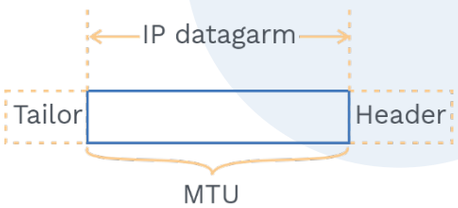
When TL segments the data in such way, that size of data can easily be taken by the network layer as well as in the data link layer.

Now, who will do fragmentation?

Sender and router, but keep in mind sender can limit the fragmentation by proper implementation.

Note:

MTU (Maximum Transmission Unit) is the maximum length that can be encapsulated in a frame.



Points for fragmentation:
It increases the datagram overhead because after fragmentation, IP header needs to be attached at every packet.
1) Total overhead = (Total number of fragmented datagram -1) * size of IP header.
2) Efficiency = Useful Bytes transferred / Total Byte transferred.
3) Bandwidth utilization or throughput = Efficiency * Bandwidth.
Understand Fragmentation using Example.

There are two networks, A and B. Network A has MTU 1020 Bytes and Network B has MTU 500 Bytes.
Host P wants to send the message to Host Q.
See the figure below,

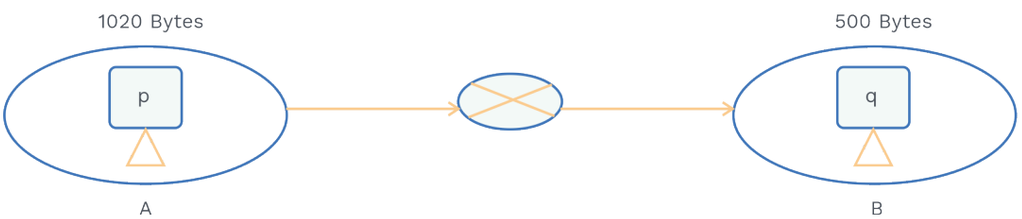


Fig. 4.2 Diagrammatic Representation of the Process of Fragmentation

Explanation how fragmentation will occur at router:

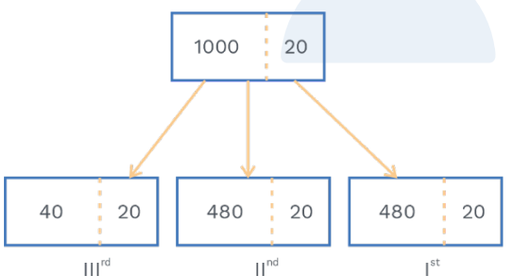
Step 1:
When Router receives the datagram packet having a Total size = 1020B, and if the DF flag is 0, now it can do fragmentation.

Step 2:
It will check if the network B MTU can accommodate the packet or not!
If not, then it will start fragmentation according to the MTU size of network B.

Step 3:
Here, MTU network B is 500 Bytes.
Out of 500 Bytes 20 Bytes will be the header, and 480 Bytes will be payload.
Maximum amount of data that can be sent at each fragment = 480.

Note:
Payload at each fragment must be multiple of 8 except the last fragment i.e. last packet may or may not have a multiple of 8 data byte.

See diagram below,



Lets see the header information of Ist fragment.
Total length = 500
Fragment offset = 0
Header checksum will be calculated again.
MF bit = 1
Identification number = same to all fragments.

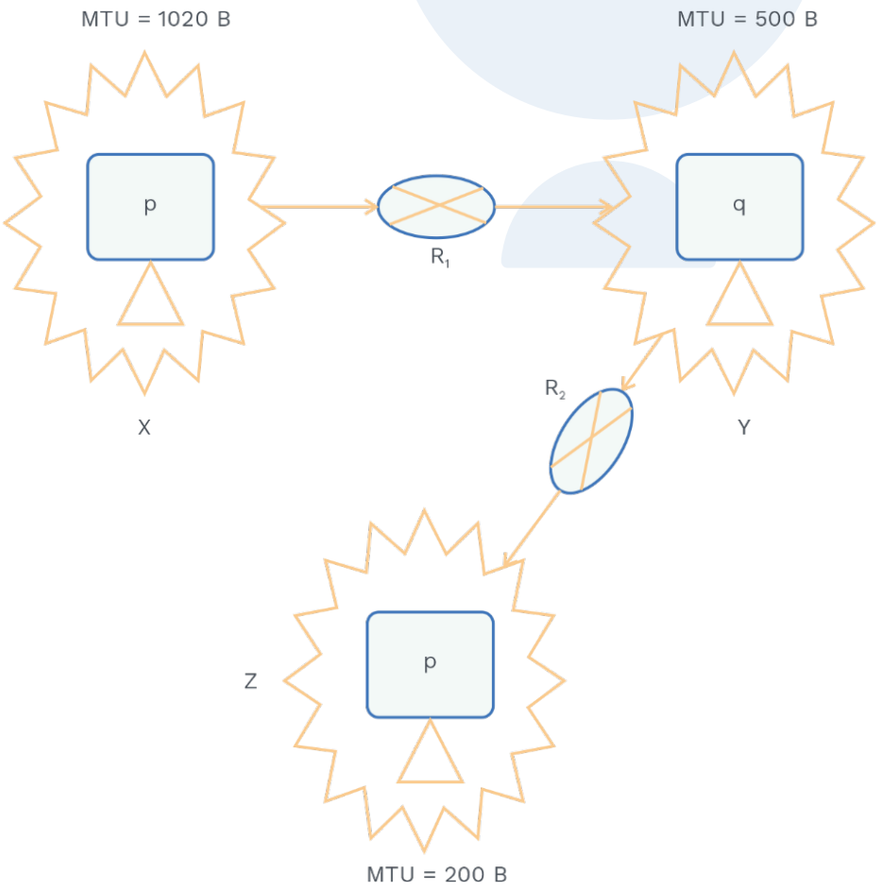
Information for IInd fragment.
Total length = 500
Fragment offset = 480/8 = 60

Header checksum will be calculated again.
MF bit = 1

Identification number = same to all fragments.
Information for IIIrd fragment.
Total length = 500
Fragment offset = (480 + 480)/8 = 120
Header checksum will be calculated again.
MF bit = 0
Identification number = same to all fragments.

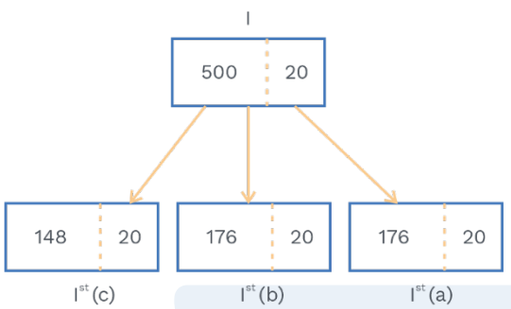
Receiver will take all the three segments and reassembly algorithms applied to get the original datagram.

Let's take the second scenario of the above example.

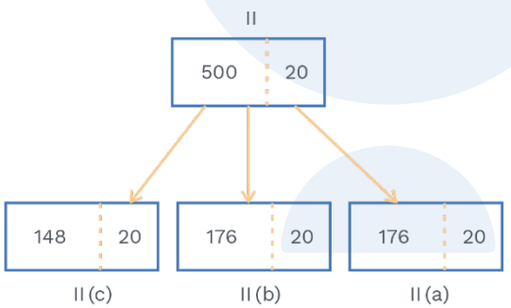


Router 2 will receive a datagram of 500B, but it can't forward directly, because MTU of next network Z is 200B.

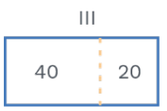
Router 2 will perform fragmentation for the Ist datagram.



Router 2 will perform fragmentation for IInd datagram.



Router 2 will not perform any fragmentation for IIIrd datagram.



Note:
We have taken 176 byte in I.a,I.b, II.a and II.b because datagram byte must be divisible by 8.

Reassembly algorithm:
Receiver applies the following steps:

I) Identifies whether datagram fragmented or not using MF bits and fragments offset bits.

II) Using Identification fields, it identifies all the fragments belonging to the same packet or not.

III) Fragment with offset field 0 is first fragment.
IV) identifies subsequent fragments using total length, header length and fragment offset.
V) Repeats step IV until MF = 0

IPv6 header:

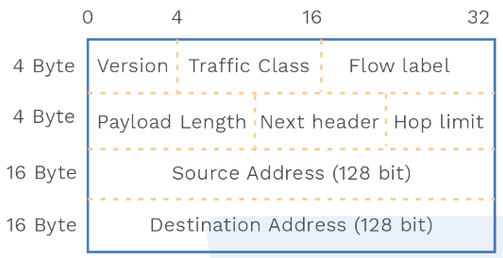


Fig. 4.3 IPV4 Header

Version: It will tell version of IP i.e 0110

Traffic class: It has 8 bits.
- The Most Significant 6 bits are used for Type of Service.
- The Last 2 bits are used for Explicit Congestion Notification.

Flow label: It has 20 bits.
- It is used for sequential flow of packet.
- It will help to avoid in re-ordering of packet.
- It is used for real time service.

Payload length: It has 16 bits.
- It tells how much information is present in the payload.

Next header: It has 8 bits.
- It is used for extension Header, if Extension Header is not present than it will inform Upper layer PDU.

Hop limit: It has 8 bits.
- It stop packets Loop to infinity.
- The value of Hop limit field decreases every time it crosses router.

Source address: It has 128 Bits.
- It indicates the address of originator.

Destination address: It has 128 bits.
- It indicates the address of indented destination.

Q7 **An IPv4 datagram carries 512 bytes of data; what is the value of the header length? What is the value of the total length field? Assume option is not given.**

Sol: Since the option is not given header length is 20 bytes,
Total length field is Header length + Data bytes
512 + 20 = 532 bytes

Q8 **The size of the option field of an IPv4 datagram is 28 bytes. What is the value of HLEN in binary?**

Sol: Total length of header is 28 + 20 = 48 Bytes.
HLEN should be the value after scaling.

48/4 = 12

In binary 1100

Q9 **Consider a datagram packet of length 7000 and fields are shown in the figure.**

Sol:

length	MF	ID	offset
7000	0	@	875

Q10 **It goes into a network where MTU is 1500 Byte, now how will the router do fragmentation?**

Sol: Since MTU is 1500 Byte it will be,

20	1480

After fragmentation packet will look like see below.

Let's see 1st fragment:

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 0 as before this fragment no data bytes are there.

Let's see 2nd fragment:

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 185 as before this fragment fragment 1 is present which is having 1480 byte of data, scaled value of 1480/8 = 185.

Let's see 3rd fragment:

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 370 as before this fragment 1 and fragment 2 is present which is having 1480 + 1480 byte of data, scaled value of 1480 *2/8 = 370.

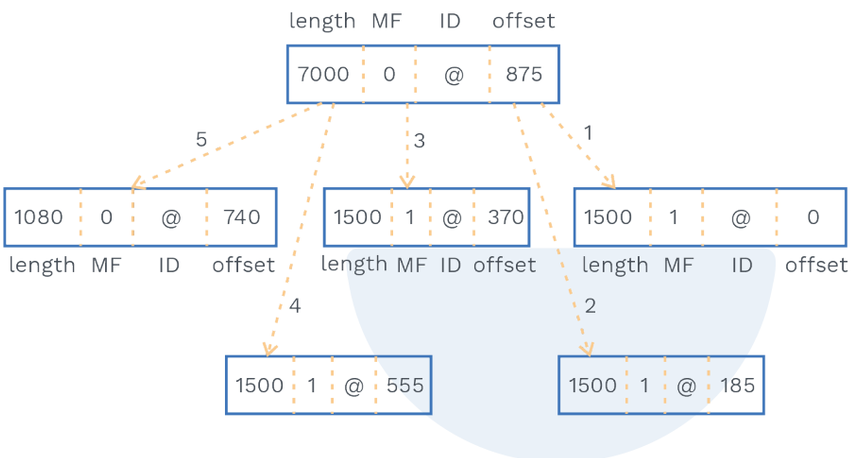
Let's see 4th fragment:

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 555 as before this fragment fragment 1, fragment 2 and fragment 3 is present which is having 1480 + 1480 + 1480 byte of data, scaled value of 1480 *3/8 = 555.

Let's see 5th fragment:

- Length field has 1080 bytes which include 20 bytes of header and 1060 bytes of payload, Why 1040? 7000 - 4 * 1480.
- MF field is 0 because no more fragments are followed.

- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 740 as before this fragment fragment 1, fragment 2, fragment 3 and fragment 4 is present which is having 1480 + 1480 + 1480 + 1480 byte of data, the scaled value of 1480 *4/8 = 740.



Previous Years' Question

Q. Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of the UDP header is 8 bytes, and the size of the IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of the offset field in the last fragment?

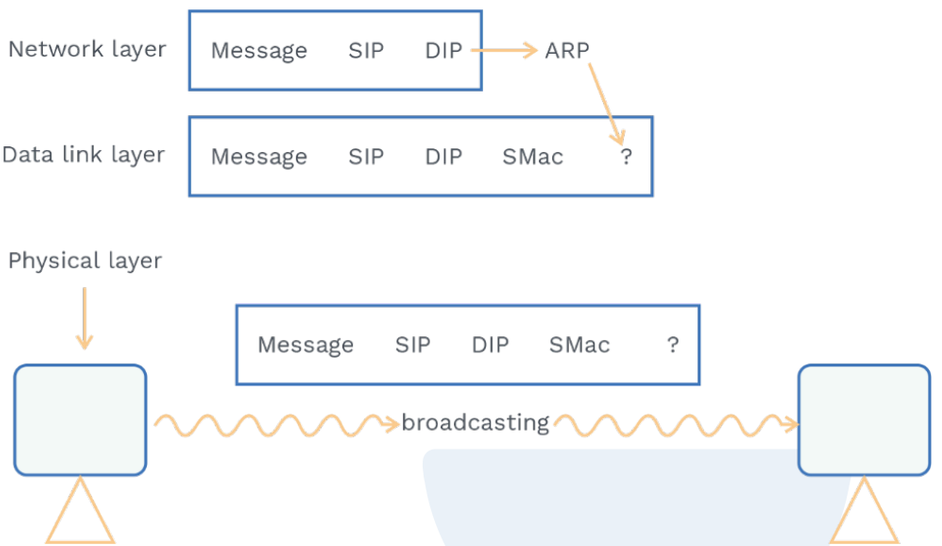
a) 6 and 925 **b)** 6 and 7400

c) 7 and 1110 **d)** 7 and 8880

Sol: c) **(GATE - 2015)**

ARP protocol:

- It is used for finding MAC addresses of corresponding IP address.
- ARP request is broadcast.
- ARP reply is unicast.
- It is used for finding MAC address of another Host or router.
- Even Router uses ARP, inorder to find MAC address of another Router or Host.



Lets understand working of ARP.

Step 1: Sender knows the target IP address.

Step 2: ARP request message is created and broadcast it which looks like.

SIP: Sender IP address.

DIP: Destination IP address.

SMac: Sender Mac Address or Sender Hardware address.

DMac = ?: Destination Mac Address which is unknown.

Step 3: The target Host or Router will Take the ARP request and reply its physical address and this reply will be unicast.

Step 4: Sender receives the reply and now it knows the target address of the machine.

Step 5: Now sender will do unicast to the destination IP address.
Let's understand better by taking example:

A host with IP address **a.b.c.d** and physical address **op:qr:st:uv:wx:yz** has a packet to send to another host with IP address **e.f.g.h** and physical address **zy:wx:uv:st:qr:op** (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

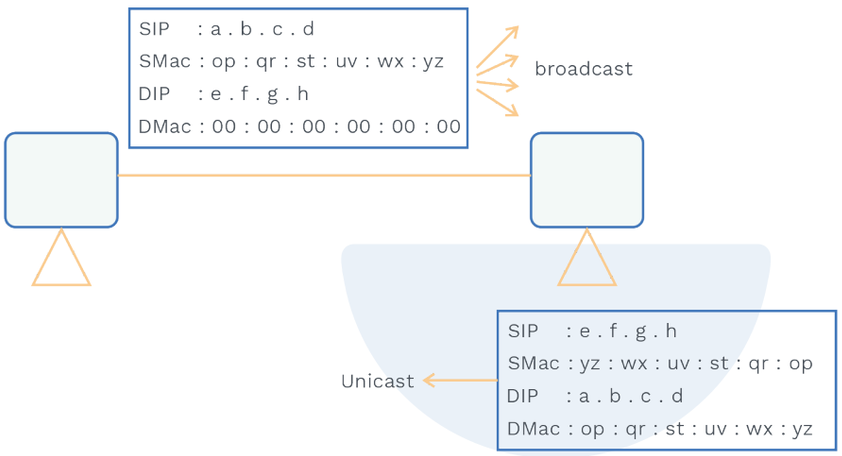


Fig. 4.4 Diagram Showing ARP Request and Reply Packet

Now we will see the Mapping of Physical to Logical address.
The possibilities when there is a need to convert from Physical to logical address are:

Case 1: While booting of diskless Node, it may find its hardware address but not an IP address.

Case 2: When IP address needs to assigned on demand, then the Host sends its MAC address and asks for short time lease.
For that, we use RARP, BOOTP and DHCP.

RARP: It will find an IP address (logical address) for given physical address.

- Machine gets its physical address by reading its NIC, By using Physical address Host can know the logical address using RARP protocol.
- RARP request is broadcast, and RARP reply is unicast, which is done by RARP Server.

MAC ⟶ RARP ⟶ IP

- Broadcasting is done at the data link layer. The MAC broadcast address does not pass the boundaries of a network.
- For this problem, the administrator has to assign a RARP server to each network, which is an overhead.

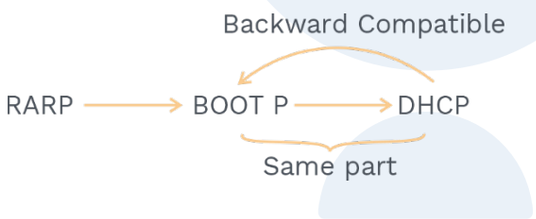
Note:
This RARP is now obsolete.

BOOTP: It is also designed such that it will convert the physical address into a logical address.

- It is similar to RARP, except it works at the application layer.
- Network, which does not have BOOTP server, has a relay agent.
- Because of the Relay agent, there is a need for only one BOOTP server.
- Disadvantage of BOOTP is that it maintains the static table.

DHCP: It will also maintain a table which helps in finding the Physical address for corresponding logical address.

- Only one DHCP server is enough in the network.
- No need for a relay agent.
- How do RARP, BOOTP and DHCP evolve?



Note:
DHCP provides static and dynamic address allocation that can be manual or automatic.

ICMP: Internet Control Message Protocol is a network layer protocol which is used by network devices to diagnose network communication issues.

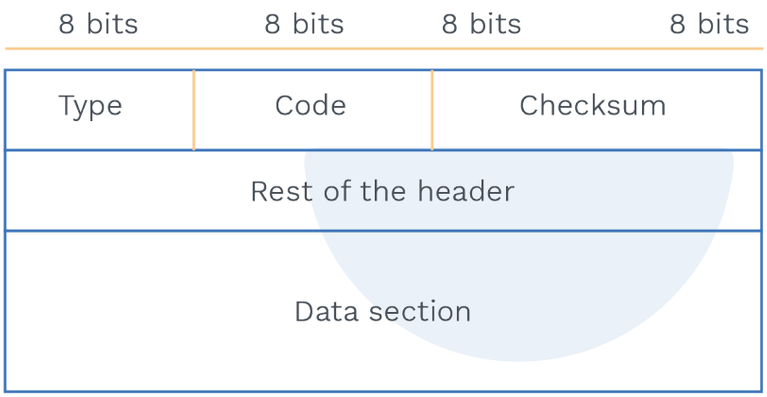
IP was designed for efficient use; It is an unreliable and connectionless datagram service which has its own advantages and disadvantages.

The two major shortcomings of IP are
I) Lack of error control and
II) Lack of providing assistance mechanism

Internet Control Message Protocol has been designed for this purpose.

Points:
ICMP has divided into two categories:
1) Error reporting message
2) Query message

Message format of ICMP:
It has 8 byte.
It has variable size data section.



