RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Information Technology, V-Semester

IT502 - Computer Networks

Course Objectives

- To provide students with an overview of the concepts and fundamentals of computer networks
- To familiarize with the basic taxonomy and terminology of computer networking area.
- Describe how computer networks are organized with the concept of layered approach
- To experience the designing and managing of communication protocols while getting a good exposure to the TCP/IP protocol suite

Unit I

Importance of computer networks, broadcast and point to point networks, Local area networks and Wide area networks , ISO-OSI reference model, TCP/IP model , interfaces and services, Protocol data unit, connection oriented and connectionless services, service primitives, Binding Protocol Address- ARP & RARP, packet format, Encapsulation.

Unit II

Data-Link layer: - Data link layer design issues, framing , flow & error control , physical addressing, Stop & Wait protocol ,Go back N ARQ ,selective repeat ARQ ,piggybacking and pipelining ,HDLC LAN Protocol stack-Logical link control and Media Access Control sublayer, IEEE 802.2 LLC Frame format; MAC layer Protocols- static and dynamic allocation, Pure and slotted ALOHA, Carrier sense multiple access, Persistent and non persistent CSMA, IEEE standard 802.3, 802.4, 802.5, FDDI,

Unit III

The Network layer- logical addressing, classful & classless addressing, packet delivery & forwarding. unicast routing protocols , multicast routing protocols, Routing algorithm- Least Cost, Dijkstra's, Bellman-ford, Introduction to Internet protocol, IPv4 header, IPv4 Datagrams, Encapsulation, Fragmentation and Reassembly, IP routing, Subnet addressing, Subnet mask, Super netting- special case of IP addresses, Ipv6-Motivation, frame format and addressing. ICMP: Introduction, ICMP Header, ICMP message types.

Unit IV

Transport layer- TCP: Introduction ,Transport services , Process to process delivery, TCP ,congestion control algorithms, quality of service, headers, connection establishment and termination, timeout of connection establishment, maximum segment size, port no. and socket addresses, TCP timers, UDP: Introduction, UDP header, UDP checksum, UDP operations, encapsulation & decapsulation, queuing, SCTP-Services, transmission sequence number, stream identifier, stream sequence number, packet format.

Unit V

Application layer - BOOTP:-operation, packet format, DHCP:-Address allocation, configuration & packet Format, DNS: Distribution of name spaces, DNS in the internet, FTP:-Connection, Communication, command processing, TFTP, E-Mail: SMTP, POP, IMAP, SNMP. study of internetworking devices and their configuration– switches, hubs, Bridges, routers and Gateways.

References

1. ."Computer Networks" - Tanenbaum ,PHI Learning
2. "Data Communication & Networks " , Fourouzan TMH
3. "TCP/IP-Protocol suite", Forouzan, TMH 3rd edition
4. "Computer Networks and Internets", D.E.Comer, Pearson
5. "TCP/IP Illustrated" W. Richard Stevens, Volume I, Addison Wesley,
6. "Internetworking with TCP/IP Vol. I, II & III", Comer , PHI Learning.

Course Outcomes

Upon successful completion of this course the students will:

- Have agood understanding of the OSI Reference Model and its Layers
- Identify core networking and infrastructure components and the roles they serve; and given requirements and constraints, design an IT infrastructure including devices, topologies, protocols, systems software, management and security;
- Analyze the requirements for a given organizational structure and select the most appropriate networking architecture and technologies
- Specify and identify deficiencies in existing protocols, and then go onto formulate new and better protocols

Department of Information Technology

Sub: Computer **Sub Code :IT-502**

UNIT I

Subject Introduction

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections (network links). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device can exchange information with the other device, whether or not they have a direct connection to each other.

Importance of computer networks

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities and also have following capabilities.

1. Resource and load sharing
2. Programs do not need to run on a single machine
3. Reduced cost
4. Several machines can share printers, tape drives, etc.
5. High reliability
6. If a machine goes down, another can take over
7. Mail and communication

Computer Network: components

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), the local operating system(LOS), and the network operating system (NOS).

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers and web servers, to name a few.

Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers.

Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.

Shared data - Shared data are data that file servers provide to clients such as data files, printer access programs, and e-mail.

Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

Network Interface Card - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents. Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are Located on the computer. Examples are MS-DOS, UNIX, Linux, Windows 2000, Windows 98, and Windows XP etc.

Network Operating System - The network operating system is a program that runs on computers and servers and allows the computers to communicate over the network.

Hub - Hub is a device that splits a network connection into multiple computers. It is a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Switch - Switch is a telecommunication device grouped as one of computer network components. The switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming message so that it can deliver the message to the right destination or port.

Like a hub, the switch doesn't broadcast the received message to the entire network; rather before sending it checks to which system or port should the message be sent.

Broadcast and point to point networks

Broadcast links and point-to-point links are two types of transmission technologies that are in widespread use. Point-to-point links is a connection between individual pairs of machines. In this connection, a short message from the source to the destination is called a “packet”.

This packet may have to visit one or more intermediate machines before returning to the destination, therefore finding good routes within the network is important in point-to-point.

A point-to-point transmission with one sender and one receiver is called unicasting. Broadcast links is in contrast a communication channel that is shared by all the machines in the network. The difference between point-to-point and broadcast, is that in broadcast networks, the packets(/the message) is sent by any machine and received by all the other machines.

Point-to-Point Connection

The point-to-point is a kind of line configuration which describes the method to connect two communication devices in a link. The point-to-point connection is a unicast connection. There is a dedicated link between an individual pair of sender and receiver. The capacity of the entire channel is reserved only for the transmission of the packet between the sender and receiver.

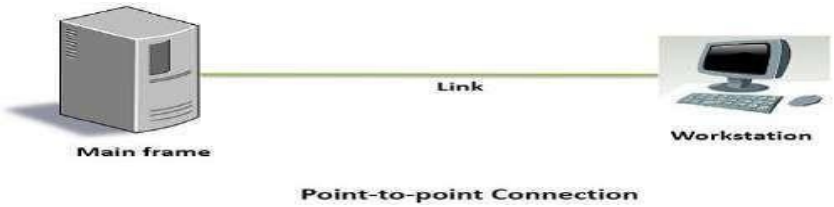


Fig 1.1 Point to Point connection

Multipoint Connection

The multipoint connection is a connection established between more than two devices. The multipoint connection is also called multidrop line configuration. In multipoint connection, a single link is shared by multiple devices. So, it can be said that the channel capacity is shared temporarily by every device connecting to the link. If devices are using the link turn by turn, then it is said to be time shared line configuration.

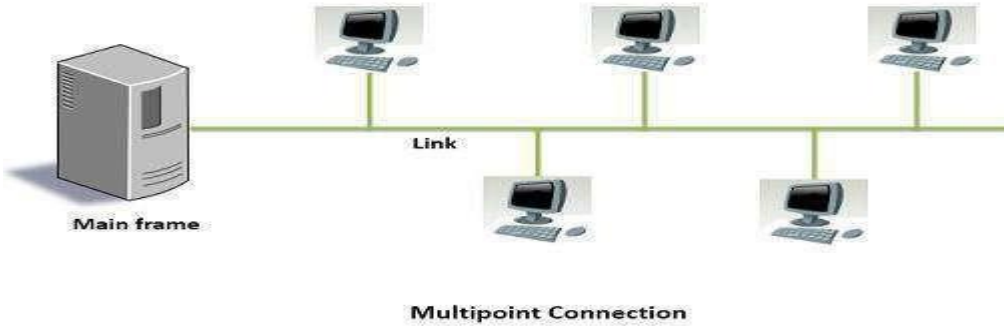


Fig 1.2 Multipoint Connection

Computer Network: Classifications & Types

Computer Network: Classifications & Types. There are three types of network classification

1) LAN (Local area network)
2) MAN (Metropolitan Area network)
3) WAN (Wide area network)

1) Local area network (LAN)

LAN is a group of the computers placed in the same room, same floor, or the same building so they relate to each other to form a single network to share their resources such as disk drives, data, CPU, modem etc. LAN is limited to some geographical area less than 2 km. Most of LAN is used widely is an Ethernet system of the bus topology.

Fig 1.3 Local Area Network

Characteristics of LAN

- LAN connects the computer in a single building; block and they are working in any limited area.
- Media access control methods in a LAN, the bus based Ethernet, token ring.
- This is private networks, not for the subject to tariffs or regulatory controls.
- LAN is a wireless there is an additional in some countries.

Advantages of local area network (LAN)

1. **Sharing of resources:**

All the resources are attached to one network and if any computer needs any resources then it can be shared with the required computer. Types of resources are the DVD drive, printers, scanners, modems and hard drives. So there is no need to purchase separate resources for each computer and it saves money.

2. **Client and server relationship:**

All the data from attached computers can be stored in one server. If any computer (Client) needs data then that computer user can simply log in and access the data from the server. For example movies and songs can be stored on the server and can be accessed by any authorized user (Client computer).

3. **Sharing of the internet:**

In offices and net cafes, we can see that one internet connection is shared between all computers. This is also the type of LAN technology in which main internet cable is attached to one server and distributed amoung attached computers by the operating system.

4. **Software program sharing:**

Software programs can also be shared on the LAN. You can use single licensed software and any user can use it in the network. It is expensive to buy a license for each user in the network so sharing software program is easy and cost-effective.

5. **Securing of data:**

Keeping data on the server is more secure. And if you want to change or remove any data you can do it easily on one server computer and other computers can access updated data. You can also give access or revoke access to specific users so that only authorized users can access the data in the network.

6. **Communication is easy, fast, and time-saving**

In LAN computers can exchange data and messages in the easy and fast way. It also saves time and makes our work fast. Every user can share messages and data with any other user on LAN. The user can log in from any computer on the network and access the same data placed on the server.

7. **Computer identification:**

Each computer is given a MAC address and is temporarily stored in the switch or router during communication. All computers on the LAN are identified by MAC addresses which are used to send and receive messages and data. Note that MAC address is stored in the network adapter that is attached in the motherboard of each computer. In old computers, network adapters were not built in with motherboards but in modern computers, they come built-in with motherboards.