- The first field defines the type of error message.
- The code field defines the reason for the particular message type.
- For each type of message there is the Header field section.
- Data Section contains information for finding the original packet in error message.
- Data Section contains information based on the type of query in query message.

Note:
ICMP always reports error messages to the original source.

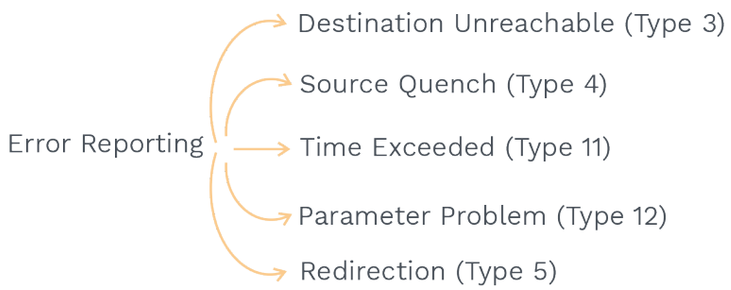
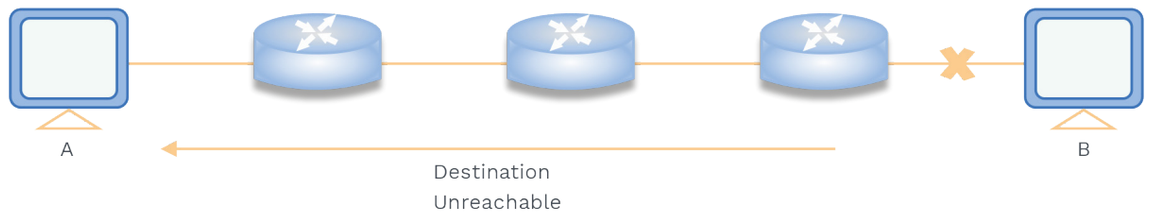


Fig. 4.5 Diagram Showing ARP Request and Reply Packet

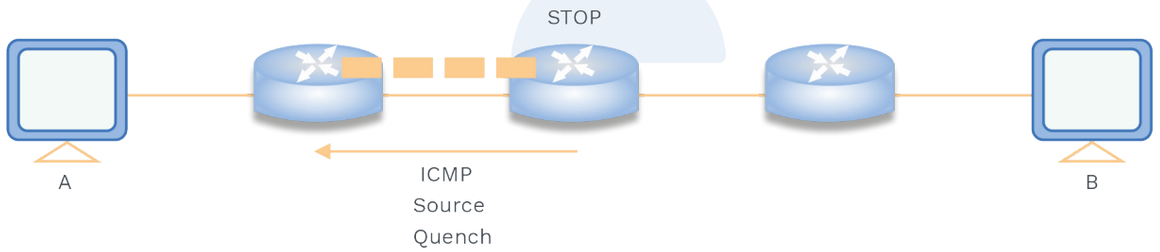
Destination unreachable: This problem occurs when the datagram does not reach to destination, the router and Host discard the packet and sends destination unreachable to the original sender.



Note:
Destination unreachable message can only be created either by destination host or router.

Source quench: The lack of flow control causes congestion in the router or destination Host.

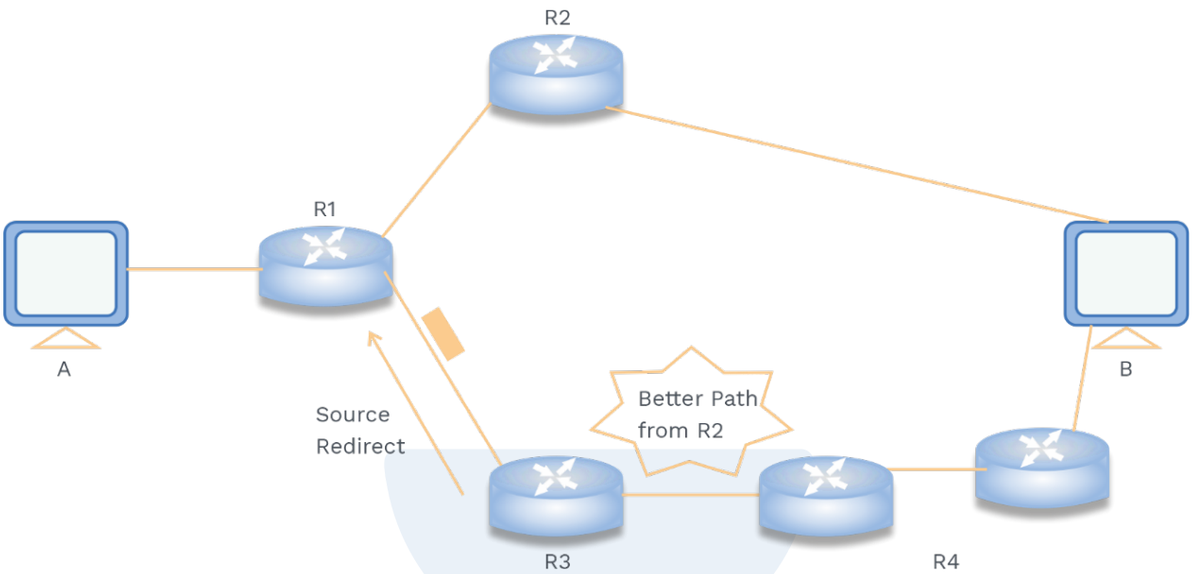
When the datagram is reached at a much higher rate so that router is not able to forward it, then it will discard the packet sending the source quench message to the source.



Time exceed message: When all fragments do not reach the destination at a certain time than Time exceed message is sends to source.

Parameter problem: If the router or the destination Host discovers the missing value or any error in the datagram packet, then it will send the Parameter problem.

Redirection: It is not an error message but just a warning message from a router to a Host that there is a better path which should be used.



Important points about ICMP error message:

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message, multicast address and special address.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

Query messages:

Query Message
- Echo Request and Reply (Type 8 and 0)
- Timestamp Request and Reply (Type 13 and 14)
- Router Solicitation and Advertisement (Type 10 and 9)
- Address Mask Request and Reply (Type 17 and 18)

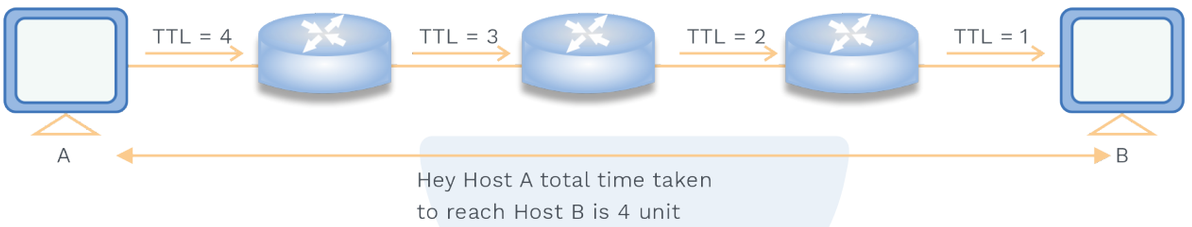
In order to solve network problems, query messages are used

Echo request and reply: The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

It is used to check if the destination is working or not, and all the routers comes along the path is working.

Note:
Nowadays Ping command is used for echo request and echo reply.

Time stamp request and reply: hosts or routers can use the timestamp request and timestamp reply messages to determine the total time needed for an IP datagram to travel between them.



Address mask request and reply: How does Host obtain its network mask? To obtain its network mask, a host sends an address-mask-request message to a router.

Now two cases arise if the Host knows the address of the router or not!

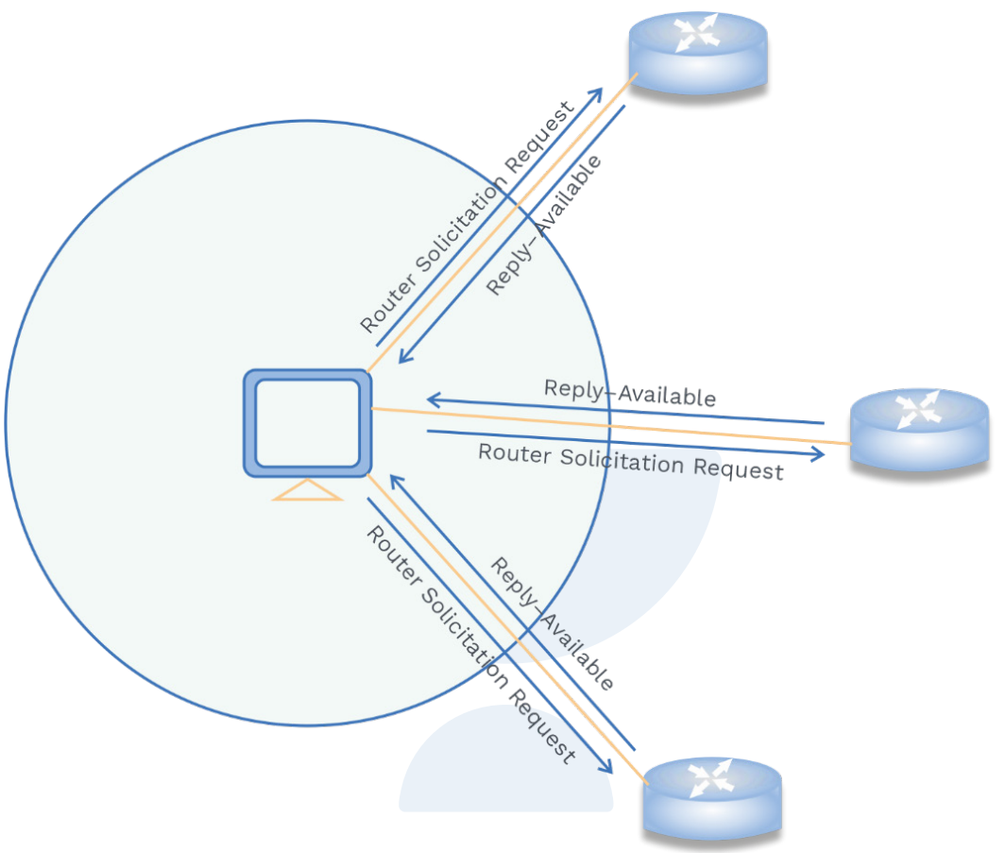
- If it knows, then it will directly send the router.
- if it does not know, then Host will broadcast the message.

Now Router will do address-mask-reply message, providing the necessary mask for the host.

Router solicitation and advertisement:

- For giving Router information, Router advertisement message is used via broadcasting.
- For finding a router Router solicitation message is used via broadcasting or multicasting.

Note:
When a router sends out an advertisement, it tells all the information of known routers also.



Now we will see the routing of an IP packet:
Flooding:
Sending packets through every possible path is flooding.

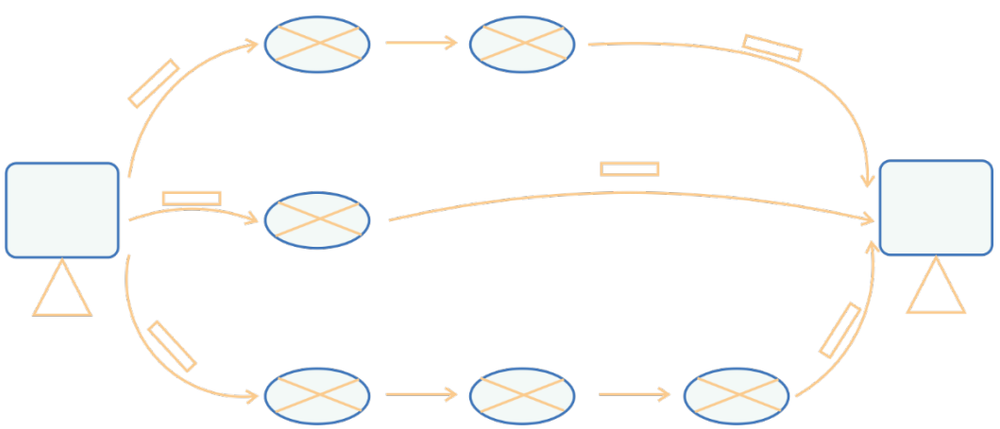


Fig. 4.5 Diagrammatic Representation of Flooding

Advantage of flooding:
- Reliability is more.
- Shortest path finding is guaranteed.

Disadvantage:
- Traffic is more.
- Duplicates packet will be more.

Routing:
Deciding the packet which path to follow by making a Routing Table is called Routing.

Note:
Putting a packet from one side and taking it to the other side is called switching.

Advantage of Routing:
- Traffic is less.
- No duplicate packet.

Disadvantage of Routing:
- Reliability is less.
- Shortest path finding is not guaranteed.

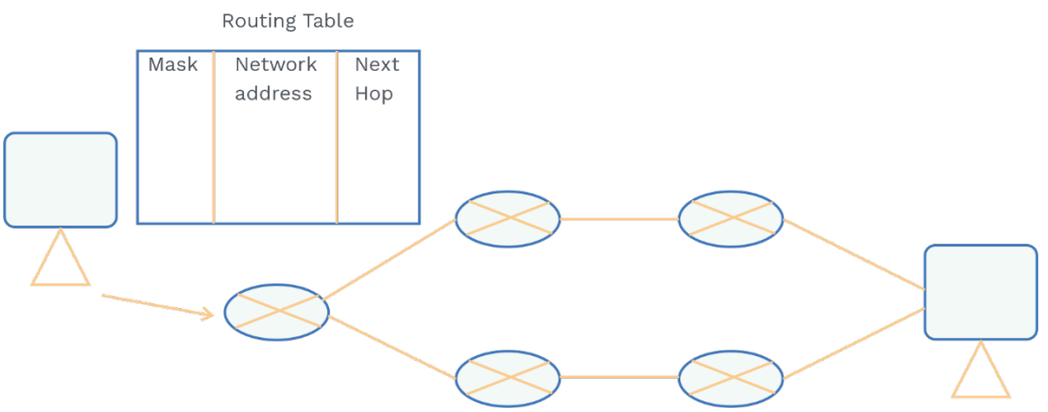


Fig. 4.6 Diagrammatic Representation of Routing

Types of Routing Algorithm:
1) Static Routing
2) Dynamic Routing
  a) DVR (Distance Vector Routing)
  b) LSR (Link state Routing)

Static Routing:

a) They don't change based on topology and traffic.
b) In static routing user-defined routes are used in the routing table.
c) Static Routing may not follow any specific protocol.
d) They are used in smaller networks.

Dynamic Routing:

a) They don't change based on topology and traffic.
b) In dynamic routing, routes will be updated as per changes are done in network.
c) They are used in larger networks.
d) Dynamic Routing follow protocol.

Distance vector Routing:

It is a dynamic routing algorithm.

Step 1: Each router makes its routing table.
Each router knows.

- All the router present in the network.
- Distance to its neighbour router.

Step 2: Each router exchanges its distant vector to its neighbour routers and prepare a new routing table.

Step 3: Repeat step 2 (n-1)times if there are n routers.

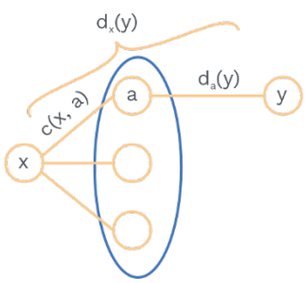
Step 4: After this routing table converge i.e. it become stable.

Note:

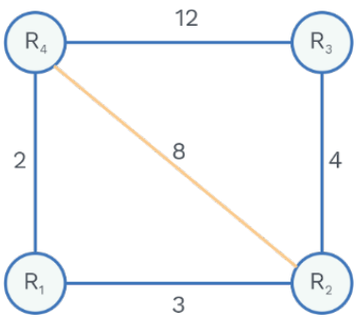
Distance vector routing uses Bellman Ford algorithm at each router.

Bellman–Ford equation

- $d_x(y) = \min_a\{c(x, a) + d_a(y)\}$
- $d_x(y)$ – least cost path from node x to y
- $\min_a$ – apply above eq. over all of x's neighbors



Let us understand using example



There are 4 routers in a network and delays or cost are mentioned on the edges.

Step 1:

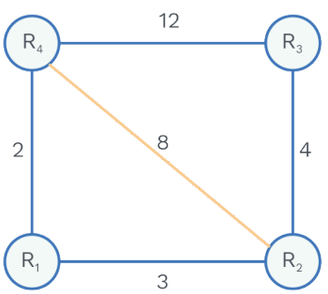
Each router will maintain a Routing table using its local knowledge.
Here we have taken Destination, Distance and next hope for building a routing table, but there may be many more fields.

for R_4

Destination	Distance	Next hop
R_1	2	R_1
R_2	8	R_2
R_3	12	R_3
R_4	0	R_4

for R_3

Destination	Distance	Next hop
R_1	∞	–
R_2	4	R_2
R_3	0	R_3
R_4	12	R_4



for R_1

Destination	Distance	Next hop
R_1	0	R_1
R_2	3	R_2
R_3	∞	–
R_4	2	R_4

for R_2

Destination	Distance	Next hop
R_1	3	R_1
R_2	0	R_2
R_3	4	R_3
R_4	8	R_4

Step 2:
Each router will exchange its distant vector and build the new routing table.

For router R1:
Router R1 will receive distance vectors from its neighbour R2 and R4.
Now router R1 will prepare a new table as,

for R_2

Destination	Distance	Next hop
R_1	3	R_1
R_2	0	R_2
R_3	4	R_3
R_4	8	R_4

for R_4

Destination	Distance	Next hop
R_1	2	R_1
R_2	8	R_2
R_3	12	R_3
R_4	0	R_4

New routing table for R1 using R2 and R4

R_2	R_4	Destination	Distance	Next hop
		R_1	0	R_1
Min (3+0,	2+8) = 3	R_2	3	R_2
Min (3+4,	2+12) = 7	R_3	7	R_2
Min (3+8,	2+0) = 2	R_4	2	R_4

For router R2:
Router R2 will receive distance vectors from its neighbour R3, R1 and R4.
Now router R2 will prepare, new table as,

for R_1

Destination	Distance	Next hop
R_1	0	R_1
R_2	3	R_2
R_3	∞	–
R_4	2	R_4

for R_3

Destination	Distance	Next hop
R_1	∞	–
R_2	4	R_2
R_3	0	R_3
R_4	12	R_4

for R_4

Destination	Distance	Next hop
R_1	2	R_1
R_2	8	R_2
R_3	12	R_3
R_4	0	R_4

New routing table for R2 using R1, R3 and R4

R_1 R_4 R_3
Min (3+0, 8+2, 4+∞)

R_3 R_4 R_1
Min (4+0, 8+12, 3+∞)

R_1 R_4 R_3
Min (3+2, 8+0, 4+12)

Destination	Distance	Next hop
R_1	3	R_1
R_2	0	R_2
R_3	4	R_3
R_4	5	R_1

For Router R3:

Router R3 will receive distant vectors from its neighbour R2 and R4. Now router R3 will prepare new table as,

for R_2

Destination	Distance	Next hop
R_1	3	R_1
R_2	0	R_2
R_3	4	R_3
R_4	8	R_4

for R_4

Destination	Distance	Next hop
R_1	2	R_1
R_2	8	R_2
R_3	12	R_3
R_4	0	R_4

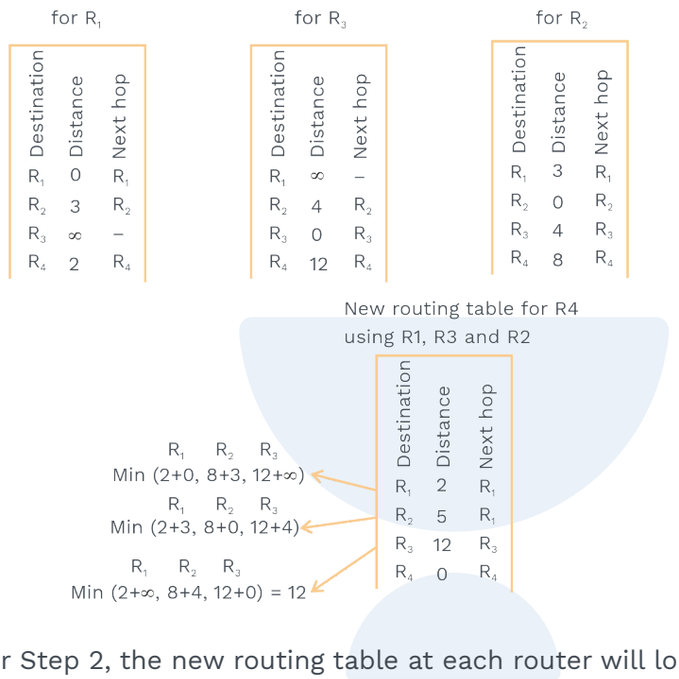
New routing table for R3 using R2 and R4

R_2 R_4
Min (4+3, 12+2) = 7
Min (4+0, 12+8) = 4
Min (4+8, 12+0) = 12

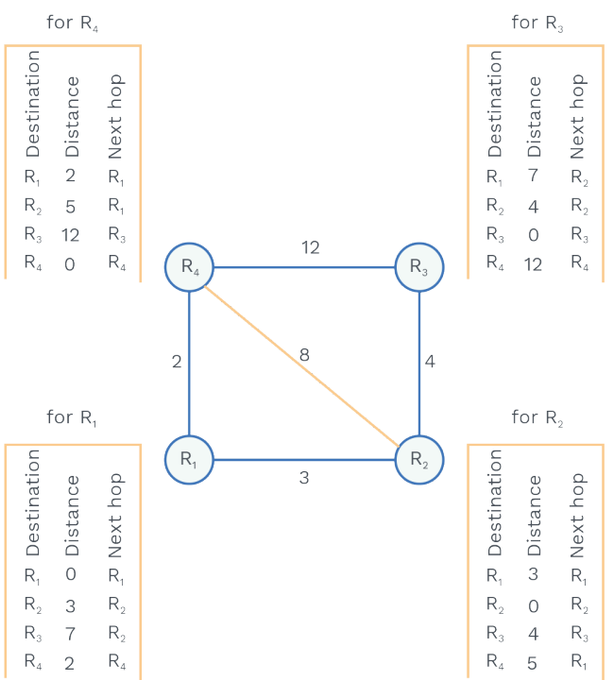
Destination	Distance	Next hop
R_1	7	R_2
R_2	4	R_2
R_3	0	R_3
R_4	12	R_4

For Router R4:

Router R4 will receive distant vectors from its neighbour R2, R3 and R1. Now router R4 will prepare new table as,



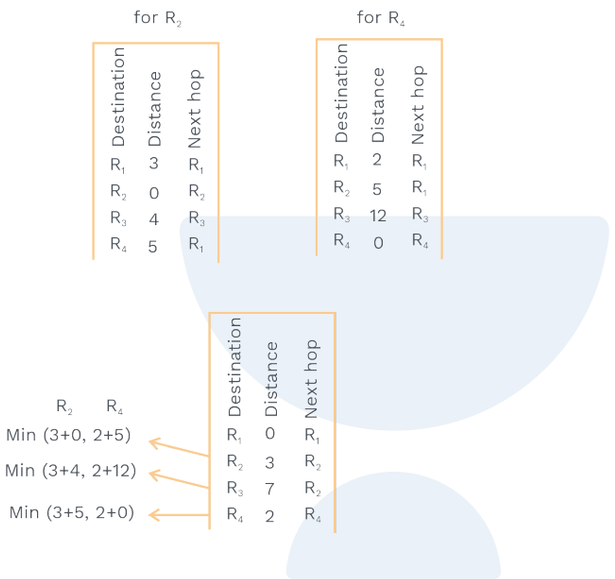
Finally after Step 2, the new routing table at each router will look like,



Step 3: Each router exchanges its distant vector obtained in step 2. After exchanging, each router will have a new routing table.

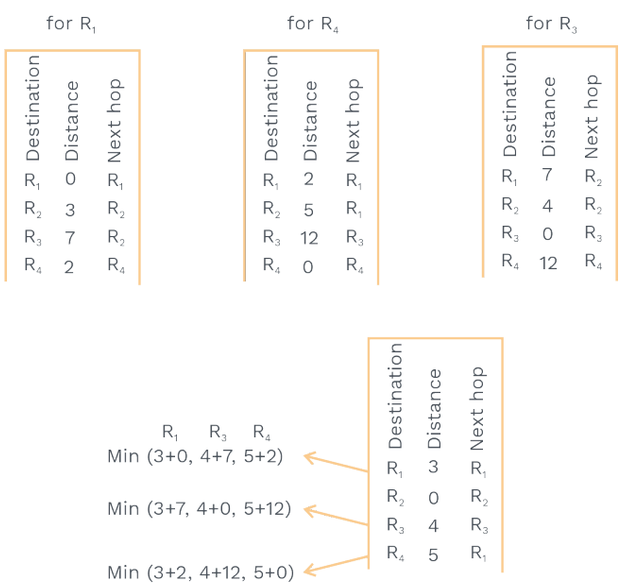
For Router R1:

Router R1 will receive distant vectors from its neighbour R2 and R4. Now router R1 will prepare new table as,



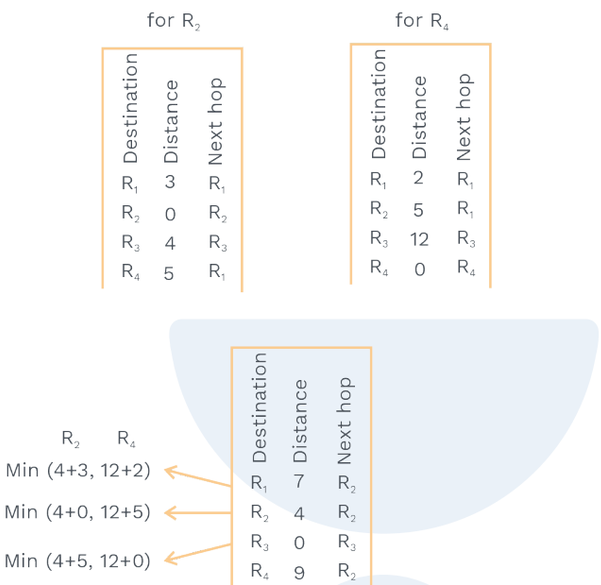
For Router R2:

Router R2 will receive distant vectors from its neighbours R1, R3 and R4. Now router R2 will prepare a new table as,



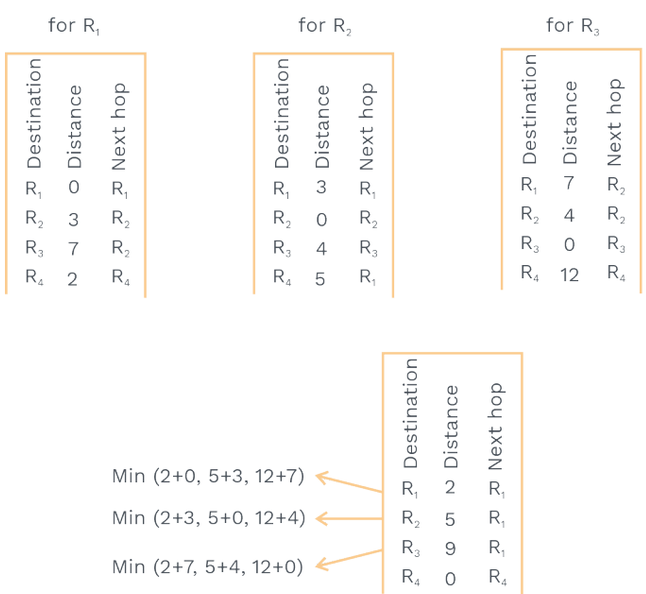
For Router R3:

Router R3 will receive distant vectors from its neighbour R2 and R4.
Now router R3 will prepare new table as,

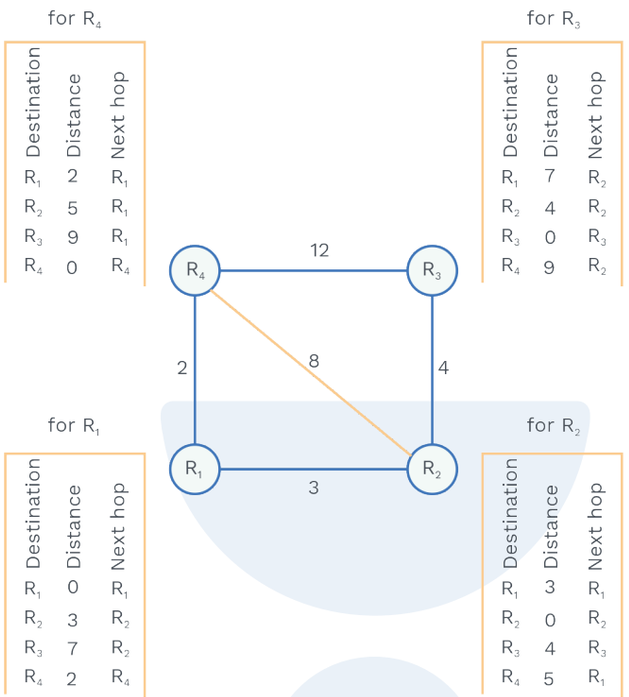


For Router R4:

Router R4 will receive distant vectors from its neighbours R2, R3 and R1.
Now router R4 will prepare a new table as

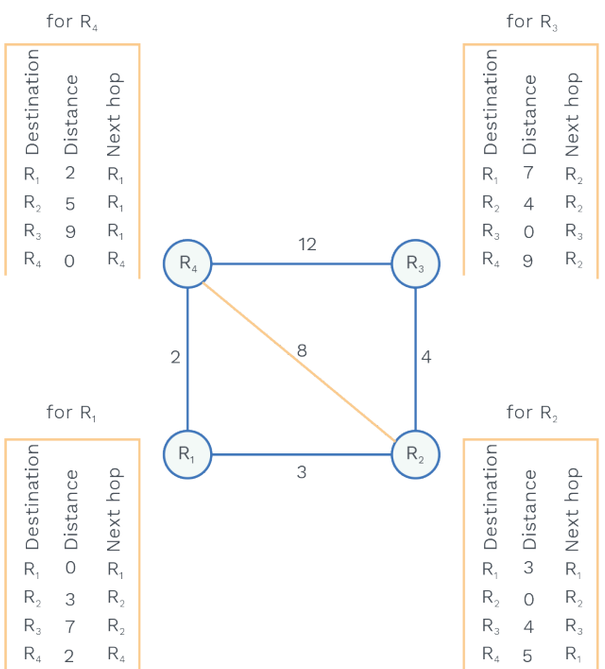


Now the routing table will be like,



Step 4:

Since there are 4 routers and 2 exchanges have been done now router will look like.



Common field of Routing table:
Till now we have seen the destination, distance and next hop in routing table but there are many other fields also.

Mask	Network address	Next–hop address	Interlace		Reference count	Use

Mask: It defines mask for a particular entry.

Network address: It defines the network of destination Host.

Next hop address: It defines the network where router will route next.

Interface: This shows the name of the interface.

Use: This field defines the number of packets transmitted through this router.

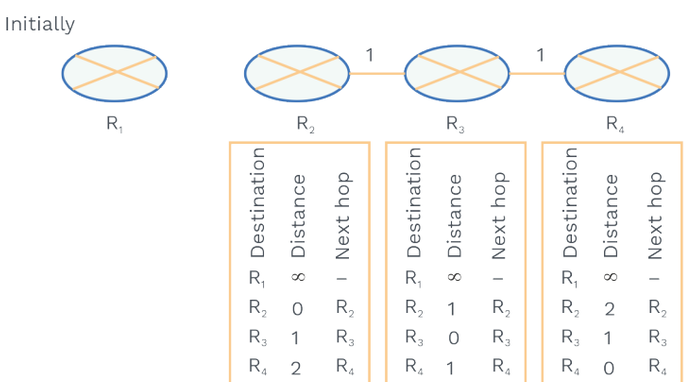
Reference count: Number of the user connected to this router at the same time, is defined by this field.

Problem with Distance Vector Routing:

- It has a count to infinity problem.

Trick to remember Count to infinity problem:
Bad News spreads slow and good news spread fast.

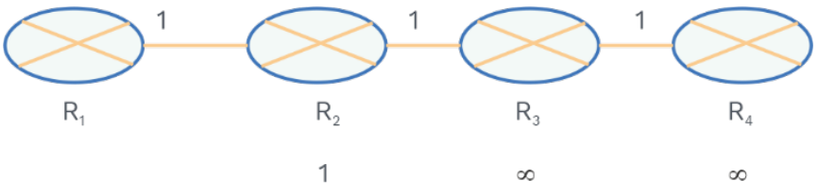
Let's understand How this problem occurs in DVR.
There is Router R1 which is not connected initially, so it looks like,



Now we will see what happens if Router R1 gets connected to the networks.

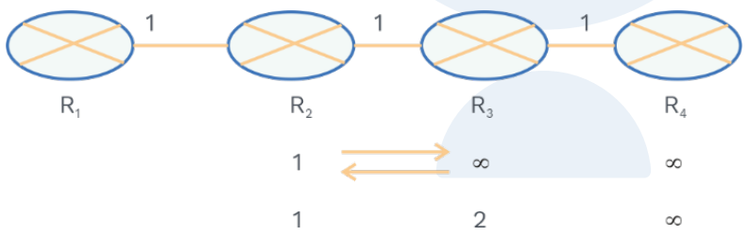
When R1 get connected to the R2, How do other router update their entry at R1 position given in diagram.

* Please Note We have taken R1 row value at every diagram.



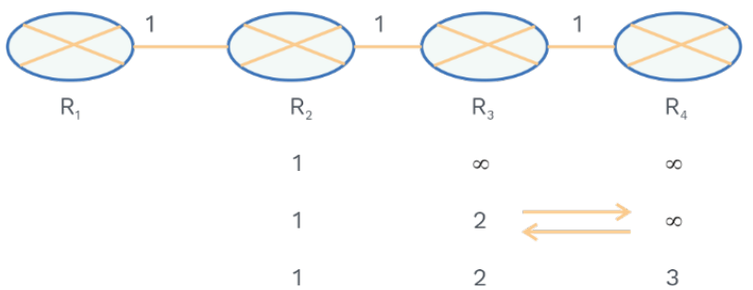
Now exchange of vectors will take place,

R3 will think R2 distance vector is showing 1 unit distant from R2 to R1, and since R2 is 1 unit to R3, So R3 will reach to R1 in 2 unit distance,



Now again exchange of vectors will take place,

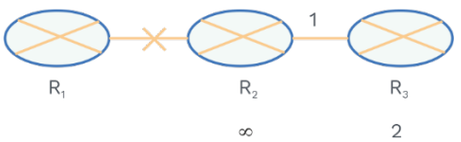
- R4 will think R3 Distance vector is showing 2 unit distant from R3 to R1, and since R3 is 1 unit to R4, So R4 will reach to R1 in 3 unit distance.



This means when R1 is added (Good news) router get to know each other soon.

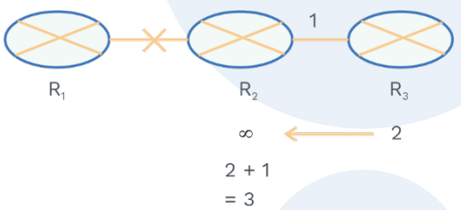
Now lets see what will happen if router get disconnected.

- R2 get to know that R1 is not there, but R3 will slowly get to know.



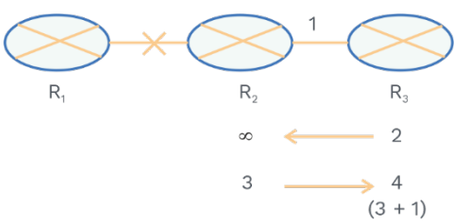
Why will R2 get updated to 3?

Now the exchange of Distance vectors takes place, R3 is saying to R2 that for reaching R1 it will take 2 units, and R3 distance is 1 unit from R2, So R2 will update 3 units.



Why will R3 get updated to 4?

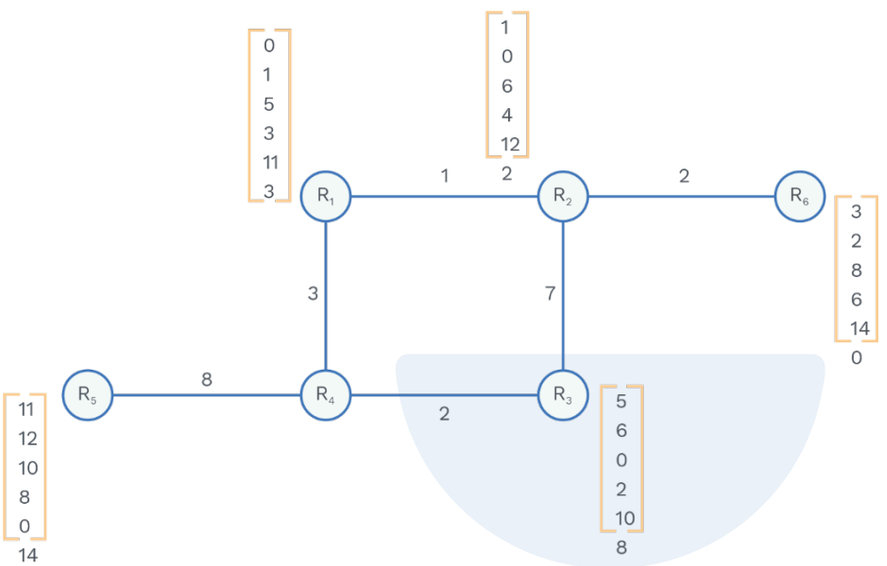
After R2 updated to 3, it will exchange its distance vector to R3, now R3 will think R2 can reach R1 in 3 unit and R2 is 1 unit distant, So R3 will update to 4.



Similarly, same exchange of routing table exchange and slowly it will lead to update.

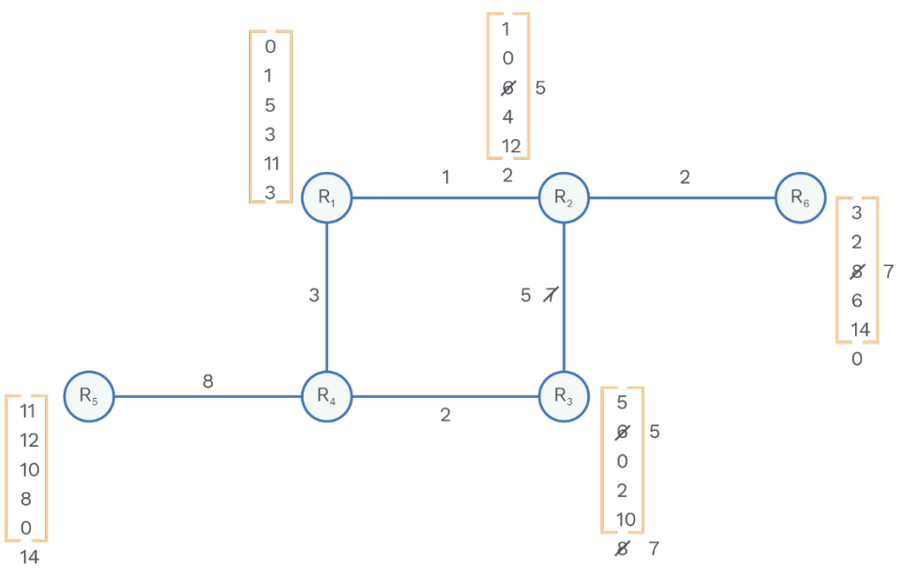
This is how Bad problem travels slow.

Let's understand, through example, How DVR works when any Routes gets changes.



Initially every router gets to know about each other through changing their distant vector.

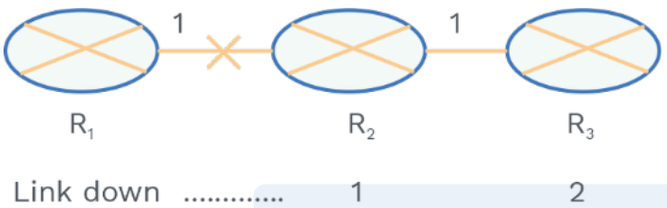
Case 1: Which link is unused!
R2 - R3 Link
Case 2: If R2 - R3 link changes to 5, What would be the distance vector of R3?