Disadvantages of local area network (LAN)

1. **Data security problem:**

If the server computer is not set up correctly and there is a leak in security then unauthorized users can access the data also. So there should be privacy policy and rules set up correctly on the server.

2. **Limitation of distance:**

Local area networks are usually made within a building or nearby building and cannot extend to the wider area.

3. **Server crashes may affect all computers:**

If any file on the server is corrupted or hard drive fails then all the attached computers face problems in functioning properly.

4. **Setting up a LAN is expensive:**

It is expensive to set up LAN because there is special software required to make a server. Also, communication devices like hubs, switches, routers, cables are costly. The special administrator is required to maintain and troubleshoot LAN for a large office.

2) Metropolitan Area network (MAN)

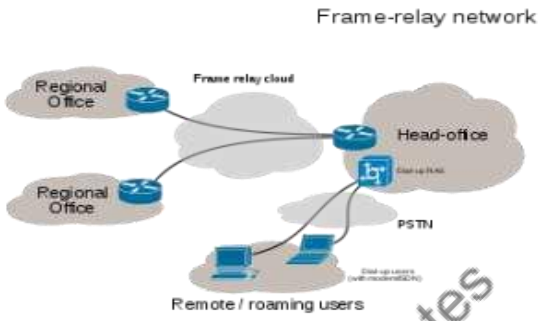


Fig.1.2 Metropolitan Area network

The metropolitan area network is a large computer network that expands a Metropolitan area or campus. It is geographic area between WAN and LAN. It's expand around 50km devices used are modem and wire/cable.

Characteristics of MAN

- Its covers the towns and cities (50km)
- It is developed in the 1980s.
- MAN is used by the communication medium for optical fiber cables, it also used for other media

Advantages of a metropolitan area network (MAN)

1. **Less expensive:**

It is less expensive to attach MAN with WAN. MAN gives the good efficiency of data. In MAN data is easily managed in a centralized way.

2. **Sending local emails:**

On MAN you can send local emails fast and free.

3. **High speed than WAN:**

MAN uses fiber optics so the speed of data can easily reach upon 1000 Mbps. Files and databases can be transferred fast.

4. **Sharing of the internet:**

In some installation of MANs, users can share their internet connection. So multiple users can get the same high-speed internet.

5. **Conversion from LAN to MAN is easy:**

MAN is a faster way to connect two fast LANs together. This is due to the fast configuration of links.

6. **High Security:**

MAN has a high-security level than WAN.

Disadvantages of metropolitan area network (MAN)

1. **Difficult to manage:**

If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra configuration.

2. **Internet speed difference:**

MAN cannot work on traditional phone copper wires. If MAN is installed on copper wires then there will be very low speed. So it required the high cost to set up fiber optics for the first time.

3. **Hackers attack:**

In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked. Data can be secured but it needs high trained staff and security tools.

4. **Technical people required to set up:**

To setup MAN it requires technical people that can correctly setup MAN. The technical people are network administrators and troubleshooters.

5. **More wires required:**

In MAN additional cables are required to connect two LAN which is another problem.

3. Wide area Network (WAN)

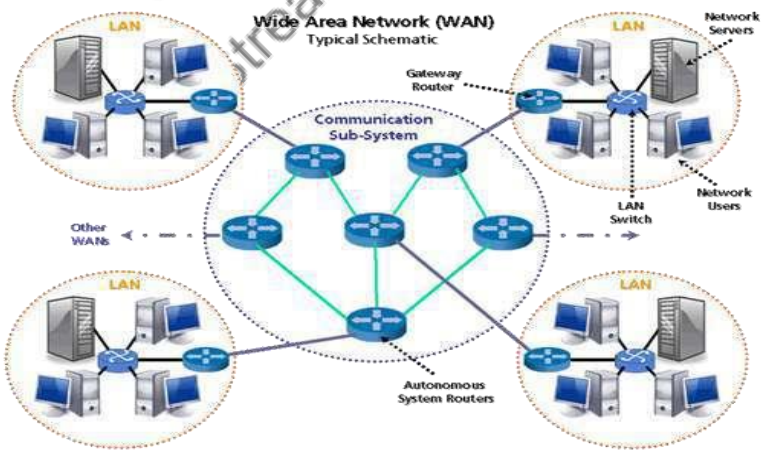


Fig. 1.3 Wide area Network

The wide area network is a network which connects the countries, cities or the continents; it is a public communications links. The most popular example of a WAN is the internet. WAN is used to connect LAN so the users and the computer in the one location can communicate with each other.

Characteristics of WAN

- It covers the large distances.
- Communication medium used are a satellite, telephones which are connected by the routers.

Advantages of WANS

If your company has branches in several locations, a wide area network is a viable option to boost productivity and increase internal communications. Below are some of the more critical business advantages to establishing a WAN:

- **Centralizes IT infrastructure** — Many consider this WAN's top advantage. A WAN eliminates the need to buy email or file servers for each office. Instead, you only have to set up one at your head office's data center. Setting up a WAN also simplifies server management, since you won't have to support, back-up, host, or physically protect several units. Also, setting up a WAN provides significant economies of scale by providing a central pool of IT resources the whole company can tap into.

- **Boosts your privacy** — Setting up a WAN allows you to share sensitive data with all your sites without having to send the information over the Internet. Having your WAN encrypt your data before you send it adds an extra layer of protection for any confidential material you may be transferring. With so many hackers out there just dying to steal sensitive corporate data, a business needs all the protection it can get from network intrusions.

- **Increases bandwidth** — Corporate WANS often use leased lines instead of broadband connections to form the backbone of their networks. Using leased lines offers several pluses for a company, including higher upload speeds than your typical broadband connections. Corporate WANS also generally offer unlimited monthly data transfer limits, so you can use these links as much as you like without boosting costs. Improved communications not only increase efficiency but also boost productivity.

- **Eliminates Need for ISDN** — WANs can cut costs by eliminating the need to rent expensive ISDN circuits for phone calls. Instead, you can have your WAN carry them. If your WAN provider "prioritizes voice traffic," you probably won't see any drop off in voice quality, either. You may also benefit from much cheaper call rates when compared to calls made using ISDN circuits. Some companies use a hybrid approach. They have inbound calls come over ISDN and outbound calls go over the WAN. This approach won't save you as much money, but it will still lower your bill.

- **Guaranteed uptime** — Many WAN providers offer business-class support. That means you get a specific amount of uptime monthly, quarterly, or yearly as part of your SLA. They may also offer you round the clock support. Guaranteed uptime is a big plus no matter what your industry. Let's face it. No company can afford to be down for any length of time in today's business environment given the stringent demands of modern customers.

- **Cuts costs, increase profits** — In addition to eliminating the need for ISDN, WANs can help you cut costs and increase profits in a wide variety of other ways. For example, WANS eliminate or significantly reduce the costs of gathering teams from different offices in one location. Your marketing team in the United States can work closely with your manufacturing team in Germany

using video conferencing and email. Saving on the travel costs alone could make investing in a WAN a viable option for you.

WANS also provide some key technical advantages as well. In addition to providing support for a wide variety of applications and a large number of terminals, WANs allow companies to expand their networks through plug-in connections over locations and boost interconnectivity by using gateways, bridges, and routers. Plus, by centralizing network management and monitoring of use and performance, WANS ensure maximum availability and reliability.

Disadvantages of WANS

While WANS provide numerous advantages, they have their share of disadvantages. As with any technology, you need to be aware of these downsides to make an informed decision about WANS. The three most critical downsides are high setup costs, security concerns, and maintenance issues.

- **High setup costs** — WANs are complicated and complex, so they are rather expensive to set up. Obviously, the bigger the WAN, the costlier it is to set up. One reason that the setup costs are high is the need to connect far-flung remote areas. However, by using public networks, you can set up a WAN using just software (SD-WAN), which reduces setup costs. Keep in mind also that the price/performance ratio of WANs is better now than a decade or so ago.

- **Security Concerns** —WANs open the way for certain types of internal security breaches, such as unauthorized use, information theft, and malicious damage to files. While many companies have some security in place when it comes to the branches, they deploy the bulk of their security at their data centers to control and manage information sent to their locations. This strategy reduces management costs but limits the company's ability to deal directly with security breaches at their locations. Some companies also have a hard time compressing and accelerating SSL traffic without significantly increasing security vulnerabilities and creating new management challenges.

- **Maintenance Issues** — Maintaining a WAN is a challenge, no doubt about it. Guaranteeing that your data center will be up and operating 24/7 is the biggest maintenance challenge of all. Data center managers must be able to detect failures before they occur and reduce data center downtime as much as possible, regardless of the reasons. Downtime is costly, in fact, a study done by infinities Research estimates that medium and large businesses in North America lose as much as $100 million annually to IT and communication technology downtime.

Layered Architecture: Interfaces and Services Protocol hierarchy, Design Issues

To tackle with the design complexity most of the networks are organize as a set of layers or levels. The fundamental idea of layered architecture is to divide the divide the design into small pieces. The layering provides modularity to the network design. The main duty of each layer is to provide offer services to higher layers and provide abstraction. The main benefits of layered architecture are modularity and clear interfaces. The basic elements of a layered model are services, protocols, and Interfaces.
A service is a set of functions that a layer offers to another layer (usually to upper layer) we know that

protocol is a set of rules. Here the protocols are used to exchange information with a peer layer. Peers means layers at the same level. The protocol consists several rules that deals with the content and the order or structure of the messages exchanged.

Five Layered Network

Layered architectures have several advantages. Some of them are

- Modularity and clear interface
- Provide flexibility to modify network services
- Ensure independence of layers
- Management of network architecture is easy
- Each layer can be analyzed and tested independently of other layers

The benefits to layering networking protocol specifications are many including Interoperability. Layering promotes greater interoperability between devices from different manufacturers and even between different generations of the same type of device from the same manufacturer.