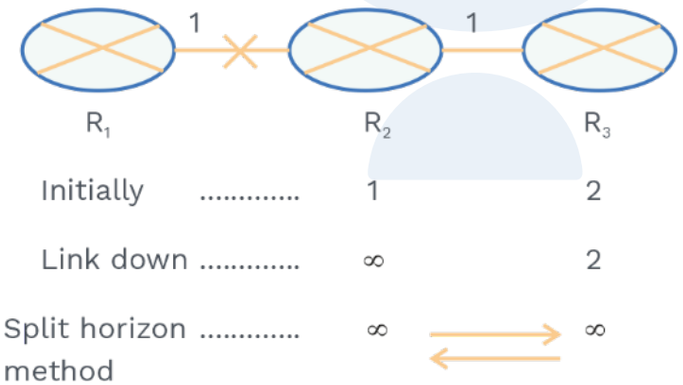
Solution to count to infinity problem is to use Split horizon method:
Split horizon is a method which prevents a router from advertising a route back on the same interface.

Rack Your Brain

What would be the distance vector of R4 before and after Link changes?



Split horizon says that in a given situation if R3 is depending on R2 inorder to Reach R1, it should not advertise its distance to R2 , it will always advertise infinity.



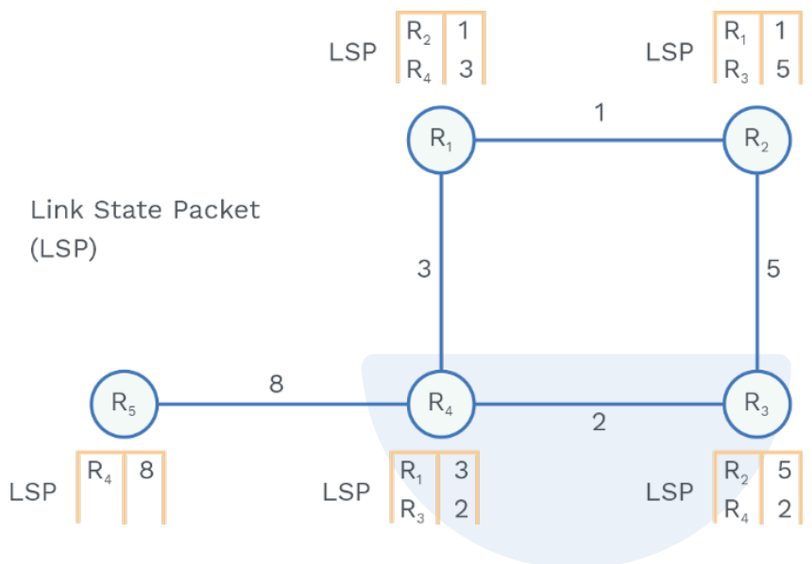
Link state router:
There are 4 steps for making routing using Link State protocol,
Step 1: Creation of states of the link by each node, those states are called Link state Packet.
Step2: Flooding Of LSP to every Router.
Step 3: Formation of the Shortest Path Tree for each node.

Note:
For creating the shortest path tree, Dijkstra algorithm is used.

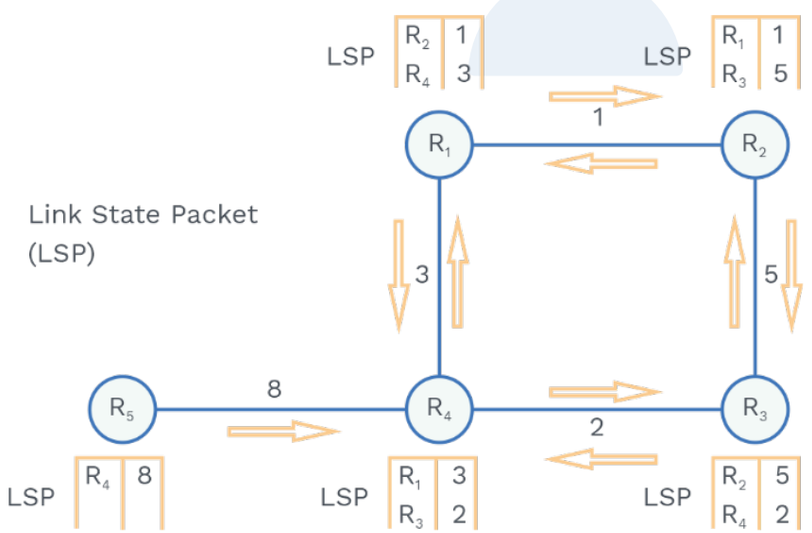
Step 4: Calculation of Routing Table based on the shortest Path tree.

Lets understand using example:

Step 1: Making Link State Packet (LSP), by knowing its neighbour.

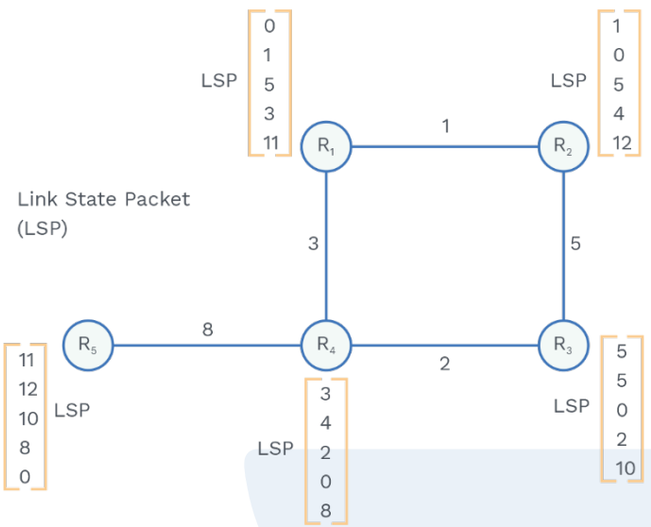


Step 2: Flood the LSP packet at every router.



Step 3 and Step 4:

At each router using Dijkstra shortest tree is made, and Routing table is computed.



Problem In Link State:

1) Router is facing heavy traffic,
Now because of heavy traffic, How routers get to know that Which Packet is latest!!
Every router will maintain a record of incoming packet and their sequence number.

2) Transient problem
(This problem occur for a short problem)
a) Black Hole problem

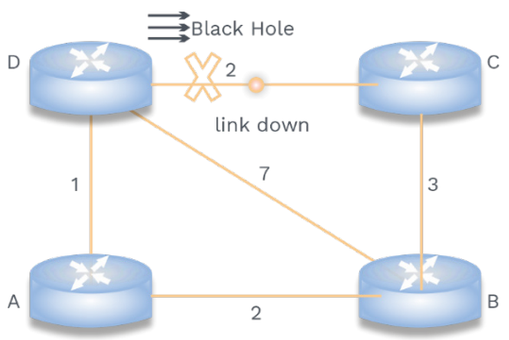


Fig. 4.7 Diagram Representing Black Hole Problem in Link State Routing

This says that if a link is down all the packet transmitted through this link will get lost, and this is called Black Hole problem.
But after some time, the Router will configure correctly, this means Black Hole problem only creates delays for some time.

b) Looping problem also arises when a link is down, it is also a transient problem.
compare DVR and Link State Routing:

Basis for Comparison	Distance Vecotr Routing	Link State Routing
Algorithm	Bellman Ford	Dijsktra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on the cost
CPU and memory	Low utilisation	Intensive
Convergence time	Moderate	Fast

Fig. 4.8 Comparison Between DVR and LSR

Note

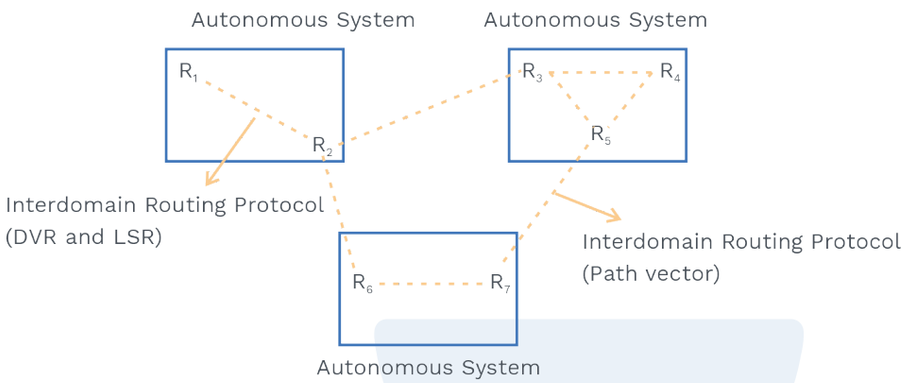
- Routing Information Protocol (RIP) is an implementation of Distance vector routing.
- Open Shortest Path First (OSPF) is an implementation of Link State Routing.
- Border Gateway Protocol (BGP) is an implementation of Path vector Routing.

Intradomain and Interdomain Routing:
Internet is divided into the autonomous system, because internet is large enough that it can't handle the records of all the router.

Note
Autonomous System (AS): It is a group of routers under guidance of single administration.

When Routing is done inside autonomous system it is considered as

intradomain Routing.
When Routing is done between autonomous system it is considered as interdomain Routing.



Till now we have discussed DVR and LSR, lets see How Path vector works, which is an Intradomain Routing.
Path vector is similar to Distance vector only except that only Speaker node can communicate with each other.

Note:
Speaker node is a node which can act as administrator of all the nodes present inside an autonomous system.

BGP is an implementation of Path vector, BGP can also be used in two ways Exterior BGP and Interior BGP.

Exterior BGP: This is used When two-speaker node used to communicate with each other.

Interior BGP: This is used when the speaker wants to collect information from other router inside an Autonomous System.

Chapter Summary

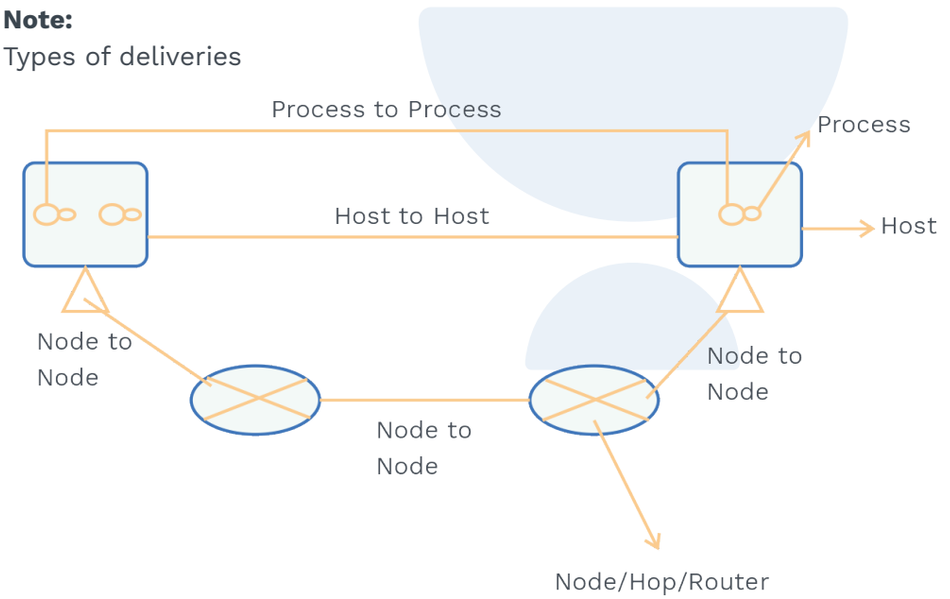
- IPv4 is 32 bit long and used to define any host universally on the Internet.
- In classful addressing, IP address can be divided into NID (network identifier used to identify network) and HID (Host identifier used to identify the Host).
- Addresses in classes A, B, or C are mostly used for unicast communication and addresses in class D are used for multicast communication.
- Dividing of the large networks into smaller ones is called Subnetting, and Supernetting combines several networks into the larger one.
- Address space is divided into variable-length blocks in Classful addressing.
- Basically 3 rules in classless addressing given below:
  1) Block must have contiguous addresses.
  2) Size of Block must be written in the power of 2.
  3) First address of the block must be divisible by the size of the block.
- IPv6 addresses use hexadecimal colon notation with abbreviation methods available.
- Unicast, multicast and anycast is used in IPv6, there is no concept of broadcast in IPv6.
- IPV4 is an unreliable connectionless protocol for source to destination delivery.
- Minimum and the maximum length of IP header are 20 and 60 bytes, respectively.
- The maximum number of bytes that a data link protocol can encapsulate is called MTU (maximum transfer unit).
- Division of packets into the smaller packets so that it can accommodate in MTU is called fragmentation.
- Mapping of a logical address to a physical address can be static or dynamic.
- At every router, checksum is calculated if it is not matched with the value present in the header, then the packet is discarded.
- Options provide Source routing, padding and record route.
- The address resolution protocol (ARP) is a dynamic mapping method that is used to find a physical address when logical address is given.
- The Reverse address resolution protocol (RARP) is used to find a logical address when the physical address is given.
- Packet Internet Groper (ping) is an application program that uses the services of ICMP to test the reachability of a host.
- A static routing entries are updated manually by an administrator and dynamic routing entries are updated automatically by a routing protocol.
- An autonomous system (AS) is a group of networks, and routers under the authority of a single administrator.
- Routing Information Protocol (RIP) is an implementation of Distance vector routing.
- Open Shortest Path First (OSPF) is an implementation of Link State Routing.
- Border Gateway Protocol (BGP) is an implementation of Path vector Routing.

5 Transport Layer

5.1 TRANSPORT LAYER

- Main objective of the Transport layer is to deliver the packet from process to process.
- Transport layer protocol may be connectionless or connection-oriented depending on the how segments are treated.
- Transport layer may be responsible for error control and flow control, but these facilities are also provided by the data link layer, so what is the need here? The need is in data link layer error control and flow control is provided on the link only, but, here error and flow control is provided end to end.
- Transport layer protocols are UDP, TCP and SCTP.

Note:
Types of deliveries



- Data link layer is responsible for Node to Node delivery.
- Network layer is responsible for Host to Host delivery.
- Transport layer is responsible for Process to Process delivery.

Addressing mode at the transport layer is done using Port number, **Why the port number is needed, is IP address and MAC address are not sufficient?** Since at any Host, there may be many process running, in order to find out which process to reach, we need port number.

Rack Your Brain

How addressing is done at the data link layer and network layer?

In TCP header port number is 16 bit field. It ranges from 0 to 65535.

Port number	Protocol	Description
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol

Fig. 5.1 Port Number and Corresponding Protocols

PRACTICE QUESTIONS

Q1 **What is socket addressing?**

Sol: The combination of Port number and IP address is called socket addressing. Client socket identifies the client process uniquely and server socket identifies the server process uniquely.

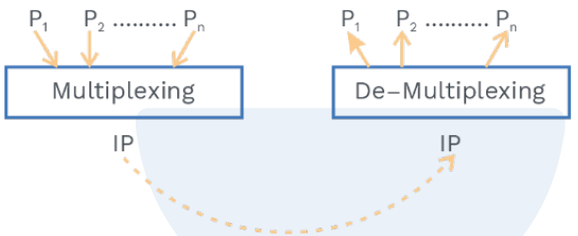
The IANA (Internet Assigned Number Authority) divides the port numbers into

- Well known,
- Registered, and
- Dynamic (or private)

Note:

Socket Address: IP Address + Port Number

Transport layer provides multiplexing and demultiplexing.

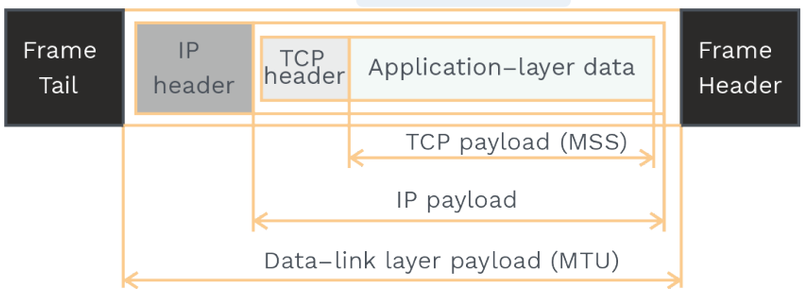


There are two types of major protocol in transport layer.

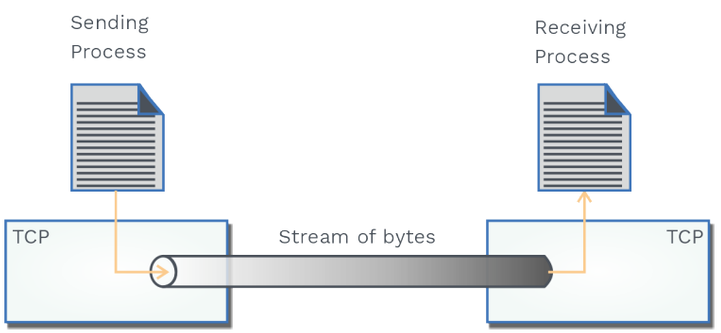
TCP and UDP

Lets see TCP,

Before going further lets see How TCP encapsulates.



- Transport layer provides stream delivery service.



TCP handles congestion (by reducing the sender window size)
How TCP Keep counts its segment,

1) Byte Number
2) Sequence Number
3) Acknowledgement Number

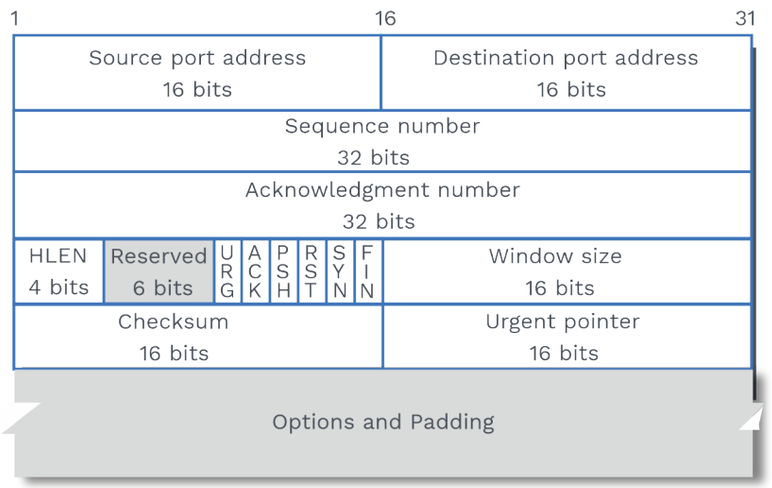
1) Byte number:
TCP count all the data bytes that needs to be transmitted.
Numbers can be started from any random number between 0 to 2^{32}-1.

Both are correct.
Data is sent to Transport Layer from Application Layer with no limitations. Now its Transport Layer duty to divide the data into chunks called as segments. Each segment is a collection of bytes.

2) Sequence number: For the first data byte of the segment, a number is given, where the same value is given in the field of the sequence number of in TCP header.

3) Acknowledgement number: The acknowledgement number defines the number of the next byte that the party expects to receive.
Lets See TCP segment format,

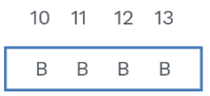
a. Segment



b. Header

Fig. 5.2 TCP Header Format

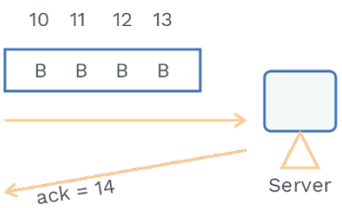
- **Source Port address:** It is a 16 bit address used for port for sending application.
- **Destination Port address:** It is a 16 bit address used for port for receiving application.
- **Sequence number:** It is 32 bit field, In order to ensure connectivity TCP need to make every byte which has to be transmitted as numbered, now the first byte number will be the sequence number.



Example: What will be the value at the sequence number field?

Sol: It is 1010 i.e 10

- **Acknowledgement number:** This field contains expected byte sequence number(i.e. expecting by receiver to get next from sender).