Greater Compatibility - One of the greatest of all the benefits of using a hierarchal or layered approach to networking and communications protocols is the greater compatibility between devices, systems, and networks that this delivers.

Better Flexibility - Layering and the greater compatibility that it delivers goes a long way to improving the flexibility; particularly in terms of options and choices, that network engineers and administrators alike crave so much.

Flexibility and Peace of Mind - Peace of mind in knowing that if worst comes to worst and a key core network device; suddenly and without warning decides to give up the ghost, you can rest assured that a replacement or temporary stand-by can be readily put to work with the highest degree of confidence that it will do the job.

Increased Life Expectancy - Increased product working life expectancies as backward compatibility is made considerably easier. Devices from different technology generations can co-exist thus the older units do not get discarded immediately newer technologies are adopted.

Scalability- Experience has shown that a layered or hierarchal approach to networking protocol design and implementation scales better than the horizontal approach. Mobility - Greater mobility is more readily delivered whenever we adopt the layered and segmented strategies into our architectural design Value **Cost Effective Quality** - The layered approach has proven time and time again to be the most economical way of developing and implementing any system(s) be they small, simple, large or complex makes no difference.

Modularity - I am sure that you have come across plug-ins and add-ons. These are common and classical examples of the benefits to be derived from the use of a hierarchal (layered) approach to design.

Standardization and Certification - The layered approach to networking protocol Specifications facilitates a more streamlined and simplified standardization and certification process; particularly from an "industry" point of view.

Compartmentalization of Functionality - The compartmentalization or layering of processes, procedures and communications functions gives developers the freedom to concentrate on a specific layer or specific functions within that layer's realm of responsibility without the need for great concern or modification of any other layer.

Side-Kicks - The development of "Helper" protocols or side- kicks is much easier when a layered approach to networking protocols is embraced. This is especially so when it comes to the development of "helper"

protocols that are developed as after-thoughts because the need arose.

Time - The time spent debugging can be greatly reduced as a direct result of taking the layered approach to developing network protocols because debugging is made easier and faster when using the layered approach as opposed to not using it.

Promotion of Multi-Vendor Development - Layering allows for a more precise identification and delineation of task, process, and methodology. This permits a clearer definition of what needs to be done, where it needs to be done, when it needs to be done, how it needs to be done and what or who will do it.

Easier Binding Implementation – The principle of binding is far easier to implement in layered, tiered, and hierarchal systems. Humans also tend to understand this form easier than the flat model.

Enhanced Troubleshooting and Fault Identification - Troubleshooting and fault identification are made considerably easier thus resolution times are greatly reduced. Layering allows for examination in isolation of subcomponents as well as the whole.

Enhanced Communications Flow and Support - Adopting the layered approach allows for improved flow and support for communication between diverse systems, networks, hardware, software, and protocols.

Support for Disparate Hosts - Communications between disparate hosts is supported seamlessly thus Unix, PC, MAC & Linux to name but a few can freely interchange data. Reduction of the Domino Effect - Another very important advantage of a layered protocol system is that it helps to prevent changes in one layer from affecting other layers. This helps to expedite technology development. Rapid Application Development (RAD) - Workloads can be evenly distributed which means that multiple activities can be conducted in parallel thereby reducing the time taken to develop, debug, optimize and package new technologies ready for production implementation.

ISO-OSI Reference Model: Principle, Model, Descriptions of various layers

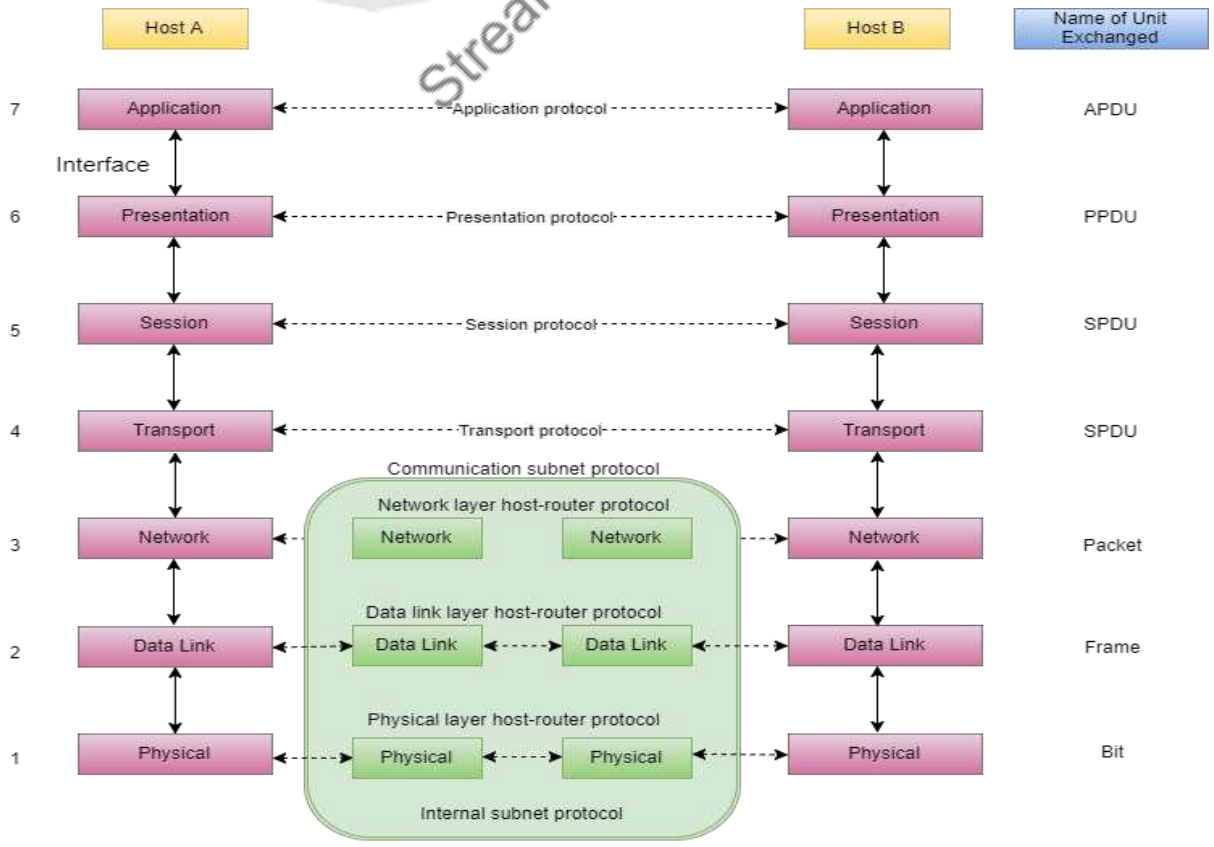


Fig. 1.4 OSI Reference Model

• Helps users understand the big picture of networking
• Helps users understand how hardware and software elements function together
• Makes troubleshooting easier by separating networks into manageable pieces
• Defines terms that networking professionals can use to compare basic functional relationships on different networks
• Helps users understand new technologies as they are developed
• Aids in interpreting vendor explanations of product functionality

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1. The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer. The recommendation X.200 describes seven layers, labeled 1 to 7. Layer 1 is the lowest layer in this model.

Layer 1: Physical layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection. It defines the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.
- It defines the protocol to establish and terminate a connection between two directly connected nodes over a communications medium.
- It may define the protocol for flow control.
- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the topology.
- It defines a protocol for the provision of a (not necessarily reliable) connection between two directly connected nodes, and the modulation or conversion between the representation of digital data in user Equipment and the corresponding signals transmitted over the physical communications channel.

• Cabling system components
• Adapters that connect media to physical interfaces
• Connector design and pin assignments
• Hub, repeater, and patch panel specifications
• Wireless system components
• Parallel SCSI (Small Computer System Interface)
• Network Interface Card (NIC)

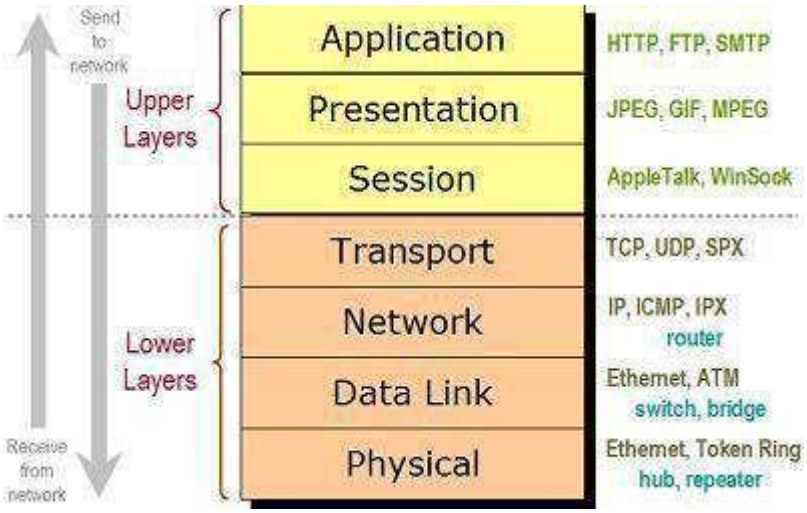


Fig.1.5 Protocols

Layer 2: Data link layer

The data link layer provides node-to-node data transfer - A reliable link between two directly connected nodes, by detecting and possibly correcting errors that may occur in the physical layer. The data link layer is divided into two sublayers:

- Media Access Control (MAC) layer - Responsible for controlling how devices in a network gain access to data and permission to transmit it.
- Logical Link Control (LLC) layer - Controls error checking and packet synchronization.

The Point-to-Point Protocol (PPP) is an example of a data link layer in the TCP/IP protocol stack.

The ITU-T standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer that provides both error correction and flows control by means of a selective-repeat sliding- window protocol.