Why ack = 14, Why not 13?
By sending acknowledgement 14 server is saying I have taken bytes from 10 to 13 and now expecting the next segment whose the sequence number should be 14.

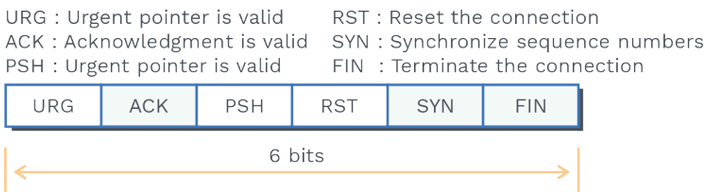
Header length:
- It has 4 bit.
- It defines length of TCP header.

Grey Matter Alert!

- We have minimum and maximum lengths of 20 and 60 bytes respectively.
- But at header length, we have only 4 bits i.e using 4 bits maximum we can go upto 15 bytes.
- It leads to the concept of scaling factor; in this case it is 4 bytes.
- Header length = Header length field value * 4 bytes.

Note:
What is the minimum and maximum length of the TCP header?
Minimum length = 20 Bytes, How? number of essential rows * size of each rows i.e 5 * 4 bytes
Maximum length = 60 bytes, How? Maximum size of options are 40 bytes, 20 + 40 = 60 bytes

- **Reserved bit:** These have 6 bit which is reserved for future use,



- **URG bit:** It tells there is some data which is urgent if the flag of the URG bit is set to 1.
  How one can know, How many bytes are urgent?
  For this reason we have an urgent pointer field.

- **ACK bit:** It tells about the validity of the acknowledgement number.
  Except for request segment, which is used in connection establishment, all the segment may have ACK = 1.

- **PSH bit:** For immediately pushing the entire buffer to receiver application, the PSH is used.

  Note:
  Difference between the URG bit and the PSH bit is that the PSH bit does not give any priority to the data and It just causes all the segments in the buffer to be pushed immediately to the receiving application.

- **RST bit:** It is used for resetting the application. It tells the receiver that something is wrong, please disconnect the resources and buffer.

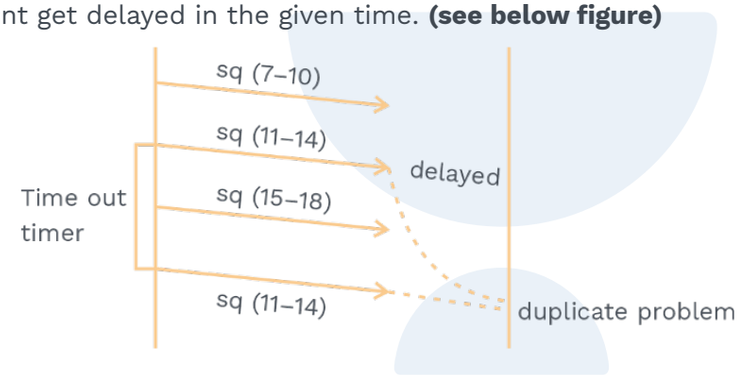
  When should I use the RST bit?
  When normal execution is not possible, there is a need for immediate termination.
  It may result in the loss of the data that are in transmission.

- **SYN bit:** This bit says about the TCP header sequence number field value to the receiver and indicates that the field value is the initial sequence number.

- **FIN bit:** For connection termination, it is used.
  Let's see **"What is wrap-around time"** and How sequence numbers deal with it !
  If the initial sequence number is chosen as S then the sequence number will be used from S to 2^{32}-1 and again from 0 to S.

The time taken to use all the sequence number is called Wrap-Around time.

- In modern computers, the lifetime of the TCP segment is 180 second.
- Entire concept lies in the fact that sequence number should be unique in a given time.
- Other wise otherwise duplicate segment problem will be there if Any segment get delayed in the given time. **(see below figure)**



PRACTICE QUESTIONS

Q2 **What will be the sequence number if we want no wrap around in the Life time of packet considering the bandwidth as B MBps.**

Sol: We know life time of packet is 180 sec.

2^x / B > 180 (let's say x is no. of bits used for sequence number)

2^x > 180 * B

Sequence Number = 180 * B

Number of bits needed for sequence number = $\log_2(180 * B)$

A wrap-around is always needed !! not at all, whenever we run out of sequence number then only wrap-around time is needed

- **Window size:** It is 16 bit field (0 to 65535)
  It defines the size of receiving window determined by the receiver.

- **Checksum:** It is 16 bit field.
  It checks for the error in the TCP header on the mandatory basis but in UDP the checksum is not mandatory.
  Receiver rejects the data that fails in CRC integrity.

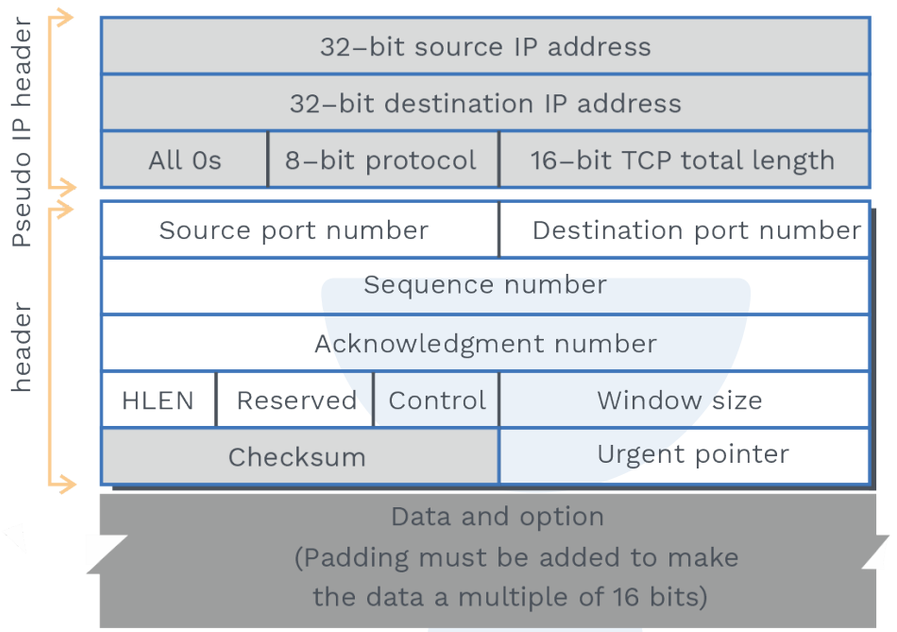


Fig. 5.3 TCP Header Format

Checksum at TCP can be done in 3 section TCP: pseudo IP header, TCP header, Data section (See above figure).

Urgent pointer: It is a 16 bit field.

Which is valid only when the urgent flag is set, it tells what number of byte is urgent in segment.

Note:
Number of urgent bytes = Urgent pointer + 1
End of urgent byte = Sequence number of the first byte in the segment + Urgent pointer

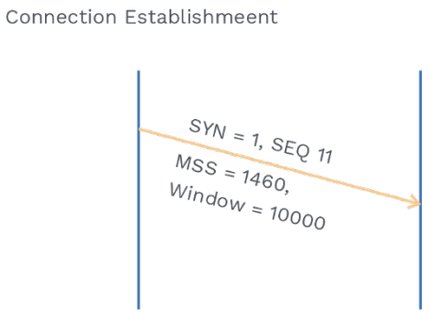
We know TCP is connection oriented, i.e. path are reserved.

TCP has 3 phases for connection oriented services:

- Connection establishment
- Data transfer
- Connection termination

Connection establishment:

Step 1



Why SYN = 1?

It is informing that the client wants to connect, this is why the SYN = 1.

Why SEQ = 11?

It is saying that the starting byte of this packet is 11, **Can it be any other number!** Yes it can be any random number between 0 to 2^{32}-1.

Why MSS = 1460?

This is the maximum segment size which the client can hold.

Why Window size = 29200?

This window size which the client can accommodate is 29200, Actually it can accommodate from 0 to 65535 and more (from options).

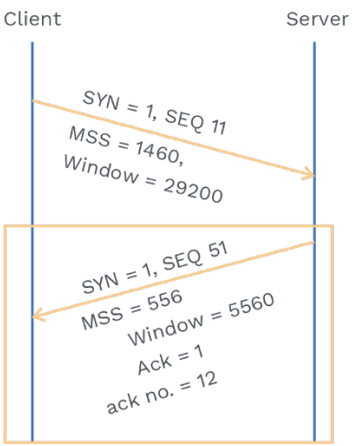
From where do we get MSS?

From option field

Note:

Though the SYN segment cannot carry data, it needs one sequence number.

Step 2



Why SYN = 1?
Now Server also wants to establish connection, that is why SYN = 1.

Why SEQ = 51?
Segment which server is sending its first-byte containing a sequence number = 51.

Why MSS = 556?
Server is saying to the client that I can accept a segment of 556 bytes only.

Why window size = 5560?
It basically tells client that my window size is 5560 bytes.

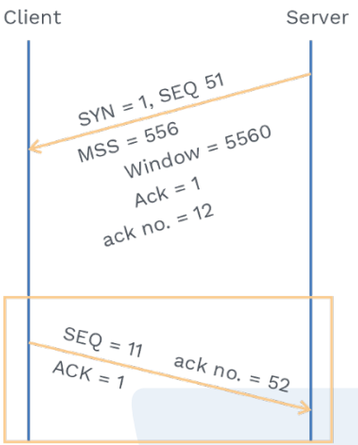
Why ACK = 1?
This means server is telling that it accepted the previous segment which client has sent.

Why is acknowledgement number 12?
Acknowledgement number always signifies the next byte, which is expected by the receiver.
It means the Server has accepted byte having sequence number 11 now expecting 12.

Note:
A SYN + ACK segment cannot carry data, but does consume one sequence number.

Note:
In any TCP segment
If SYN bit = 1 and ACK bit = 0, then it must be request segment.
If SYN bit = 1 and ACK bit = 1, then it must be reply segment.
If SYN bit = 0 and ACK bit = 1, then it must be pure acknowledgement or data segment.
If SYN = 0 and ACK = 0, then this is not possible.

Step 3



Why Seq = 11?
(Since Server ack no = 12, this means server was asking for that byte whose sequence no is 12.) Since, SIN = 0 and ACK = 1, it is a pure acknowledgment. Pure acknowledgment does not consume any sequence number. It will use previously used sequence number.

Why ack no = 52?
As client had taken 1 byte, when the server sent a segment having sequence number 51, the next sequence number that the client is expecting from server is 52.

Note:
If no data is carrying ,It consumes no sequence number by an Ack segment.

Data transfer:
Lets send some data:
Let's say the client has some data (11 bytes) to send, it will tell its sequence number as 12, and acknowledgement number as 52.

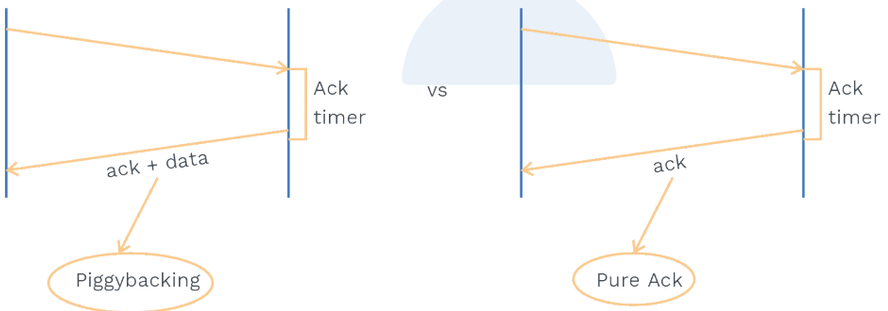
Now, the server has also some data (20 bytes) to send, it will send to the client and tells its seq no = 52 (next byte which client is expecting) and acknowledgement number as 23 (next byte which server is expecting)

Connection termination:

Any of the two parties can close the connection, although it's mainly dependent on the client-side.

Note:

Piggy backing and pure acknowledgement,

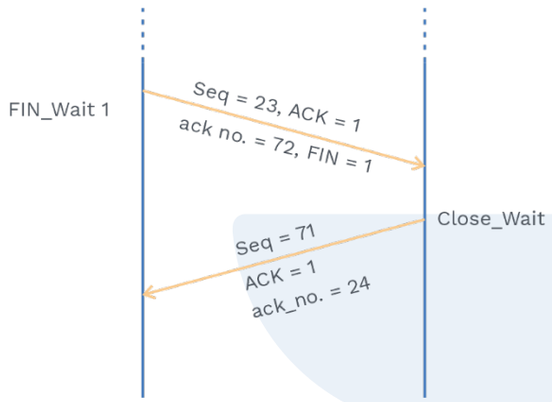


Note:

A TCP connection is terminated using the FIN segment where the FIN bit is set to 1.

Why Seq = 23?
Client is saying that my first byte starts with 23 only.

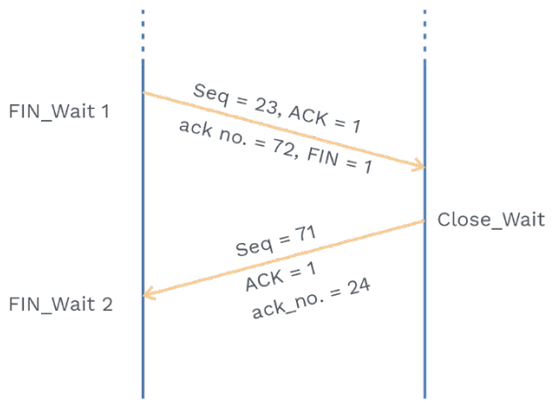
Why FIN = 1?
Client says that,It wants to end the connection, and it is going under FIN_WAIT 1 state.



Now the server sends an ACK to the client, and delivers outstanding data in its queue
to the application, and goes to the CLOSE-WAIT state.

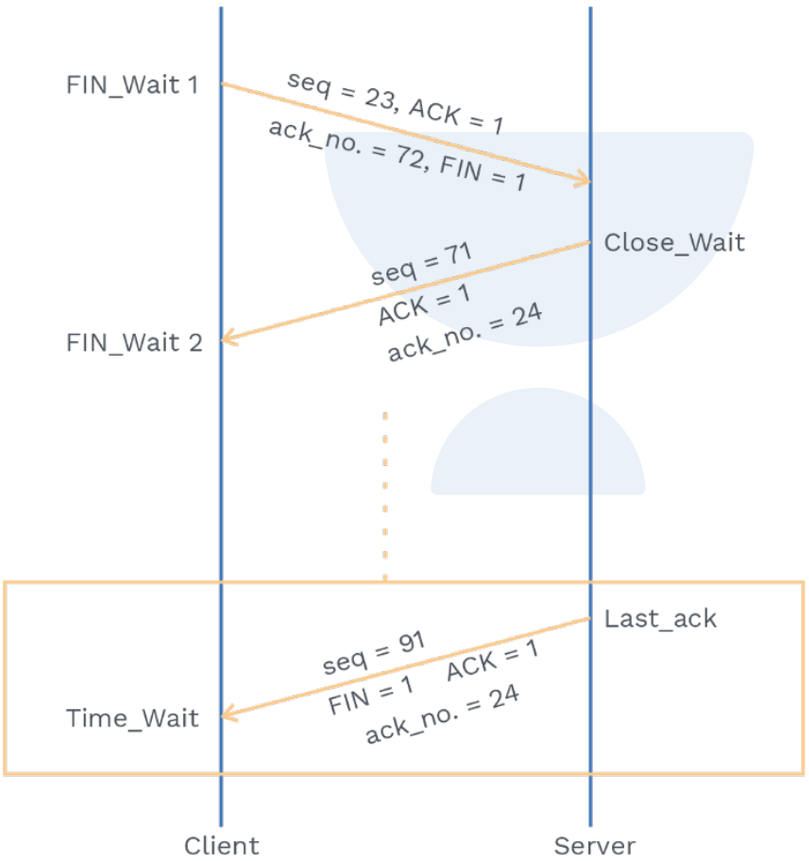
Why seq = 71, when the server is sending ACK?
Since this is pure acknowledgement. It does not use any sequence number.

Why acknowledgement no = 24?
Server is saying, if you want the next byte to be sent, then its sequence number is 24.
After receiving the acknowledgement from the server, the client enters the FIN_WAIT_2 state.



Note:
After Ack is received from server. Server releases its buffers. Though the client can still send pure acknowledgements to the server but not any data. But both data and ack server can send to client.

If server wants to close a connection, then it will send a FIN segment. After receiving FIN segment client goes into a Time wait state and sends ACK to Server saying that it is also freeing up my buffer.



Note:
The TIME_WAIT state allows the client to resend the final acknowledgement if it gets lost and the time spent by the client in TIME_WAIT maybe 2 min or 1 min it depends on the implementation of the protocol.

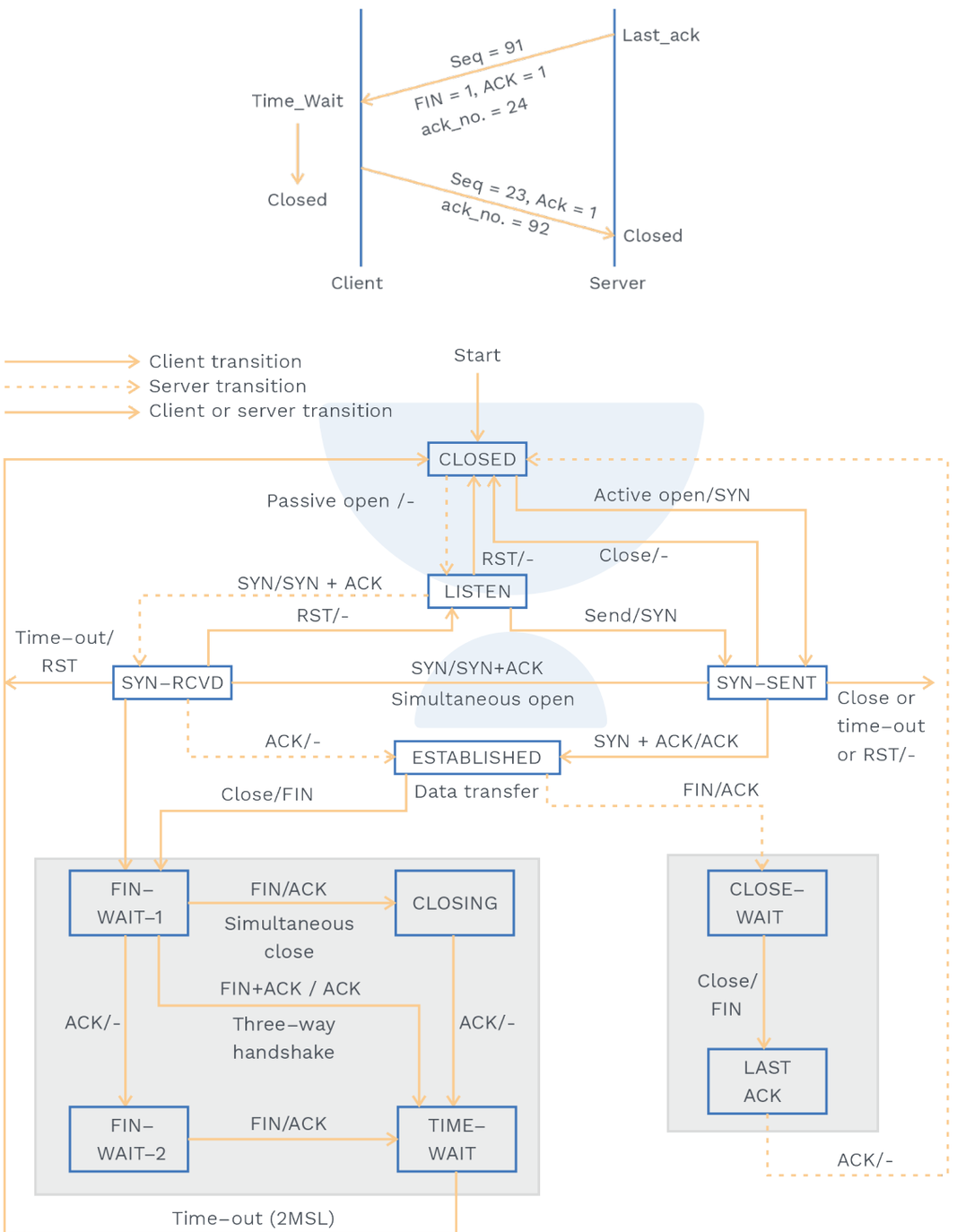


Fig. 5.4 TCP State Transition diagram

PRACTICE QUESTIONS

Q3 **What would be size of the window for host, if the value of receiver window is 1000 bytes and the value of cwnd is 999 bytes?**

Sol: Size of window for Host is min (rwnd, cwnd) => min(1000, 999) => 999.

rwnd → receiver window size

cwnd → congestion window size

Q4 **How Error control is provided by TCP?**

Sol: TCP provides reliability using error control by finding out what are segments which have been lost, by detecting corrupted segments, by finding out of order segments.

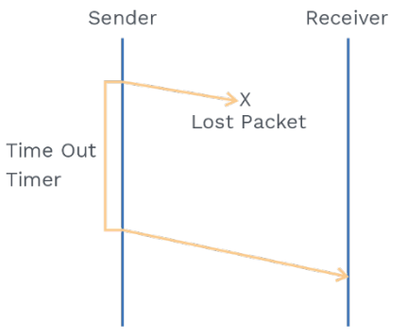
Note:
TCP has 3 main tools for detecting and correcting errors Checksum, acknowledgement and time out.

1) Checksum: If the checksum field is corrupted, then it means the segment has some error, and it will be discarded.
2) Acknowledgement: It is used for maintaining the confirmation of receiving the data segments.
3) For understanding the **Time out,** lets see how retransmission works in TCP.

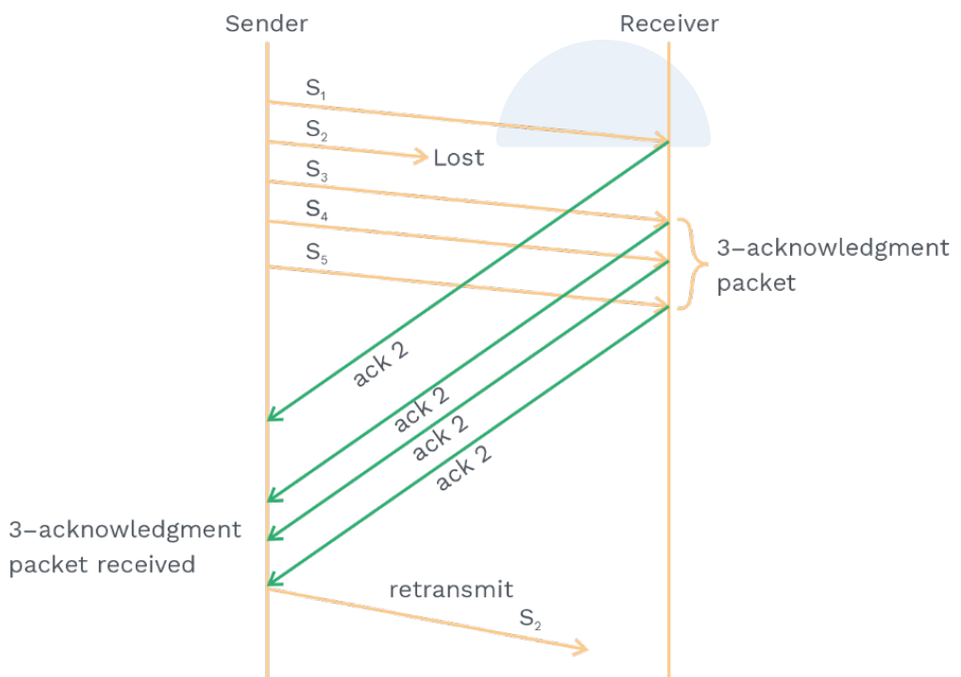
When the TCP segments get lost, then receiver needs to tell the sender using acknowledgement so that the sender can retransmit the packet.

Basically there are 2 cases in which the sender retransmits the packet.
1) **Timeout occurs**
2) **Three duplicates acknowledgements come back to the sender**

When Time Out occurs then sender will send the packet again.



- It leads to the possibility of strong congestion.
- When 3 duplicate acknowledgements come back to the sender, then it assumes that the corresponding segment is lost. Without waiting for the completion of time Out timer sender will retransmit the packet. (See the diagram below)
- After having the retransmitted S2, the Receiver sends the acknowledgement asking for S6 directly from the sender, and it will not ask for 3,4,5.
- It leads to the possibility of mild congestion.



Now, lets see congestion window.

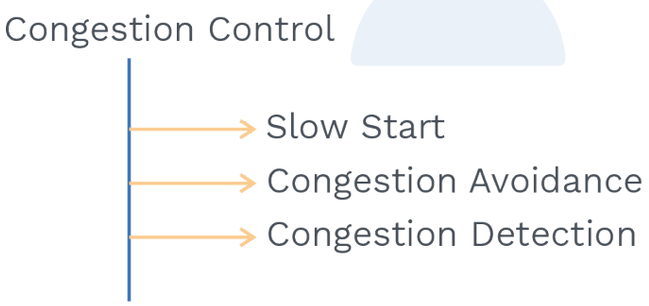
Sender has the information of rwnd size and cwnd size.

Note:
Actual swnd = min(rwnd size and cwnd size)
Swnd: Sender window
rwnd: receiver window
cwnd: congestion window

Congestion: It refers to the state of a system which slows down the network performance due to heavy traffic, and we can't avoid congestion completely.

Congestion control technique:
There is an assumption here, receiver window size (rwnd) is much larger than congestion window size (cwnd), so the sender window size is always equal to cwnd.

1) With this technique either we can prevent congestion before it happens.
2) We can remove congestion after it has happened.



Slow start phase:
The slow start algorithm is based on the idea that the size of the congestion window (cwnd) starts with 1 maximum segment size (MSS).

When will MSS be determined ! During the connection establishment phase.

- From where will we get MSS during the Connection establishment phase! From Options.
- The size of the window will increases 1 MSS each time one acknowledgement arrives.

Note:
Algorithm starts slowly, but grows exponentially.

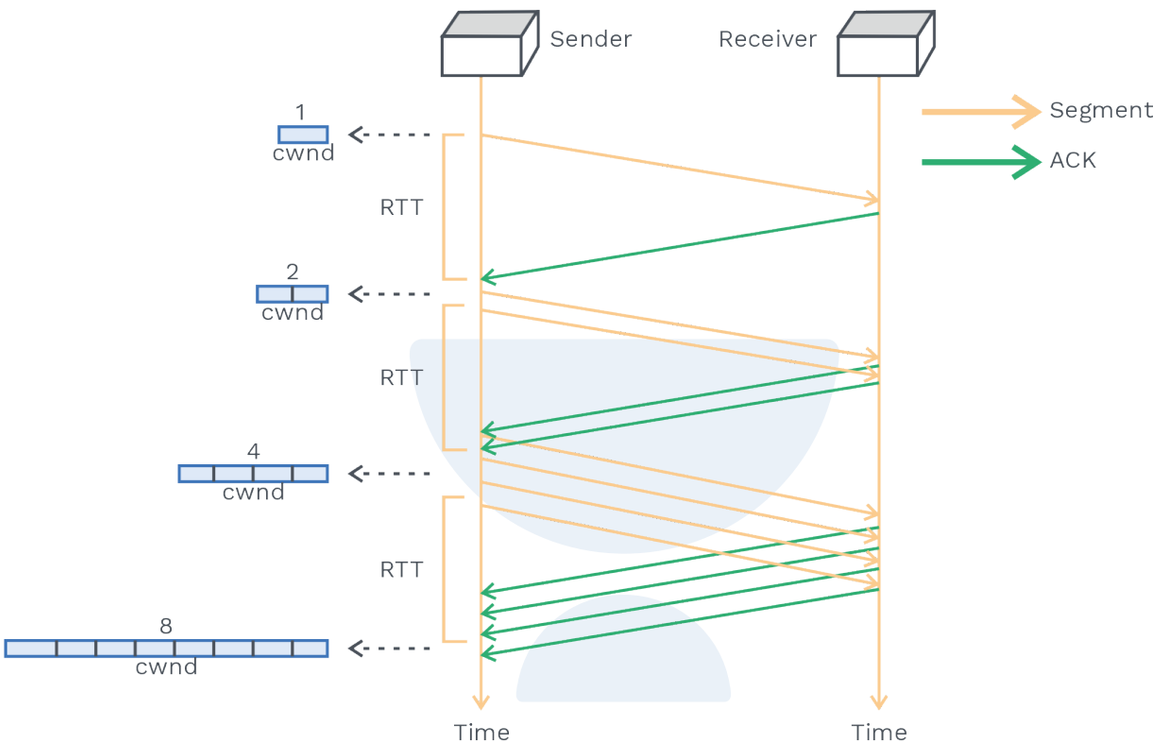


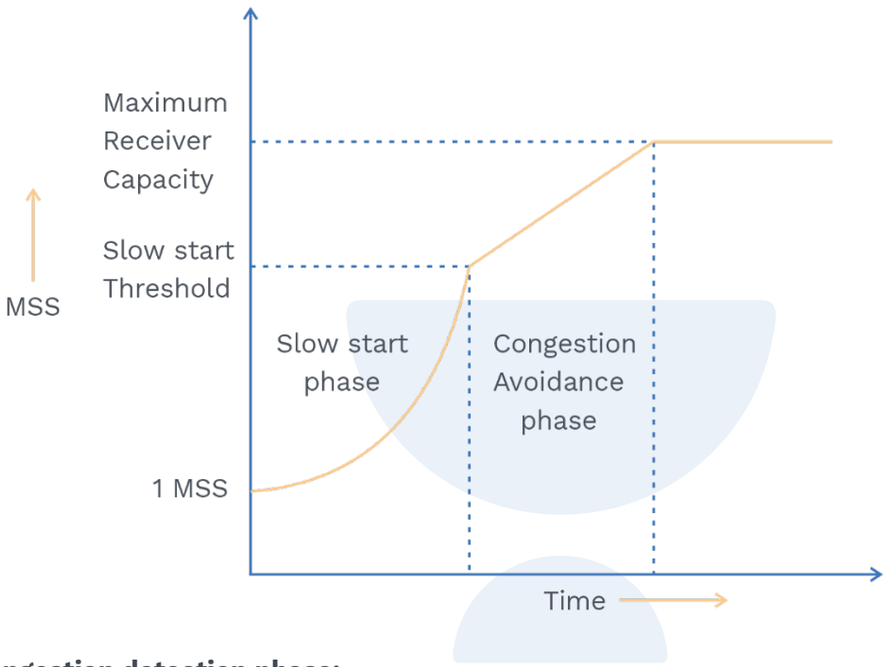
Fig. 5.5 Diagrammatic Representation of Congestion Control

Note:
In the slow start algorithm, the size of the congestion window increases exponentially until it reaches a threshold.

Congestion avoidance phase:
We need to avoid congestion before it happens, it must slow down this exponential growth.
So, in this phase, the cwnd is incremented in a linear manner, i.e. after every ack receiving by the sender.
The sender increments the cwnd size by 1 mss.

cwnd: congestion window

Note:
This phase will go until the congestion window size becomes equal to the receiver window size or congestion is detected.



Congestion detection phase:
Case 1: When the timeout timer expires before receiving the acknowledgement for a segment. This case suggests a stronger possibility of congestion in the network.
What is the solution then!

- Sender in the slow start can set the half the size of current cwnd as the threshold.
- Decreasing the congestion window size to 1 MSS and Resume the slow start phase.

Case 2: When 3 duplicates acknowledgements are received. This case suggests the weaker possibility of congestion in the network.
What is the solution then!

- Sender should set the slow start threshold to half of the current congestion window size.
- Decreasing the congestion window size to slow the start threshold and resume the congestion avoidance phase.

USER DATAGRAM PROTOCOL

It is unreliable and connectionless protocol.

Why is UDP important?

When process communication depends on small message transfer and not on reliability, then UDP is important.

It does not guarantee in-order delivery, and it does not provide congestion control mechanism.

UDP header:

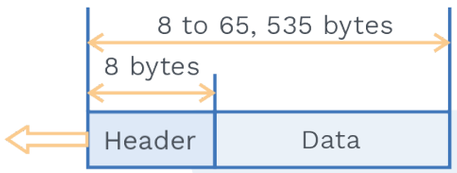


Fig. 5.5a. UDP user Datagram

Fig. 5.5b. Header Format

- **Source Port number:** It is the 16 bit field, It is the port number used by the process running on the source port.
  If the source host is the server, the port number, in most cases, is a well-known port number.
- **Destination Port number:** It is the 16 bit field, It identifies the port of the receiving application.
- **Total length:** It is the 16 bit field; It defines the total length.

  Total Length = Length of UDP Header + Length of data.
- **Checksum:** It is a 16 bit field. It is calculated on UDP Header, IP pseudo-header and data. Checksum calculation is not mandatory in UDP.

Previous Years' Question

Q) In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, and the value of total length is 400, and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are:

a) Last fragment, 2400 and 2789
b) First fragment, 2400 and 2759
c) Last fragment 2400 and 2750
d) Middle fragment 300 and 689

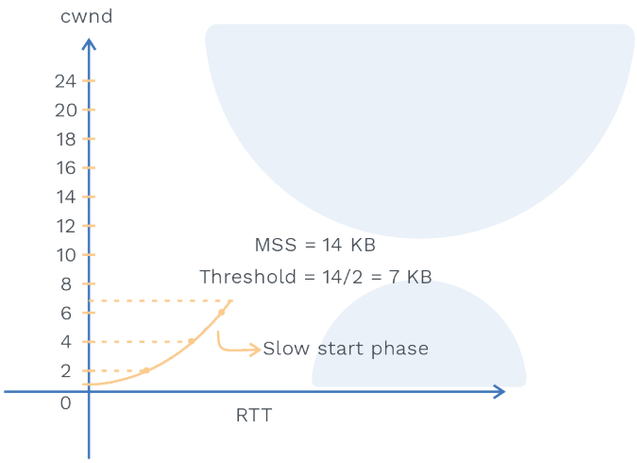
Sol: c) **(GATE-2013)**

Note:
Size of the UDP header is fixed.

PRACTICE QUESTIONS

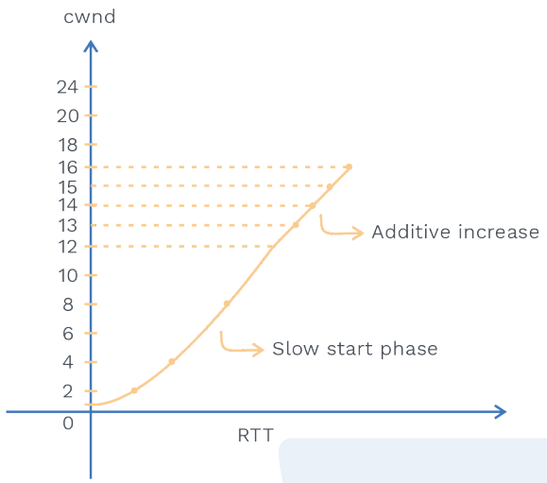
Q5 **Draw the graph if the congestion window size when time out occurs is 14KB in the slow start phase?**

Sol:



Q6 **Draw the graph to show how additive increase will behave if congestion window size when time out occurs is 24 KB?**

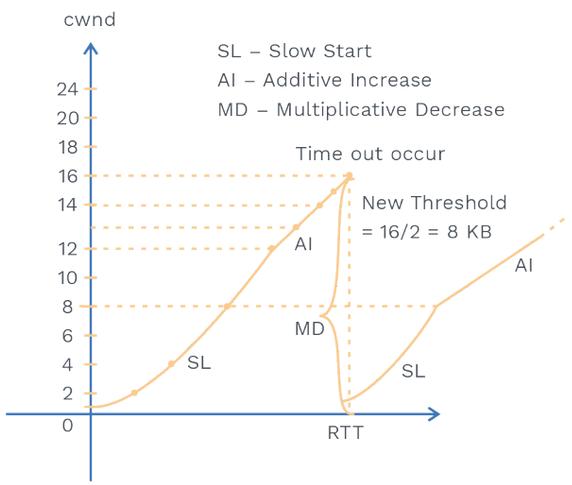
Sol: Threshold = 24 / 2 = 12. Till 12 KB it will be in slow start phase and after 12 KB it will be in additive increase.



In additive increase it will go to the MSS or Time Out occurs.

Q7 **Draw the graph to show how additive increase will behave if congestion window size is 24 KB and initial threshold is 12KB and time out occurs at 16KB?**

Sol: When Time out occurs at 16KB it will go into slow start phase.

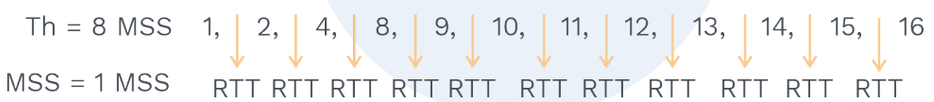


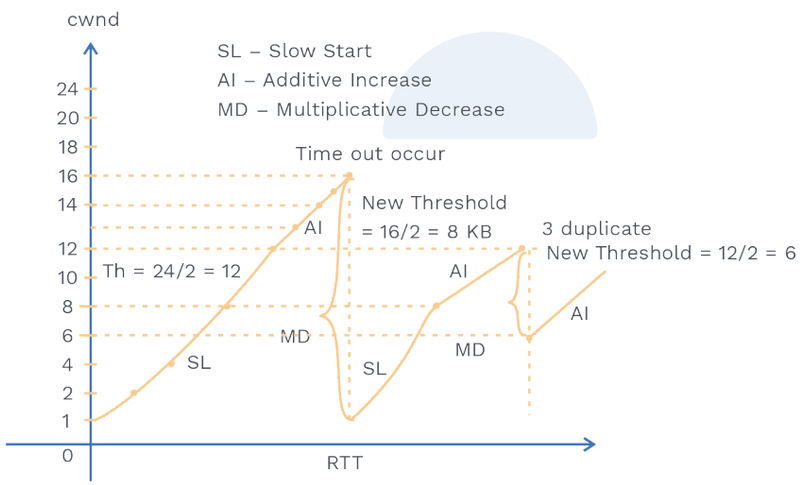
Q8 **Draw the graph to show how additive increase will behave if congestion window size when time out occurs is 24 KB, and Time out occurs at 16KB and after that show, what will happen when window size is 12KB and 3 acks event happens?**

Sol: When window size is 12 KB, and 3 ack event happens it will go into congestion avoidance phase.

Q9 **If congestion window size when time out occurs is 16 MSS, after how many RTT sender will reach 16 MSS?**

Sol: **after 11 RTT,**



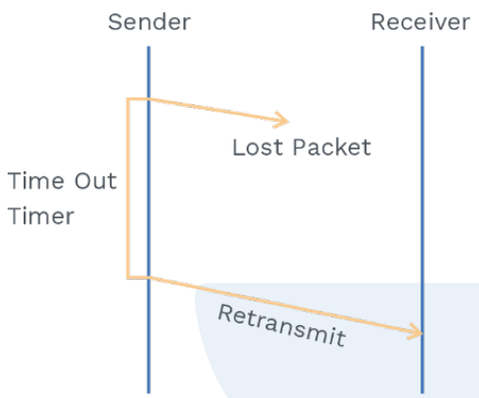


TCP timers:

There are types of timers,

- Retransmission timer
- Persistence timer
- Time wait timer
- Keep alive timer

Retransmission timer: It is basically used to retransmit lost segments. Sender starts the timer when it transmits the packet; the timer stops when the sender receives the acknowledgement.
Retransmission Timer is also called Time out timer.



How Time Out (TO) timer can be calculated.
In real scenario two cases may arise in which TO timer can be calculated,

1) High traffic (It may increase)
2) Low traffic (It may decrease)

There are 3 algorithm which can be used to calculate TO Dynamically.