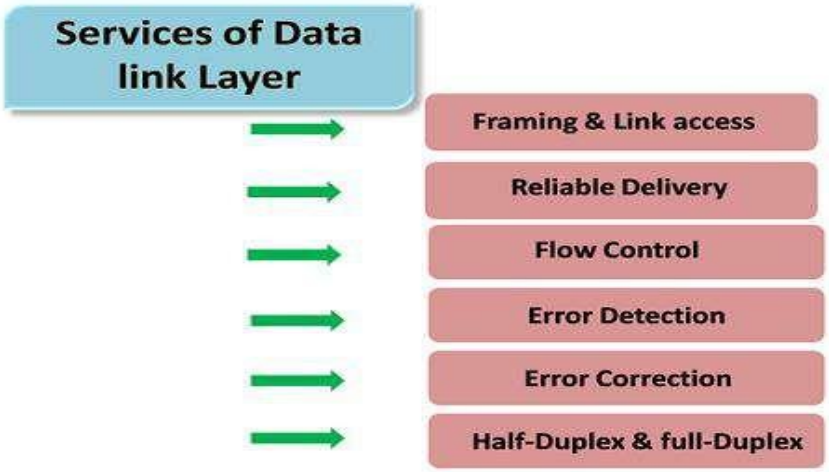


Fig . 1.6 Services are provided by the Data Link Layer

- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.

- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Basic Functions

• Allows a device to access the network to send and receive messages
• Offers a physical address so a device's data can be sent on the network
• Works with a device's networking software when sending and receiving messages
• Provides error-detection capability
Common networking components that function at layer 2 include:
• Network interface cards
• Ethernet and Token Ring switches
• Bridges

Layer 3: Network layer

- The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network.
- It translates logical network address into physical machine address.
- Routing is also one of the main functions of the Network Layer, routing is the process of selecting paths in a network over which to send packets.
- Internet Control Message Protocol (ICMP) is network layer protocol and one of the main protocols of the Internet Protocol suite and is used for error handling and diagnostic purposes.

  The main functions performed by the network layer are:

  - **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
  - **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

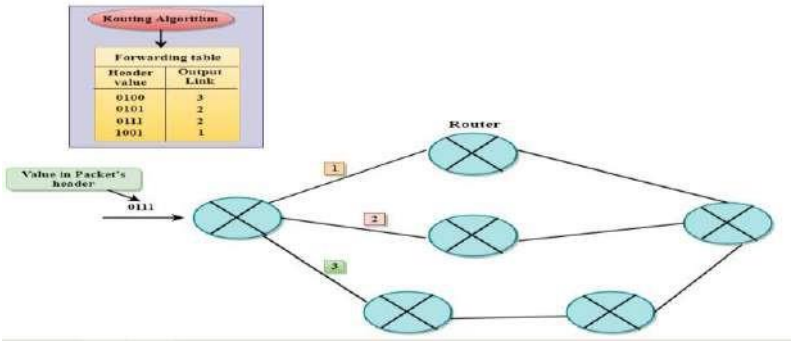


Fig1.7 Routing forwarding table

Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Layer 4: Transport layer

The transport layer provides the functional and procedural means of transferring variable- length data sequences from a source to a destination host via one or more networks while maintaining the quality of service functions.

An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP).

Some of the functions offered by the transport layer include:

• Application identification
• Client-side entity identification
• Confirmation that the entire message arrived intact
• Segmentation of data for network transport
• Control of data flow to prevent memory overruns
• Establishment and maintenance of both ends of virtual circuits

• Transmission-error detection
• Realignment of segmented data in the correct order on the receiving side
• Multiplexing or sharing of multiple sessions over a single physical link
The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Flow control
- Multiplexing
- Addressing
- Reliable delivery

Layer 5: Session layer
The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application.
It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network. Session layer functionality includes:
• Virtual connection between application entities
• Synchronization of data flow
• Creation of dialog units
• Connection parameter negotiations
• Partitioning of services into functional groups
• Acknowledgements of data received during a session
• Retransmission of data if it is not received by a device
Layer 6: Presentation layer
The presentation layer, is responsible for how an application formats the data to be sent out onto the network. The presentation layer basically allows an application to read (or understand) the message.
Examples of presentation layer functionality include:
• Encryption and decryption of a message for security
• Compression and expansion of a message so that it travels efficiently
• Graphics formatting
• Content translation
• System-specific translation
Layer 7: Application layer

The application layer, provides an interface for the end user operating a device connected to a network.
This layer is what the user sees, in terms of loading an application (such as Web browser or e-mail.
Examples of application layer functionality include:

• Support for file transfers
• Ability to print on a network
• Electronic mail
• Electronic messaging
• Browsing the World Wide Web

Some examples of application layer implementations include:

- On OSI stack:
- FTAM File Transfer and Access Management Protocol
- X.400 Mail
- Common Management Information Protocol (CMIP)
- On TCP/IP stack:
- Hypertext Transfer Protocol (HTTP),
- File Transfer Protocol (FTP),
- Simple Mail Transfer Protocol (SMTP),
- Simple Network Management Protocol (SNMP), etc.

TCP/IP reference model

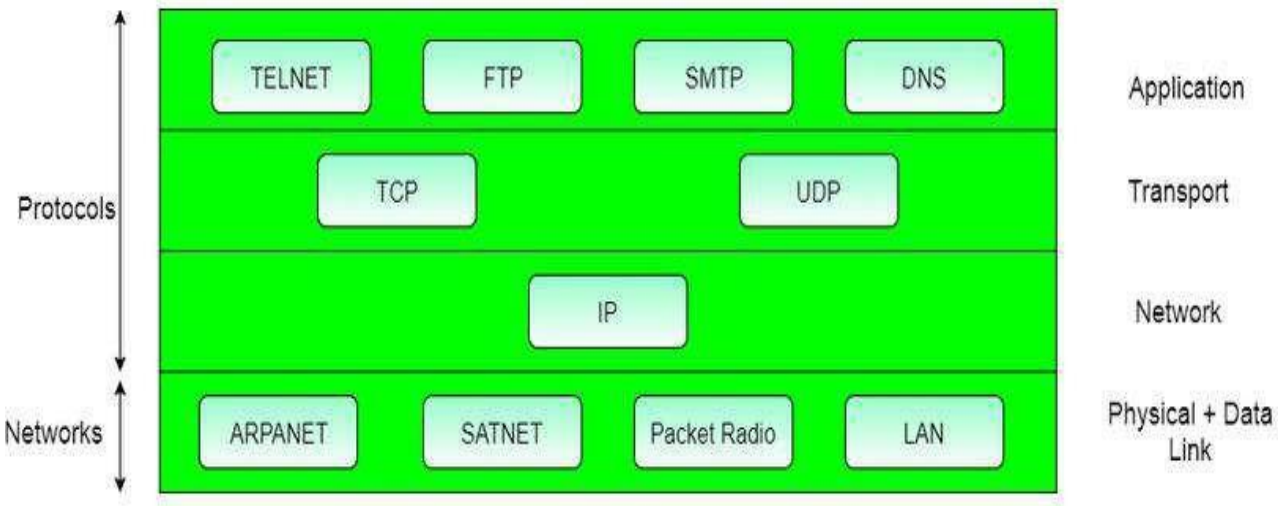


Fig .1.8 TCP/IP reference model

The TCP/IP reference model is the network model used in the current Internet architecture. It is considered as the grandfather of the Internet the ARPANET. The reference model was named after two of its main protocols, TCP (Transmission control Protocol) and IP (Internet Protocol).

There are versions of this model with four layers and with five layers. The original four-layer version of the model is shown below.

Layer 4: Process Layer or Application Layer: This is where the "higher level" protocols such as FTP, HTTP, etc. Operate. The original TCP/IP specification described many different applications that fit into the top

layer of the protocol stack. These applications include Telnet, FTP, SMTP, and DNS.

Layer 3: Host-To-Host (Transport) Layer: This is where flow-control and connection protocols exist, such as TCP. This layer deals with opening and maintaining a connection, ensuring that packet is in fact received the transport layer is the interface between the application layer and the complex hardware of the.

Two modes are an available, full-duplex and half-duplex. In full-duplex operation, both sides can transmit and receive data simultaneously, whereas, in half duplex, a side can only send or receive at one time.

Layer 2: Internet or Internetworking Layer: This layer defines IP addresses, with many routing schemes for navigating packets from one IP address to another. The job of the network layer is to inject packets into any network and have them travel independently to the destination. Packet routing is a major job of this protocol.

Layer 1: Networking Access Layer: This layer describes the physical equipment necessary for communications, such as twisted pair cables, the signaling used on that equipment, and the low-level protocols using that signaling. That Host-to-Network layer interfaces the TCP/IP protocol stack to the physical network.

TCP/IP Protocol Suite:

The TCP/IP protocol suite has two sets of protocols at the Internet layer:

- IPv4, also known as IP, is the Internet layer in common use today on private intranets and the Internet.
- IPv6 is the new Internet layer that will eventually replace the existing IPv4 Internet layer.

X.25 is a standard used by many older public networks specially outside the U.S.

• This was developed in 1970s by CCITT for providing an interface between public packet-switched network and their customers.

• The packet switching networks use X.25 protocol. The X.25 recommendations were first prepared in 1976 and then revised in 1978, 1980 and 1984.

• X.25 was developed for computer connections, used for terminal/timesharing connection.

• This protocol is based on the protocols used in early packet switching networks such as ARPANET, DATAPAC, and TRANSPAC etc.

• X.25 Packet Switched networks allows remote devices to communicate with each other across high speed digital links without the expense of individual leased lines.

• A protocol X.21 which is a physical layer protocol is used to specify the physical electrical and procedural interface between the host and network.

• The problem with this standard is that it needs digital signal rather than analog signals on telephone lines.

• So not many networks support this standard. Instead RS 232 standard is defined.

• The data link layer standard has a number of variations. It is designed for error detection and corrections.

• The network layer protocol performs the addressing, flow control, delivery confirmation etc.

• It allows the user to establish virtual circuits and send packets on them. These packets are delivered to the destination reliably and in order.

• X.25 is a connection oriented service. It supports switched virtual circuits as well as the permanent circuits.

• Packet Switching is a technique whereby the network routes individual packets of HDLC data between different destinations based on addressing within each packet.

• A switched virtual circuit is established between a computer and network when the computer sends a

packet to the network requesting to make a call to another computer.
• Packets can then be sent over this connection from sender to receiver.
• X.25 provides the flow control, to avoid a fast sender overriding a slow or busy receiver.
• A permanent virtual circuit is analogous to-a leased line. It is set up in advance with a mutual agreement between the users.
• Since it is always present, no call set up is required for its use.
• In order to allow the computers which do not use the X.25 to communicate with the X.25 network a packet assembler disassembler (PAD) is used.
• PAD is required to be installed along with each computer which does not use X.25.
• X.25 defines the interface for exchange of packets between a DTE and switch data subnetwork node.

Three Layers of X.25:

The X.25 interface is defined at three levels:
The three levels are:
(i) Physical layer (level 1)
(ii) Data link layer (level 2)
(iii) Packet layer (level 3).
• These three layers correspond to the three lower most layers of the ISO-OSI reference model. The physical layer takes care of the interface between a computer terminal and the link which attaches it to the packet switching node.
• The X.25 defines the interface for exchange of packets between the user's machine (DTE) and the packet switching node to which this DTE is attached which is called as DCE.
• The three layers of X.25 interface are as shown in below figure.
• At the physical level X.21 physical interface is being used which is defined for circuit switched data network. At the data link level, X.25 specifies the link access procedure-B (LAP-B) protocol which is a subset of HDLC protocol.

Protocol data unit (PDU)

In telecommunications, a protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol specific control information and user data. In the layered architectures of communication protocol stacks, each layer implements protocols tailored to the specific type or mode of data exchange. For example, the Transmission Control Protocol (TCP) implements a connection-oriented transfer mode, and the PDU of this protocol is called a segment, while the User Datagram Protocol (UDP) uses datagram's as protocol data unit for connection-less transfer. A layer lower in the Internet protocol suite, at the Internet layer, the PDU is called a packet, irrespective of its payload type.

For application data to travel uncorrupted from one host to another, header (or control data),which contains control and addressing information, is added to the data as it moves down the layers. The process of adding control information as it passes through the layered model is called encapsulation. De capsulation is the process of removing the extra information and sending only the original application data up to the destination application layer.

Each layer adds control information at each step. The generic term for data at each level is protocol data unit (PDU), but a PDU is different at each layer. For example, a PDU at the internetwork layer is different from the PDU at the transport layer, because in network layer data has been added to the transport layer data. The different names for PDUs at each layer are listed below.

Data --------- →Application layer PDU

Segment --- →Transport layer PDU

Packet------→Internetwork Layer PDU

Frame ------ →Network Access Layer PDU

Bits -------- →PDU used for the physical transmission of binary data over media

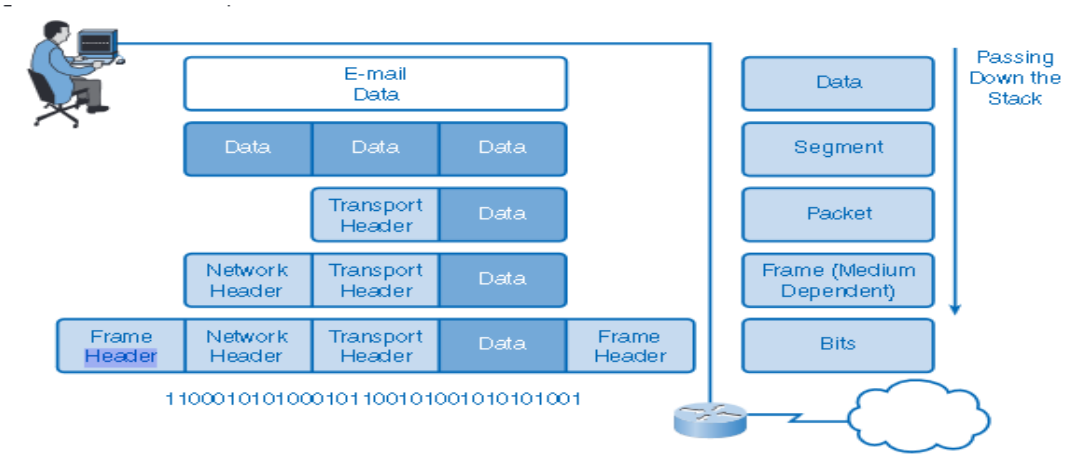


Fig 1.9 PDU Encapsulation

Connection Oriented & Connectionless Services, Service primitives, Design issues & its functionality

Connection-oriented communication is a network communication mode in telecommunications and computer networking, where a communication session or a semi- permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent.

- **Connection-oriented**

There is a sequence of operation to be followed by the users of connection-oriented service. They are:

1. Connection is established
2. Information is sent
3. Connection is released

In connection-oriented service we must establish a connection before starting the communication. When connection is established we send the message or the information. Then we release the connection.

Connection oriented service is more reliable than connectionless service. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

• **Connectionless**

It is similar to postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

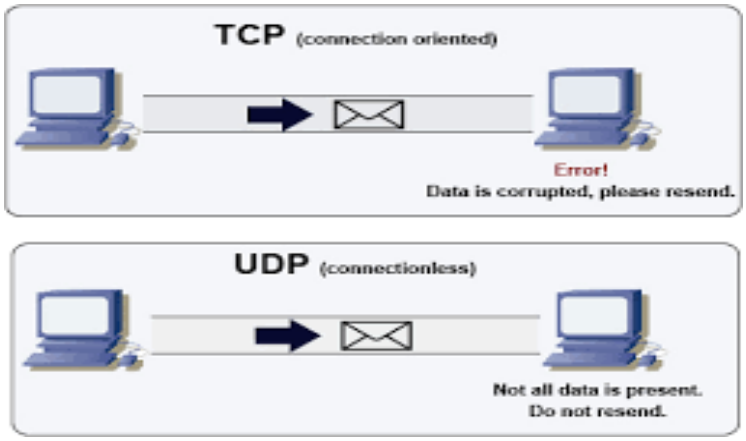


Fig. 1.10 Connection Oriented & Connectionless Services

#Service Primitives

Connection Oriented Service Primitives

LISTEN	Block waiting for an incoming connection
CONNECTION	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Sending a message to the peer
DISCONNECT	Terminate a connection

Connectionless Service Primitives

UNIDATA	This primitive sends a packet of data
FACILITY, REPORT	Primitive for enquiring about the performance of the network, like delivery statistics.

Design issues & its functionality

- **Justifying a Network**: - Some applications may be best satisfied by individual point to point connections to handle very specific communication requirements.
- **Scope**: - The scope of the network is viewed as bounded on one side by the offerings of the common carriers who provide communication facilities from which the network is built and on the other side by the application on which it is interconnected.

- **Network Architecture**: - While designing the network architecture, network may be a single homogeneous mesh comprised of a single type of node and a single type of link. Network architecture might be hierarchical network with one type link riding on another.
- **Switch Mode**: - For data transmission, different types of switching methods are possible. These are packet switching, circuit switching and hybrid switching.
- **Node Placement and sizing**: - A fundamental problem in the topological optimization of a network is the selection of the network node sites and where to place multiplexers, hubs and switch.
- **Link Topology and sizing**: - It involves selecting the specific links interconnecting nodes. At the highest level, that is where the architecture of the network is derived. Thus a hierarchy that include a backbone as well as LAN'S may be defined. It is possible to permit the backbone to be a mesh while LAN is constrained to be trees.
- **Routing**: - It involves selecting paths for each requirements. At higher level, this involves selecting the routing procedure itself.

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Address Resolution Protocol (ARP)

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.

In order to send the data to destination, having IP address is necessary but not sufficient; we also need the

physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.

Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

If a machine talks to another machine in the same network, it requires its physical or MAC address. But ,since the application has given the destination's IP address it requires some mechanism to bind the IP address with its MAC address.This is done through Address Resolution protocol (ARP).IP address of the destination node is broadcast and the destination node informs the source of its MAC address.

1. Assume broadcast nature of LAN
2. Broadcast IP address of the destination
3. Destination replies it with its MAC address.
4. Source maintains a cache of IP and MAC address bindings

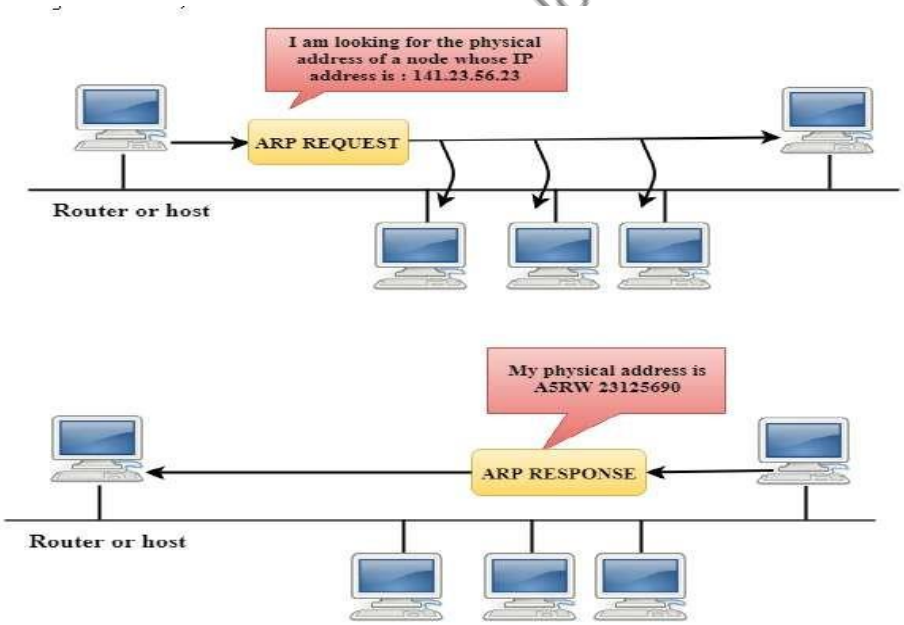


Fig.11 ARP Request and Response

But this means that every time machine A wants to send packets to machine B, A has to send an ARP packet to resolve the MAC address of B and hence this will increase the traffic load too much, so to reduce the communication cost computers that use ARP maintains a cache of recently acquired IP_ to_ MAC address bindings, i.e. they don't have to use ARP repeatedly. ARP Refinements Several refinements of ARP are possible: When machine A wants to send packets to machine B, it is possible that machine B is going to send packets to machine A in the near future .So to avoid ARP for machine B, A should put its IP_ to _MAC address binding in the special packet while requesting for the MAC address of B. Since A broadcasts its initial

request for the MAC address of B, every machine on the network should extract and store in its cache the IP_ to _MAC address binding of A When a new machine appears on the network (e.g. when an operating system reboots) it can broadcast its IP _to_ MAC address binding so that all other machines can store it in their caches. This will eliminate a lot of ARP packets by all other machines, when they want to communicate with this new machine.