1) Basic algorithm:

Lets see using example,
In TCP, the initial RTT is 12 msec. The acknowledgements for the first two segments are received in time 17 msec, 22 msec. Find the time out timer value for the first two segments using a basic algorithm. Use α = 0.6.
Here, α is called smoothing factor where $0 <= \alpha <= 1$
(value will be always given in questions)

For first segment:
Initial Round trip time (IRTT) = 12 msec.
Time out Timer (TO) = 2 * RTT = > 24msec.
Actual Round trip time (ARTT) for first segment = 17 msec.

For second segment:
Next round trip time (NRTT) =

$$NRTT = \propto IRTT + (1 - \propto) ARTT$$

$$= 0.6 * 12 + 0.4 * 17$$

= 14 msec

So, for second segment IRTT = 14msec

TO = 2 * 14 = 28msec

Actual Round trip time (ARTT) for second segment = 22 msec.
This is how basic algorithm computes Time out timer.

2) Jacobson's algorithm:

In TCP, the initial RTT is 12 msec, and the initial deviation is 7 msec. The acknowledgements for the first two segments are received in time 22 msec, 12 msec.
Find the time out timer value for the first two segments using Jacobson's Algorithm. Use α = 0.6.
For first segment,

IRTT = 12 msec

ID = 7 msec

TO = 4 * ID + IRTT

4 * 7 + 12

40 msec

ARTT = 22msec
Actual deviation = | ARTT - IRTT | = >| 22 - 12 | = 10msec

For second segment:

$$NRTT = \propto IRTT + (1- \propto) ARTT$$

$$= 0.6 * 12 + 0.4 * 22$$

= 16 msec

So for second segment, IRTT = 16msec

$$ND = \propto ID + (1- \propto) AD$$

$$= 0.6 * 7 + 0.4 * 10$$

= 8.2 msec

So for second segment, ID = 8.2msec

TO = 4 * ID + IRTT

4 * 8.2 + 16

48.8 msec

ARTT = 12msec
Actual deviation = | ARTT - IRTT | = >| 12 - 16 | = 4msec

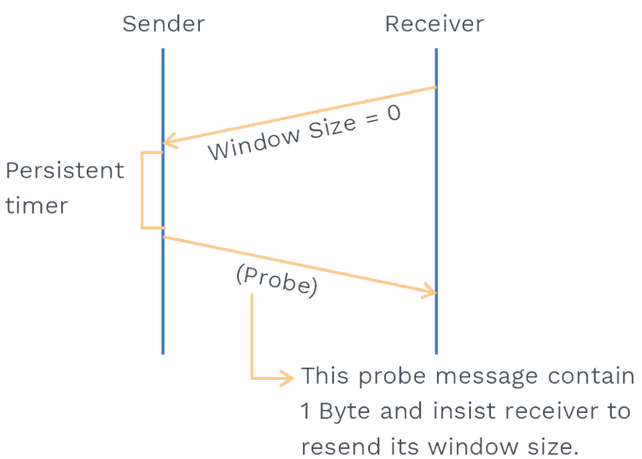
3) Karn's modification states:
Since actual RTT is not available, there is no need to find Time out timer we can double the time out timer (TOT) whenever the timer times out and make a retransmission.

Persistence timer:

- It is used to deal with a Zero window size situation.
- If the receivers announce that its window size is zero then the sender will stop transmitting and wait for an acknowledgement.

Note:
There is no retransmission if Ack segment is lost, and also the Ack segments are not acknowledged.

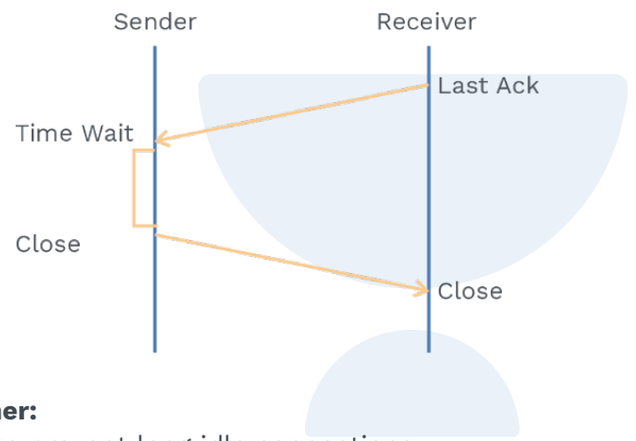
- There might be a case when the receiver has announced that it has a zero window size and because of this sender, was waiting and later when the receiver has gained a buffer for window and sent a segment to sender to update but this segment get lost now sender is still waiting for acknowledgement from the receiver, This is **deadlock state.**
- Inorder to overcome from deadlock situation, TCP uses persistence timer for each connection.



If the sender does not receive any message even after the probe message, it will double the persistent timer size.

Time wait timer:

- TCP uses a time wait timer during connection termination.
- Sender starts the time wait timer after sending the ACK for the second FIN segment, and It allows it to resend the final acknowledgement if it gets lost.
- What does it basically do? It prevents the just close segments to response it again to some other application.



Keep alive timer:

- It is used to prevent long idle connections.
- Client opens a TCP connection to a server, transfers some of the data, and becomes silent. There may be the possibility that the client has crashed. In this case, the connection remains open forever.
- In order to overcome this situation server will use Keep alive timer, so that it gets to know that whether client is down or not.

Improving quality of service using traffic shaping:

In traffic shaping two technique are used

1) Leaky bucket

2) Token bucket

Leaky bucket:

If the bucket has a small hole at the bottom, then the rate at which water flows out from the hole does not depend on how much rate water enters the bucket. It always flows out at a constant rate.

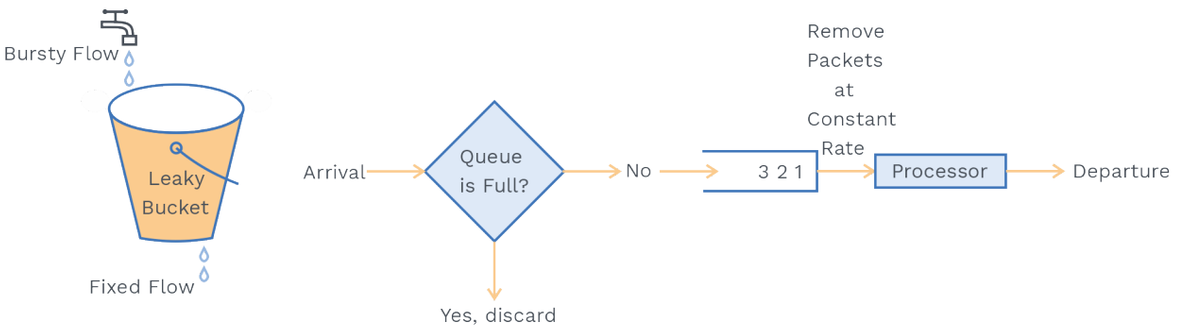


Fig. 5.6 Leaky Bucket Implementation

In a similar way, the leaky bucket algorithm can smooth the bursty traffic.

Token bucket:

- In the Leaky bucket, there is a chance when Host remains idle when there is no data to send.
- And when the host has some data then also it sends data at an average rate which affects the performance of system.
- The token bucket allows bursty traffic at a regulated maximum rate.

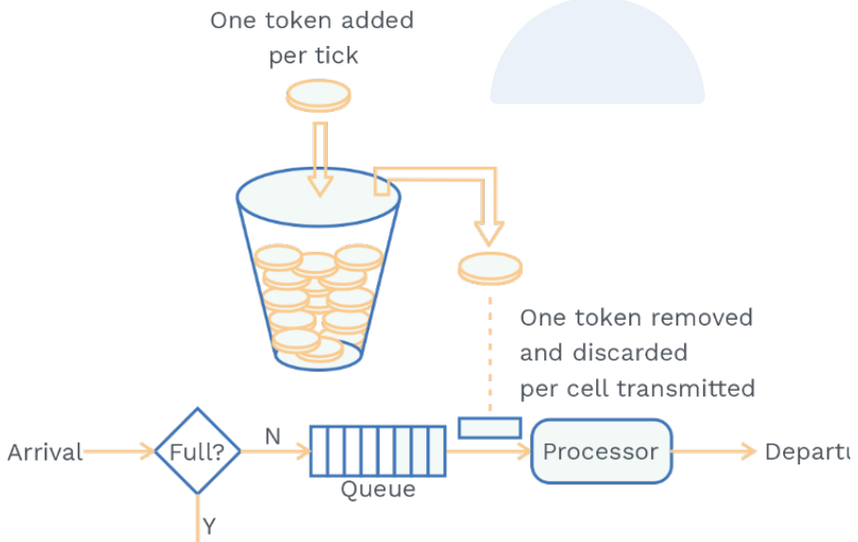


Fig. 5.7 Diagrammatic Representation of Token Bucket

Assume that there are 50 tokens, and the Host removes one token for every byte of data sent. The Host was idle for 50 units. In that time, the bucket collected 2500 Tokens, Now If the Host wants to consumes all these Token in one unit of time, then the rate should be 2500 byte/unit.

Chapter summary

- The objective of the Transport layer is to deliver the packet from process to process.
- Socket address is a combination of IP address and port address.
- Transport layer has two major protocol TCP and UDP.
- TCP Keep counts its segment Byte Number, Sequence Number and Acknowledgement Number.
- TCP count all the data bytes that needs to be transmitted.
- TCP has 3 phases for connection-oriented services:
  Connection Establishment
  Data transfer
  Connection termination
- In any TCP segment:
  If SYN bit = 1 and ACK bit = 0 , then it is request segment.
  If SYN bit = 1 and ACK bit = 1 , then it is reply segment.
  If SYN bit = 0 and ACK bit = 1 , then it is pure acknowledgement or data segment.
  If SYN = 0 and ACK = 0, then this is not possible.
- A SYN + ACK segment cannot carry data, but does consume one sequence number.
- A SYN segment cannot carry data, but it consumes one sequence number.
- If the server wants to close a connection, then it will sent a FIN segment.
- TCP has 3 main tools for detecting and correcting errors:
  Checksum, acknowledgement and time out.
- **Congestion:** It refers to the state of a system which slows down the network performance due to heavy traffic and we can't avoid congestion completely.
- Basically there are 2 cases in which the sender retransmits the packet:
  Either timeout occurs or
  3 duplicates acknowledgements come back to sender
- **UDP:** It is an unreliable, and connectionless protocol.
- **TCP Timers:**
  Retransmission timer
  Persistence timer
  Time wait timer
  Keep alive timer

6 Application Layer

Having discussed all the types of layers, we have now reached the layer where all applications are found.
In this chapter, we will discuss some real network applications.
Application layer assumes that there is an imaginary direct connection through which they can communicate.

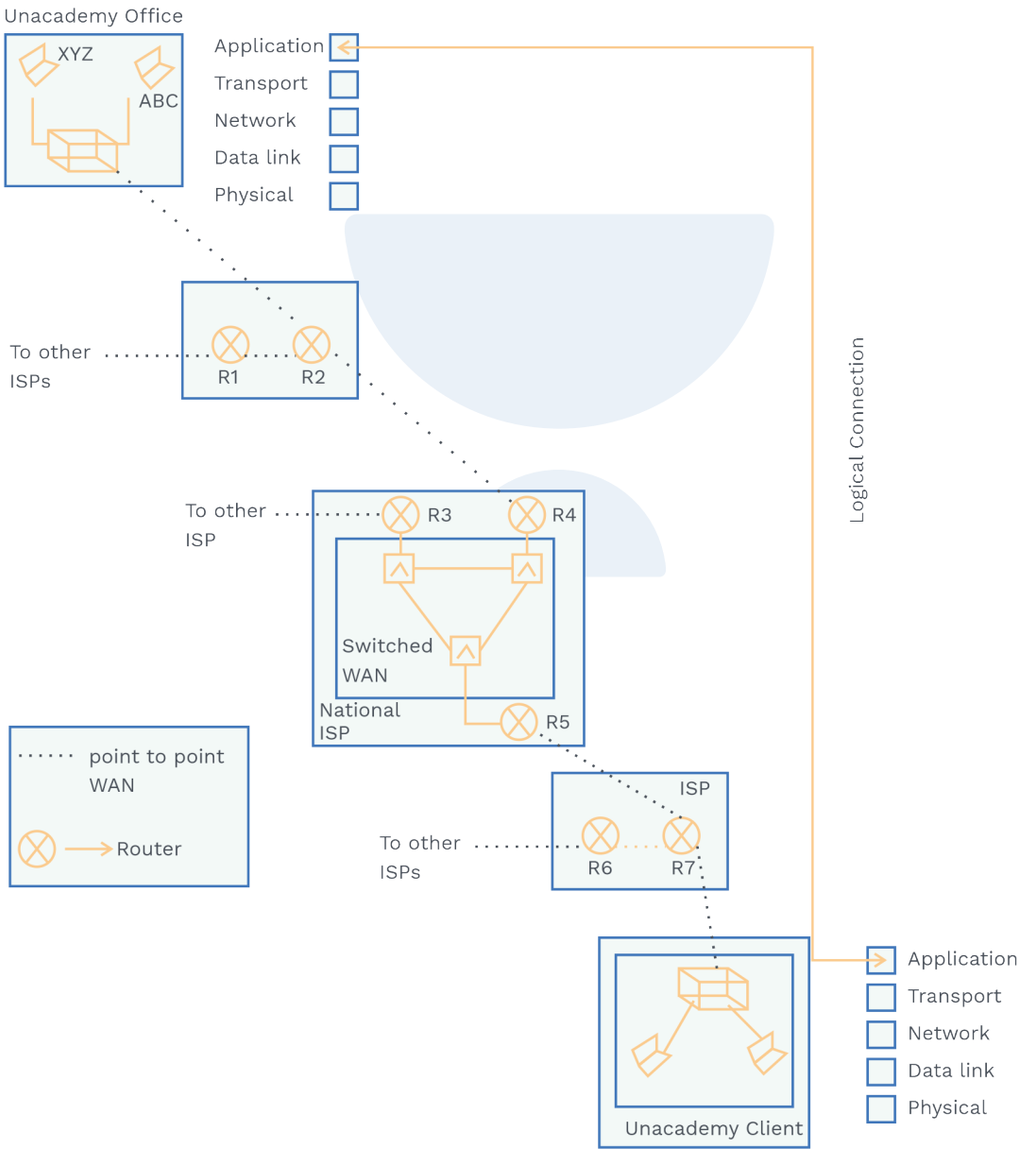


Fig 6.1 Shows The Idea Behind This Logical Connectivity.

6.1 DNS

Hey learners! Do you know which protocol handles naming within internet? DNS.
Let's discuss about DNS.

The DNS name space:

- Managing a large set of names is really non–trivial.
- For the Internet, the top of the naming hierarchy is managed by an organization called ICANN (Internet Corporation for Assigned Names and Numbers).
- Internet is divided into many top–level domains where each domain covers many hosts.
- Each domain is divided into sub–domains, and these sub domains are further divided.
- All the domains can be represented in the form of a tree.
- The leaves of the tree indicate domains that have no sub–domains.
- A leaf domain may contain a single host or it may represent a company that contains thousands of hosts.

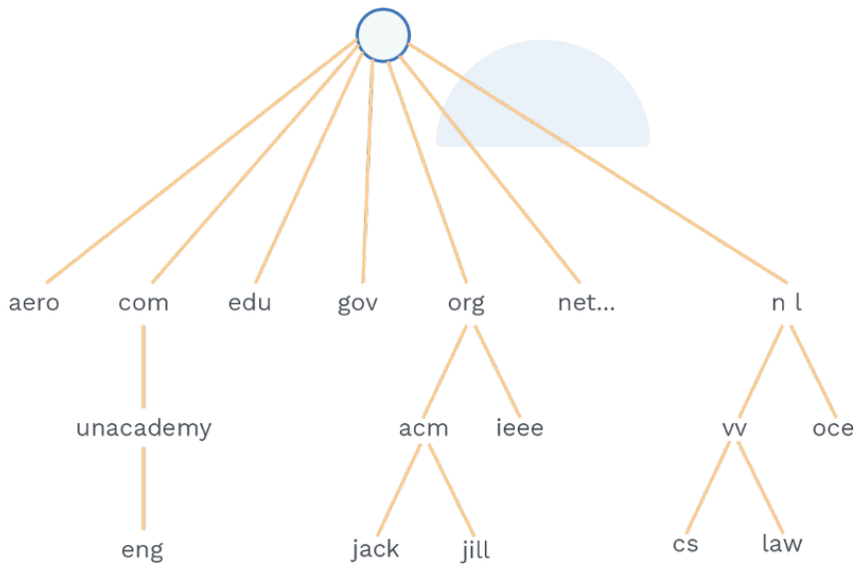


Fig. 6.2 Portion Of The Internet Domain Name Space

Domain resource records:

- Every domain, whether it is a single host or a top-level domain, has a set of resource records. These records are present in the DNS database.
- A resource record has five-tuples:
  <Domain_name, Time_to_live, Class, Type, Value>

Name servers:

- The DNS name space is divided into non-overlapping zones.
- It distributes the information among many computers.
- Name server divides the whole space into many domains based on the first level.
- The root stands alone and creates as many domains (subtrees) as possible, these are first–level nodes.
- We have a hierarchy of servers in the same way that we have a hierarchy of names.

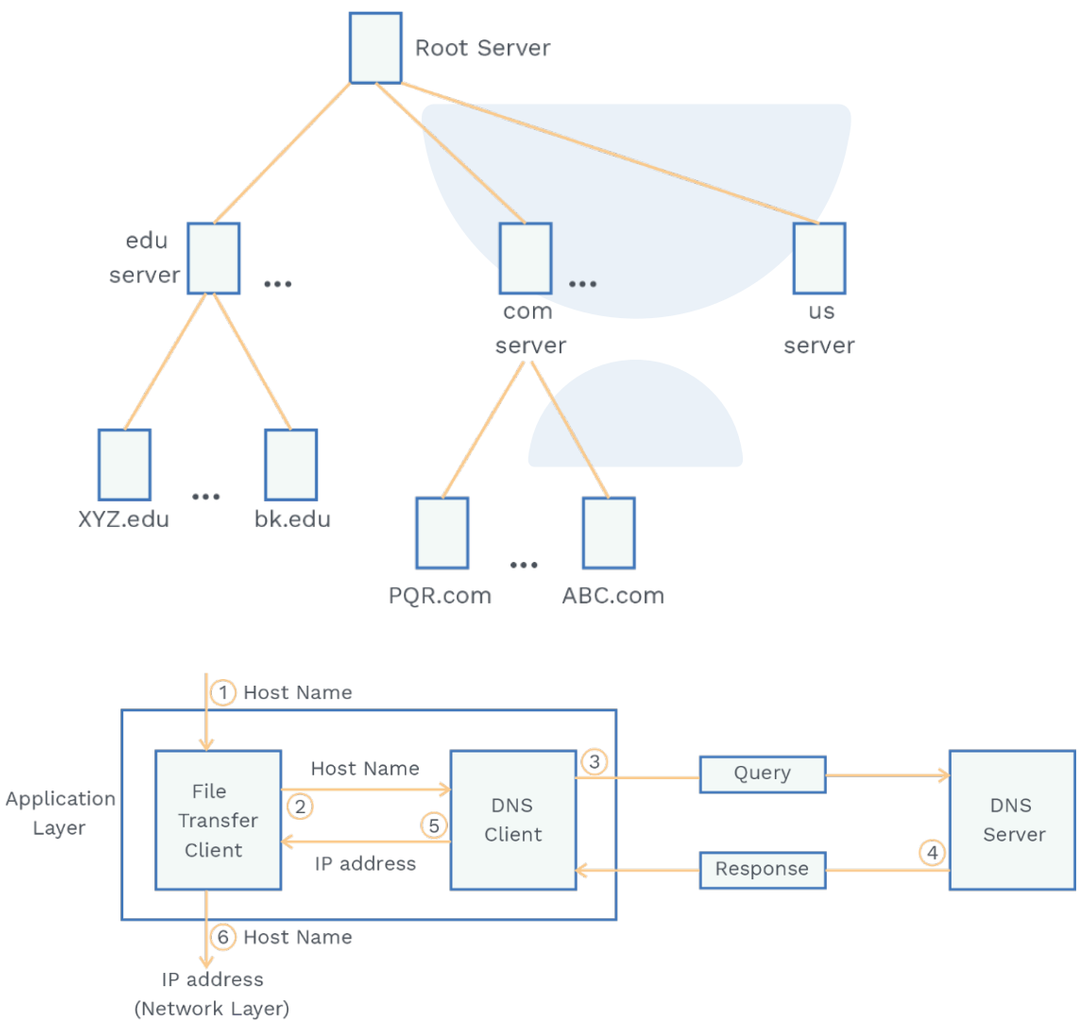


Fig. 6.3 Purpose Of DNS

- The TCP/IP suits require the IP address of the file transfer server to establish the connection.