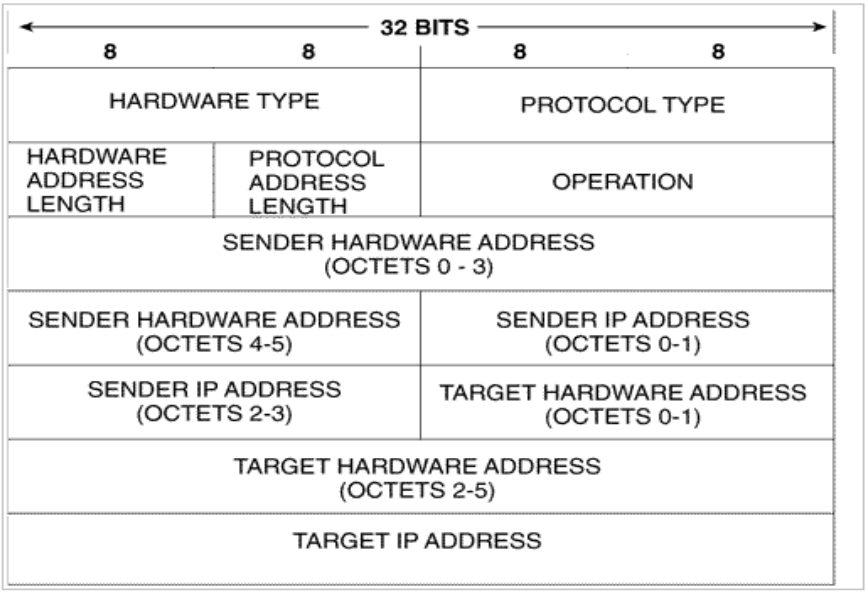


Fig 1.12 ARP Packet Format

Packet Format Description

Hardware type 16 bits.

Hardware Type: Hardware Type field in the Address Resolution Protocol (ARP) Message specifies the type of hardware used for the local network transmitting the Address Resolution Protocol (ARP) message. Ethernet is the common Hardware Type and he value for Ethernet is 1. The size of this field is 2 bytes.

Protocol type 16 bits.

Value	Description
0x800	IP.

Hardware addresses length 8 bits.
Length of the hardware address in bytes.

Protocol addresses length 8 bits.
Length of the protocol address in bytes.

Opcode 16 bits.

Value	Description	References
0	Reserved	RFC 5494
1	Request.	RFC 826
2	Reply.	RFC 826, 1868 5227
3	Request Reverse.	RFC 903
4	Reply Reverse.	

Table No. 01 Packet Format Description

Source hardware address Variable length.

Source protocol address Variable length.

Destination hardware address Variable length.

Destination protocol address Variable length.

Reverse Address Resolution Protocol (RARP)

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

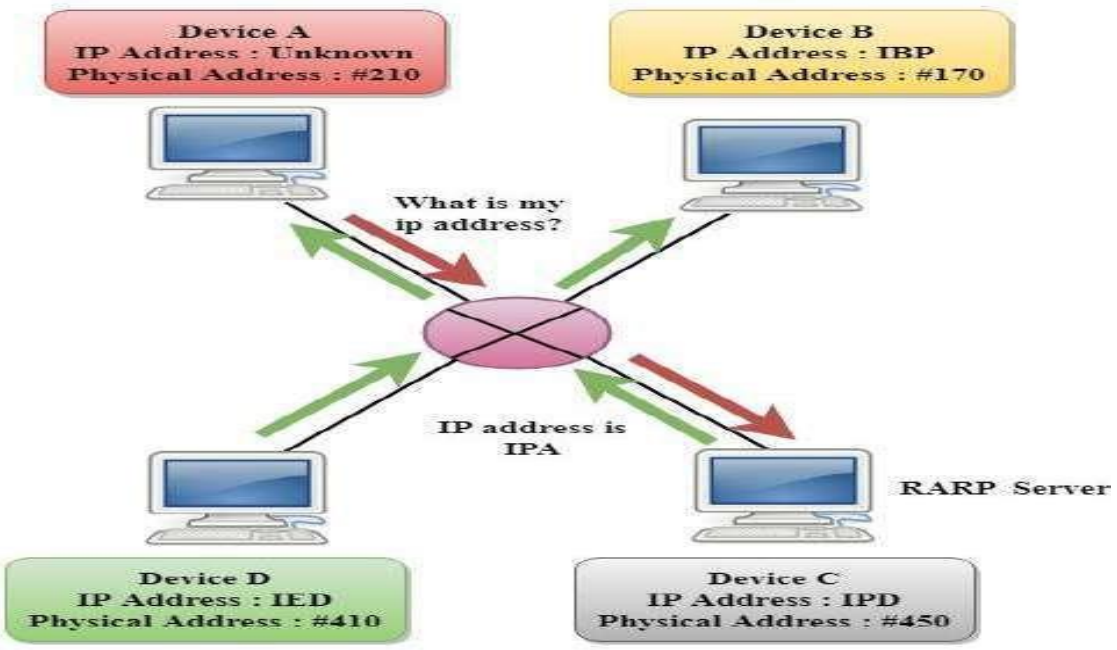


Fig. 13 Reverse Address Resolution Protocol

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. This is needed since the machine may not have permanently attacded disk where it can store its IP address permanently. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Medium Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Detailed Mechanism

Both the machine that issues the request and the server that responds use physical network addresses during their brief communication. Usually, the requester does not know the physical address. So, the request is broadcasted to all the machines on the network. Now, the requester must identify is self uniquely to the server. For this either CPU serial number or the machine's physical network address can be used. But using the physical address as a unique id has two advantages.

- These addresses are always available and do not have to be bound into bootstrap code.
- Because the identifying information depends on the network and not on the CPU vendor, all machines on a given network will supply unique identifiers.

Request:

Like an ARP message, a RARP message is sent from one machine to the another encapsulated in the data portion of a network frame. An Ethernet frame carrying a RARP request has the usual preamble, Ethernet source and destination addresses, and packet type fields in front of the frame. The frame contains the value 8035 (base 16) to identify the contents of the frame as a RARP message. The data portion of the frame contains the 28-octet RARP message. The sender broadcasts a RARP request that specifies itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All machines on the network receive the request, but only those authorized to supply the RARP services process the request and send a reply, such machines are known informally as RARP servers. For RARP to succeed, the network must contain at least one RARP server.

Reply:

Servers answers request by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request.

Timing RARP Transactions

Since RARP uses the physical network directly, no other protocol software will time the response or retransmit the request. RARP software must handle these tasks. Some workstations that rely on RARP to boot, choose to retry indefinitely until the receive a response. Other implementations announce failure after only a few tries to avoid flooding the network with unnecessary broadcast.

Multiple RARP Servers

Advantage: More reliability. Disadvantage: Overloading may result when all servers respond. So, to get away with disadvantage we have primary and secondary servers. Each machine that makes RARP request is assigned a primary server. Normally, the primary server responds but if it fails, then requester may time out and rebroadcast the request. Whenever a secondary server receives a second copy of the request within a short time of the first, it responds. But, still there might be a problem that all secondary servers respond, thus overloading the network. So, the solution adopted is to avoid having all secondary servers transmit responses simultaneously. Each secondary server that receives the request computes a random delay and then sends a response.

RARP Packet Format :

00	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
Hardware type																Protocol type															
Hardware address length								Protocol address length								Opcode															
Source hardware address																															
Source protocol address																															
Destination hardware address																															
Destination protocol address																															

Fig 1.14 RARP Packet Format

Hardware type 16 bits.

Protocol type 16 bits.

Protocol	**Description**
0x800	IP.

Hardware addresses length 8 bits.
Length of the hardware address in bytes.

Protocol addresses length 8 bits.
Length of the protocol address in bytes.

Opcode 8 bits.

Opcode	Description	References
3	Request Reverse.	RFC 903
4	Reply Reverse.	RFC 903

Source hardware addresses Variable length.

Source protocol addresses Variable length.

Destination hardware addresses Variable length.

Destination protocol addresses Variable length.

ARP Encapsulation :

An ARP is directly encapsulate in data link frame Type field indicates that data carried by the frame is ARP packet

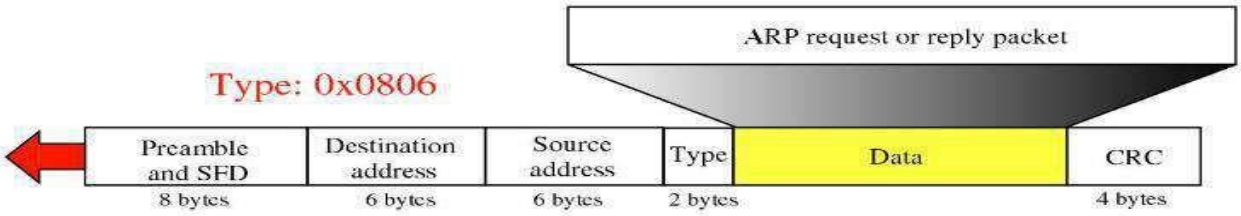


Fig 1.15 Encapsulation of ARP

Drawbacks of RARP

- Since it operates at low level, it requires direct address to the network which makes it difficult for an application programmer to build a server.
- It doesn't fully utilizes the capability of a network like Ethernet which is enforced to send a minimum packet size since the reply from the server contains only one small piece of information, the 32-bit internet address.