The steps below are used to map the hostname to IP address:

1) The user sends the hostname to the file transfer client.
2) The file transfer client sends the hostname to the DNS client.
3) Each computer, after being booted knows the address of its DNS server. DNS client sends query message to a DNS server. DNS query includes file transfer server name and it is sent using known IP address of DNS server.
4) The DNS server responds with the IP address of the desired file transfer server.
5) DNS server sends the IP address to the file transfer client.
6) The received IP address is being used by file transfer client to access file transfer server.

Note:

- DNS uses port number 53.
- DNS is stateless protocol.

There are two ways in which DNS can contact the server:
Method 1: Iterative Approach

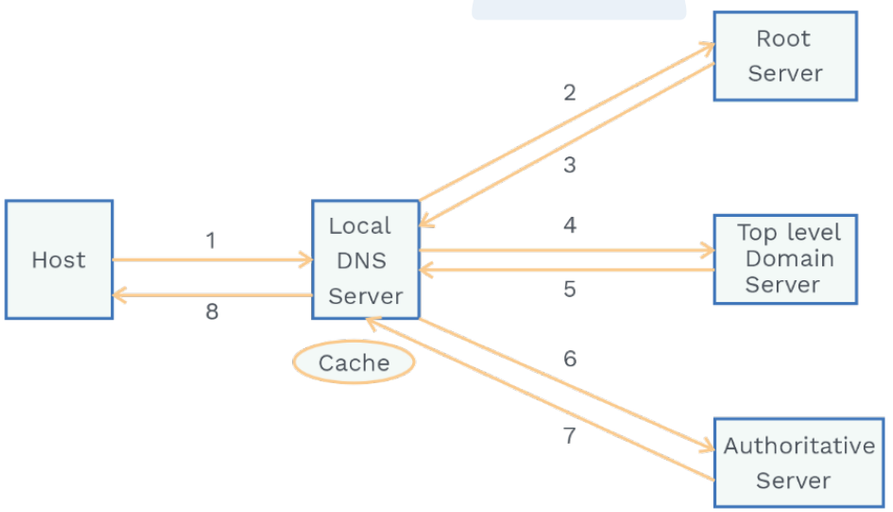


Fig. 6.4 Iterative Approach

Lets say www.unacademy.com needs to be find using DNS iterative approach
Step 1: Host will ask Local DNS server do you have www.unacademy.com address, If no Go to step 2, else send me

Step 2: Local DNS Server will ask Root Server do you have www.unacademy.com address,

If (false) // i.e no information about address at Root Server
Local DNS Server: Ask Top Domain Server
else
Local DNS Server: Take address from Root Server // Step 3

Step 4: Local DNS Server will ask Top Level Domain Server do you have www.unacademy.com address,

If (false) // i.e no information about address at Top Level Domain Server
Local DNS Server: Ask Authoritative Server
else
Local DNS Server: Take address from Top Level Domain Server // Step 5

Step 6: Local DNS Server will ask Authoritative Server do you have www.unacademy.com address,

If (true) // i.e information present about address at Authoritative Server
Local DNS Server: Take address from Authoritative Server // Step 7

Step 8: Local DNS server will send the address of www.unacademy.com to host and also local DNS server maintains the address mapping in cache.

Method 2: Recursive Approach

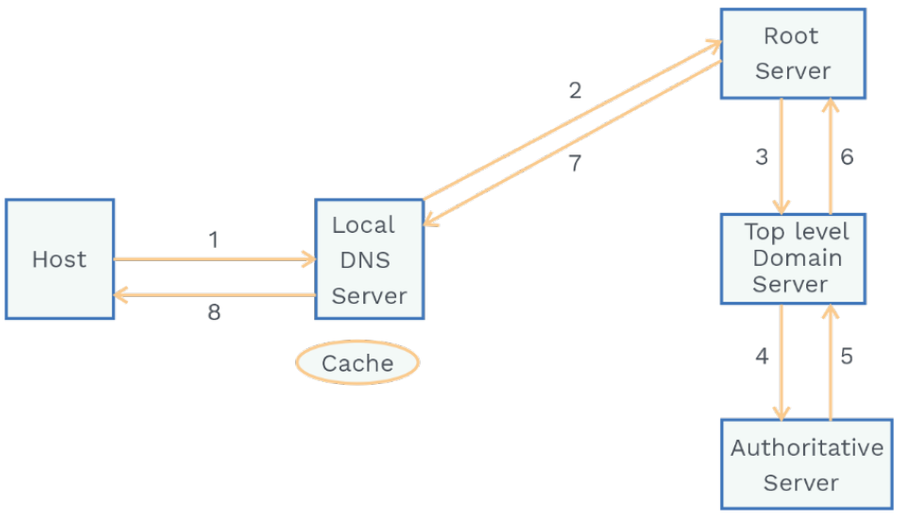


Fig. 6.5 Recursive Approach

Step 1: Host will ask the Local DNS server do you have www.unacademy.com address, If not Go to Step2

Step 2: Local DNS Server will ask Root Server do you have www.unacademy.com address,

If (false) // i.e no information about address at Root Server
ask Top Level Domain Server

Step 3: Root Server will ask Top Level Domain Server do you have www.unacademy.com address,

If (false) // i.e no information about address at Top Level Domain Server
Ask Authoritative Server

Step 4: Top Level Domain Server will ask Authoritative Server do you have www.unacademy.com address,

If (true) // i.e information present about address at Authoritative Server
Give address back

Step 5: Give Information to Top Level Domain Server.
Step 6: Give information back to Root server.
Step 7: Give information back to Local DNS server.
Step 8: Give information back to Host and also DNS will maintain address mapping in its cache.

6.2 HYPERTEXT TRANSFER PROTOCOL (HTTP)

- HTTP defines how the client–server programs are written to retrieve web pages from the web.
- An HTTP client sends an HTTP request and an HTTP server returns a response.
- HTTP uses the services of TCP. A connection has to be established between client and server before any transaction that takes place between client and server.
- The clients and servers need not worry about erroneous/corrupted messages exchanged or loss of any message because the underlying transport layer protocol is TCP which is highly reliable.

Note:
HTTP prior to version 1.1 specified non–persistent connections, while persistent connections are default in version 1.1, but it can be changed by the user.

Nonpersistent connections:

- One TCP connection is established for each request/response in a non–persistent connection.

- Three steps are involved in this strategy:
  1) The client initiates a TCP connection and sends a request.
  2) The server sends the response and terminates the connection.
  3) The client reads the data until it encounters an end-of-file marks it then closes the connection.

Grey Matter Alert!

If a file contains links to M different pictures in different files (all located on the same server), the connection must be opened and closed M+1 times. The non–persistent strategy imposes a high overhead on the server because the server needs M+1 different buffers every time a connection is opened.

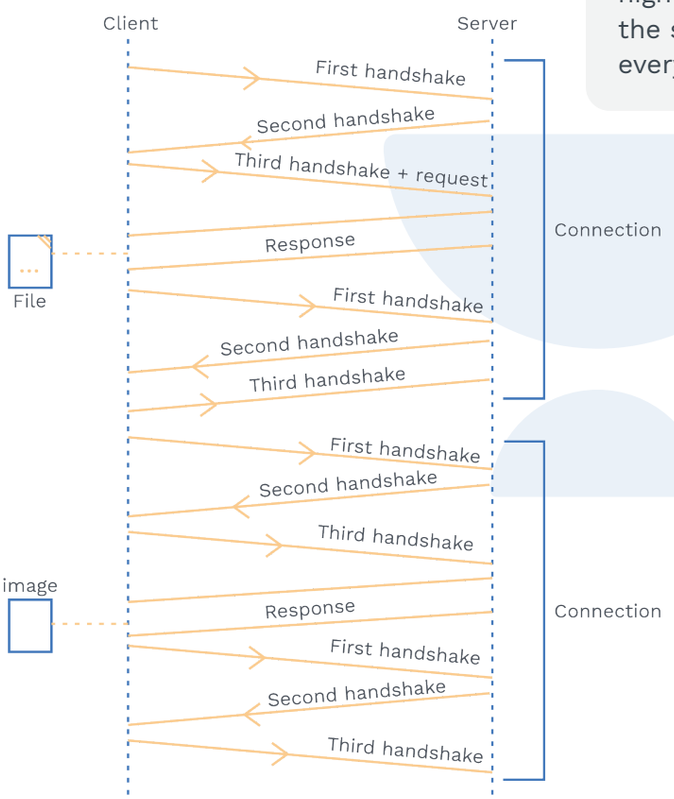


Fig. 6.6 Non–Persistent–Connection

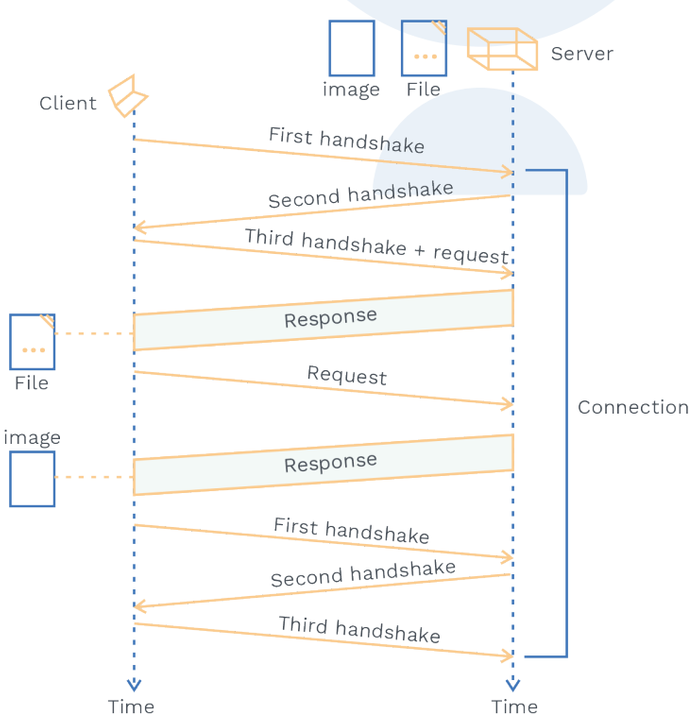
Persistent connection:

- By default HTTP 1.1 uses persistent connection.
- In persistent connection, the connection is left open for more requests.
- If the client requests or if the timer times out, server can close the connection.
- Resources and Time are saved using a persistent connection.

- The method field defines the HTTP request type. In HTTP 1.1, several methods are defined.

Method	Action
GET	Request a document from server
HEAD	Request information about a document but not the document itself
PUT	Sends a document from the client to the server.
POST	Sends some information from the client to server
TRACE	Echoes the incoming request
Delete	Removes the web page
Connection	Reserved
Options	Enquires about available options

Fig 6.7 Different Methods of HTTP



6.3 FILE TRANSFER PROTOCOL (FTP)

- FTP is a standard protocol provided by TCP/IP for copying a file from one host to another.
- Can we transfer files using HTTP?
  Yes, we can, but the FTP is the better choice to transfer bigger files.
- Basic model of FTP has three components – the user interface, the client control process and the client data transfer process.
- The server has a server control process and server data transfer process.

Grey Matter Alert!

Hey learners!! What is cookie?, Well cookie is information about a client gathered by server in a file or string. The information might include domain name of the client.

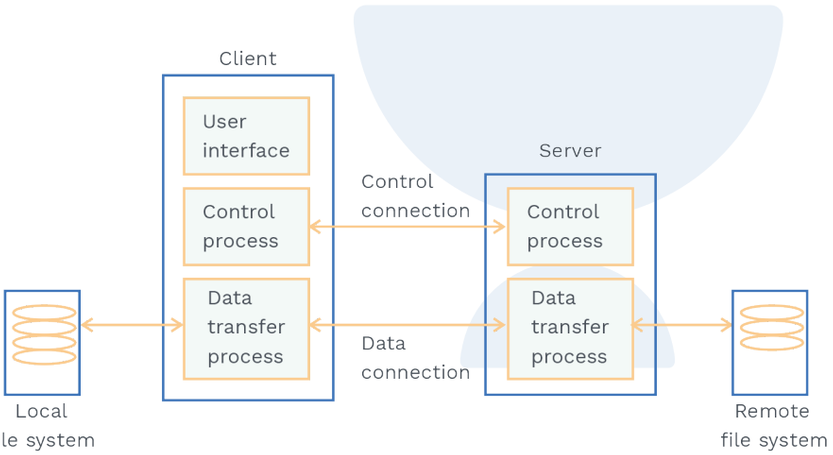


Fig. 6.8 Basic Model Of FTP

- There are two connection in FTP → Control Connection
  → Data Connection
- The control connection remains connected during the entire FTP session.
- The data connection is opened and closed for each file transfer activity.

Note:

FTP use two well-known TCP ports. It uses port 21 for the control connection and port 20 for data connection.

- Below are few FTP commands that can be performed on the remote host through local host after connecting to remote host.

Command	Description
• ABOR	Abort the previous command
• DELE	Delete a file
• LIST	List subdirectories
• MKD	Make new directory
• PORT	Client chooses a port
• PWD	Display name of current directory
• QUIT	Logout of the system
• MODE	Define transmission mode (S: Stream) (B: Block) (C: compressed)

Table 6.9 Commands

Note:
File transfer in FTP involves three steps:
- Retrieving a file (server to client)
- Storing a file (client to server)
- Directory listing (server to client)

6.4 ELECTRONIC MAIL (E–MAIL)

- It allows users to exchange messages.
- Unlike FTP or HTTP, in the case of E–mail the server program need not run all the time.
- Now we will discuss, how is it possible?

UA: User Agent
MTA: Message Transfer Agent
MAA: Message Access Agent

Previous Years' Question

Identify the correct order in which the following actions take place in an interaction between web browser and a web server.

1) The web browser requests a webpage using HTTP.
2) The web browser establishes a TCP connection with the web server.
3) The web server sends the requested webpage using HTTP.
4) The web transfer resolves the domain name using DNS.

a) 4, 2, 1, 3 **b)** 1, 2, 3, 4
c) 4, 1, 2, 3 **d)** 2, 4, 1, 3

Sol: a) **(GATE-2014 (Set–1))**

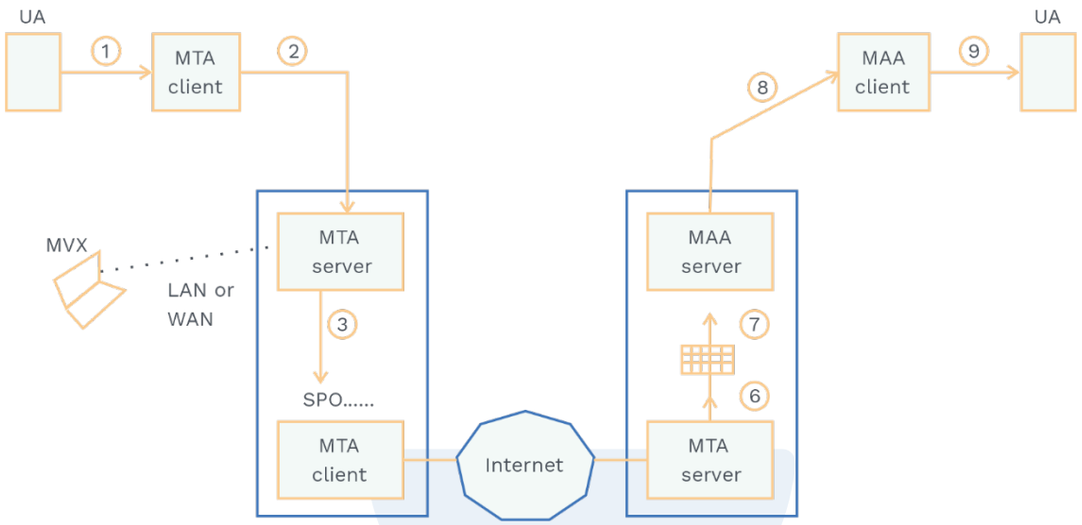


Fig. 6.9 Basic Architecture Of E–mail

Message transfer agent:

- Simple Mail Transfer Protocol (SMTP) is used twice, between the sender and sender's mail server, and also between two mail servers.

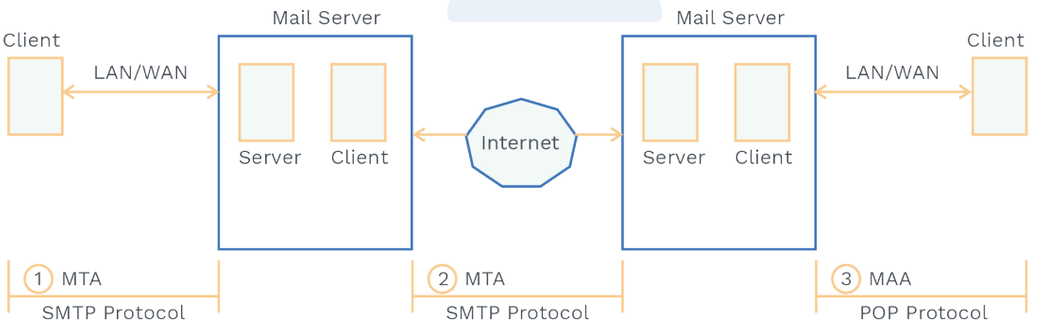


Fig. 6.10 Protocol Used In E–mail

- Command is sent from an MTA client to an MTA server.
- The format of a command is:
  Keyword: argument(s)
- SMTP defines 14 commands:
  i) HELO
  ii) MAIL FROM
  iii) RCPT TO
  iv) DATA

v) QUIT
vi) RSET
vii) VRFY
viii) NOOP
ix) TURN
x) EXPN
xi) HELP
xii) SEND FROM
xiii) SMOL FROM
xiv) SMAL FROM

Message Access Agent: POP

- It is used to retrieve mail from the mail server.
- The client POP3 software is installed on the recipient computer.
- The server POP3 software is installed on the mail server.
- POP3 has 2 modes: the delete mode and the keep mode.
- In keep mode, the mail remains in the mail box after retrieval. In Delete mode,the mail gets removed from the mailbox.
- POP3 is a stateful protocol.

IMAP4:

- It is another mail access protocol like POP3 but is more powerful and has more features than POP3.
- POP3 does not allow to check the mail contents partially before the user downloads.
- Advantages of IMAP4 over POP3:
  - **i)** A user can check mail contents before downloading.
  - **ii)** A user can search the contents of e (mail) for specific strings of characters prior to downloading.
  - **iii)** A user can partially download email.
  - **iv)** A user can create, delete or rename mailboxes on the mail server.

Previous Years' Question

Which of the following is/are example(s) of stateful application layer protocol?

i) HTTP **ii)** FTP
iii) TCP **iv)** POP3

a) i) and ii) only
b) ii) and iii) only
c) ii) and iv) only
d) iv) only

Sol: c) **(GATE-2016 (Set–1))**

Chapter summary

- DNS: Maps host name to IP address.
- HTTP: Retrieves web pages from the web.
- Non-persistent HTTP connection–One TCP connection is made for each request/response.
- Persistent HTTP connection: The server leaves the connection open for more requests after sending a response.
- FTP: Standard protocol provided by TCP/IP for copying a file from one host to another.
- Two components of FTP → Control Connection; Data Connection
- Email: • UA [User Agent]
  • MTA [Message Transfer Agent] → SMTP
  • MAA [Message Access Agent] → POP3; IMAP4