Department of Information Technology

Sub: Computer Network **Sub Code :IT-502**

UNIT II

DATA LINK LAYER:

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

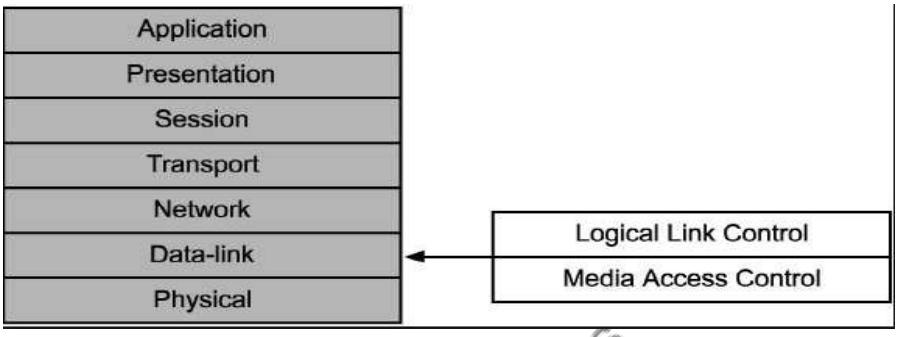


Fig. 2.1 Seven Layer Architecture

Data link layer has two sub-layers:

- Logical Link Control: It deals with protocols, flow-control, and error control
- Media Access Control: It deals with actual control of media

DATA LINK LAYER: SERVICE PROVIDED

- Encapsulation of network layer data packets into frames.
- Frame synchronization.
- Error Control
- Flow control, in addition to the one provided on the transport layer.
- LAN switching (packet switching) including MAC filtering and spanning tree protocol
- Data packet queuing or scheduling
- Store-and-forward switching or cut-through switching

DATA LINK LAYER: FRAMING

Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters. The four framing methods that are widely used are

- Character count
- Starting and ending characters, with character stuffing
- Starting and ending flags, with bit stuffing

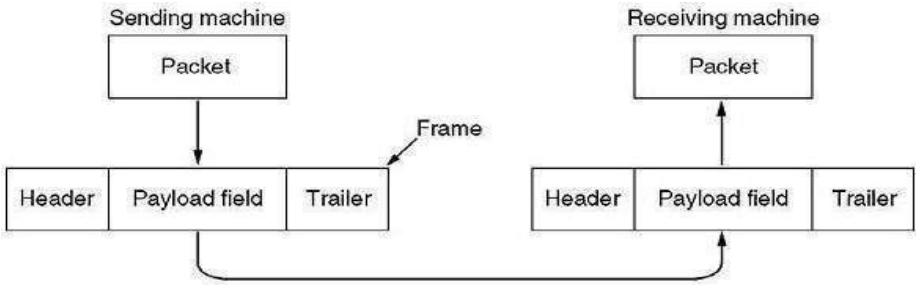


Fig. 2.2 Data Link Layer: Framing

Character Count

This method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow, and hence where the end of the frame is. The disadvantage is that if the count is garbled by a transmission error, the destination will lose synchronization and will be unable to locate the start of the next frame. So, this method is rarely used.

Character stuffing

In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX. This method overcomes the drawbacks of the character count method. However, character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

Bit stuffing

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing

Physical layer coding violations

The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

DATALINK LAYER: FLOW CONTROL

Flow control coordinates that amount of data that can be sent before receiving acknowledgement.

- It is one of the most important duties of the data link layer.
- Flow control tells the sender how much data to send.
- It makes the sender wait for some sort of an acknowledgment (ACK) before continuing to send more data.
- Flow Control Techniques: Stop-and-wait, and Sliding Window

DATA LINK LAYER: ERROR CONTROL

Error control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

To ensure reliable communication, there needs to exist flow control (managing the amount of data the sender sends), and error control (that data arrives at the destination error free).

- Flow and error control needs to be done at several layers.
- For node-to-node links, flow and error control is carried out in the data-link layer.
- For end-point to end-point, flow and error control is carried out in the transport layer.

There may be three types of errors:

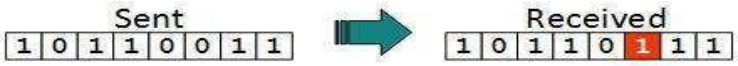


Fig. 2.3 Single bit error

In a frame, there is only one bit, anywhere though, which is corrupt.

Fig. 2.4 Multiple bits error

Frame is received with more than one bit in corrupted state.

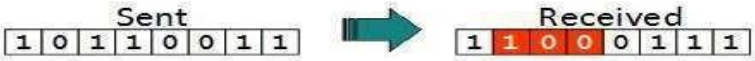


Fig. 2.5 Burst error

Frame contains more than1 consecutive bits corrupted.

DATA LINK LAYER PROTOCOL

The basic function of the layer is to transmit frames over a physical communication link. Transmission may be half duplex or full duplex. To ensure that frames are delivered free of errors to the destination station (IMP) a number of requirements are placed on a data link protocol. The protocol (control mechanism) should be capable of performing:

1. The identification of a frame (i.e. recognises the first and last bits of a frame).
2. The transmission of frames of any length up to a given maximum. Any bit pattern is permitted in a frame.
3. The detection of transmission errors.
4. The retransmission of frames which were damaged by errors.
5. The assurance that no frames were lost.
6. In a multidrop configuration some mechanism must be used for preventing conflicts caused by simultaneous transmission by many stations.
7. The detection of failure or abnormal situations for control and monitoring purposes.

It should be noted that as far as layer 2 is concerned a host message is pure data, every single bit of which is to be delivered to the other host. The frame header pertains to layer 2 and is never given to the host.

Elementary Data Link Protocols

- Data are transmitted in one direction only
- The transmitting (Tx) and receiving (Rx) hosts are always ready
- Processing time can be ignored
- Infinite buffer space is available

- No errors occur; i.e. no damaged frames and no lost frames (perfect channel)

Sliding Window protocol:

A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data Link Layer (OSI model) as well as in the Transmission Control Protocol (TCP).

The Sliding Window ARQ has three techniques

1. 1-bit
2. Go- Back N
3. Selective Repeat

1-bit

One-bit sliding window protocol is also called Stop-And-Wait protocol. In this protocol, the sender sends out one frame, waits for acknowledgment before sending next frame, thus the name Stop-And-Wait.

Problem with Stop-And-Wait protocol is that it is very inefficient. At any one moment, only in frame is in transition. The sender will have to wait at least one round trip time before sending next. The waiting can be long for a slow network such as satellite link.

Stop and Wait Protocol

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

Useful Terms:

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

  Propagation Delay = (Distance between routers) / (Velocity of propagation)
- RoundTripTime (RTT) = 2* Propagation Delay
- TimeOut (TO) = 2* RTT
- Time To Live (TTL) = 2* TimeOut. (Maximum TTL is 180 seconds)

Simple Stop and Wait

Sender:

Rule 1) Send one data packet at a time.

Rule 2) Send next packet only after receiving acknowledgement for previous.

Receiver:

Rule 1) Send acknowledgement after receiving and consuming of data packet.

Rule 2) after consuming packet acknowledgement need to be sent (Flow Control)

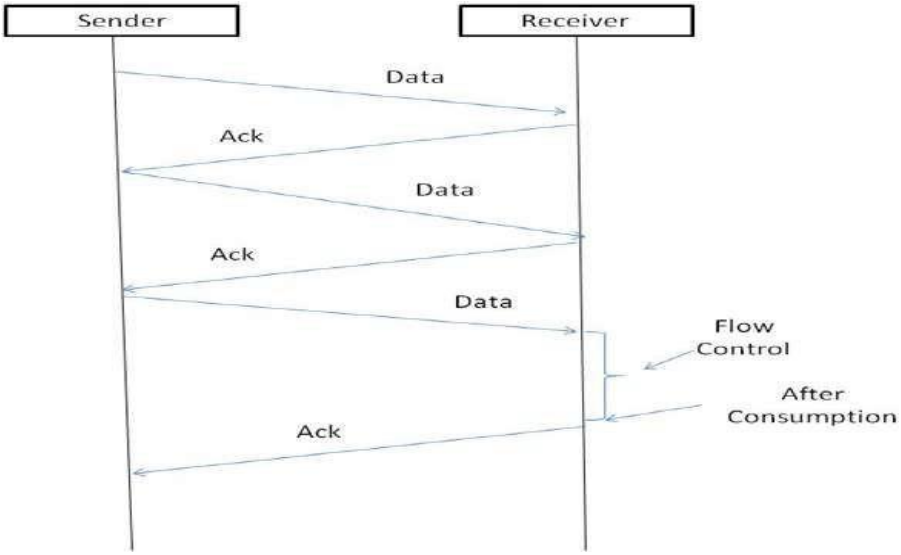


Fig. 2.6 Stop and Wait

Problems:

1. Lost Data

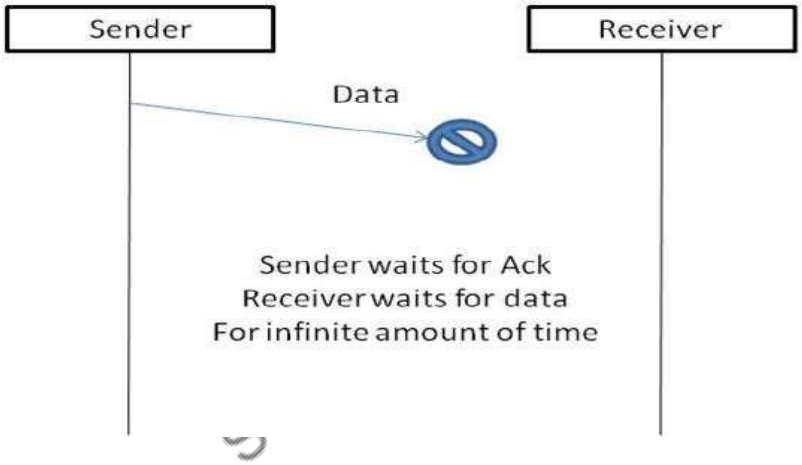


Fig. 2.7 Stop and Wait- Lost Data

2. Lost Acknowledgement:

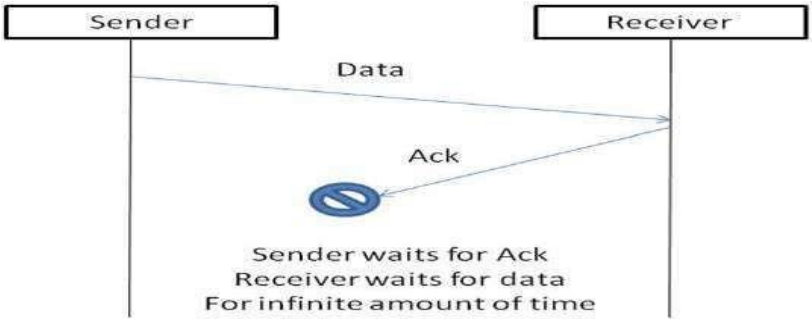


Fig. 2.8 Stop and Wait- Lost Acknowledgement

3. Delayed Acknowledgement/Data: After timeout on sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ (Automatic Repeat Request)

Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.

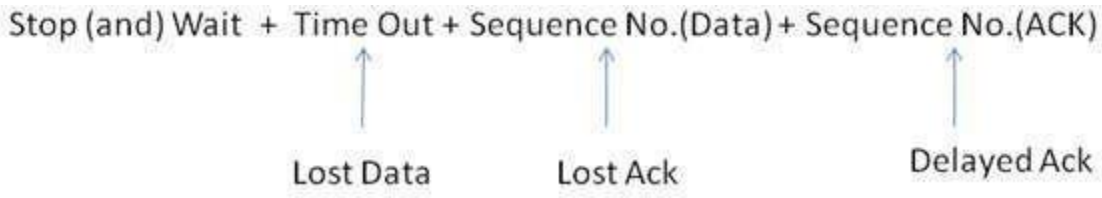


Fig. 2.9 Stop and Wait ARQ (Automatic Repeat Request)

1. Time Out:

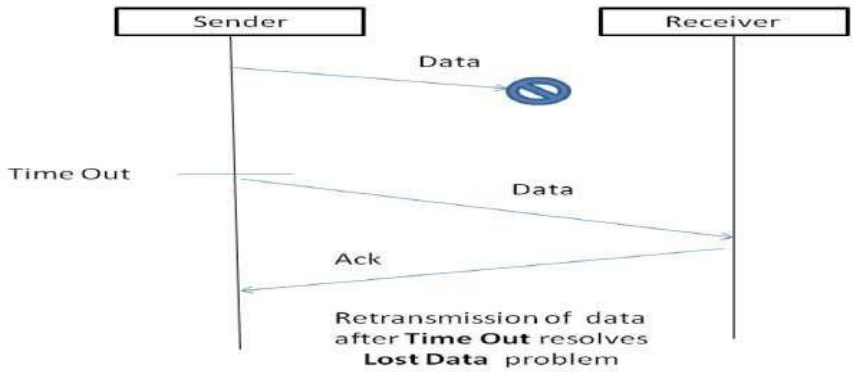


Fig. 2.10 Stop and Wait ARQ-Time Out

2. Sequence Number (Data)

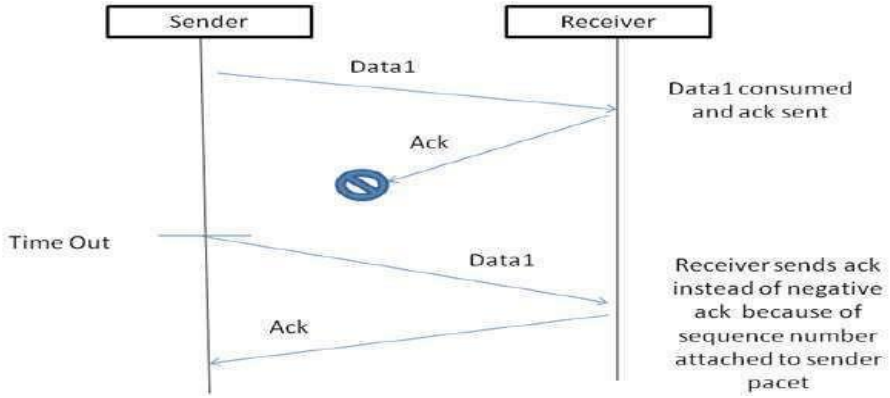


Fig. 2.11 Stop and Wait ARQ-ACK Lost

3. Delayed Acknowledgement:

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ:

1) Sender A sends a data frame or packet with sequence number 0.

2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)

There is only one-bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.

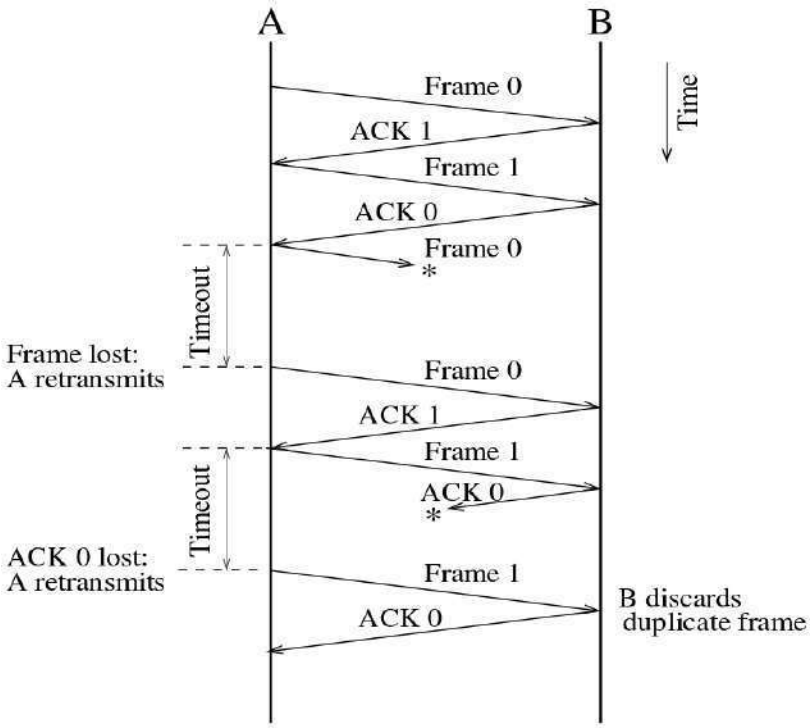


Fig. 2.12 Working of Stop and Wait ARQ

Characteristics of Stop and Wait ARQ:

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "**Closed Loop OR connection oriented** "protocols
- It is a special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequences numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. We will be discussing these protocols in next articles.

So, Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Go- Back N protocol

Go-Back-N protocol is a sliding window protocol. It is a mechanism to detect and control the error in datalink layer. During transmission of frames between sender and receiver, if a frame is damaged, lost, or an acknowledgement is lost then the action performed by sender and receiver.

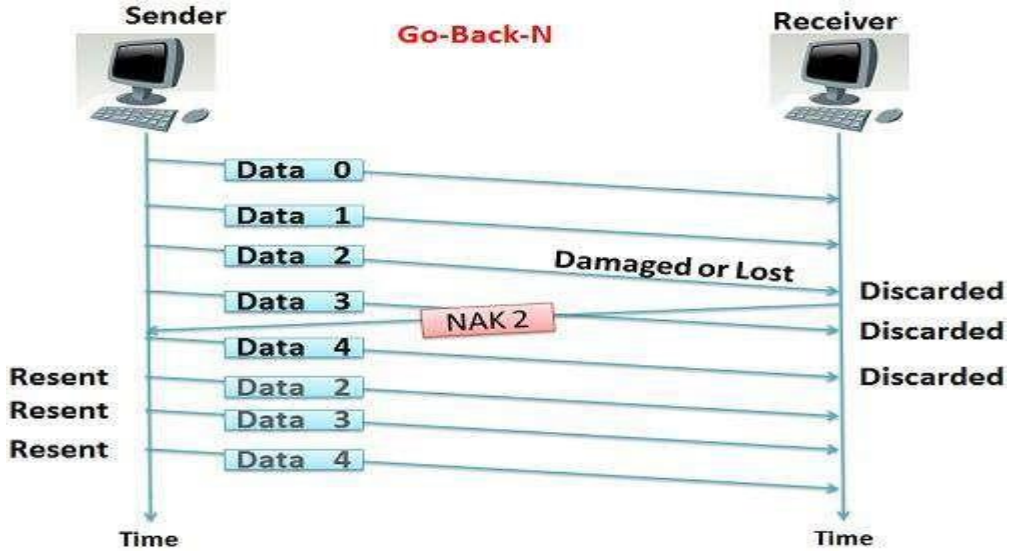


Fig. 2.13 Go- Back N protocol

Selective Repeat ARQ protocol

Selective repeat is also the sliding window protocol which detects or corrects the error occurred in datalink layer. The selective repeat protocol retransmits only that frame which is damaged or lost. In selective repeat protocol, the retransmitted framed is received out of sequence. The selective repeat protocol can perform following actions

- The receiver is capable of sorting the frame in a proper sequence, as it receives the retransmitted frame whose sequence is out of order of the receiving frame.
- The sender must be capable of searching the frame for which the NAK has been received.
- The receiver must contain the buffer to store all the previously received frame on hold till the retransmitted frame is sorted and placed in a proper sequence.
- The ACK number, like NAK number, refers to the frame which is lost or damaged.
- It requires the less window size as compared to go-back-n protocol.

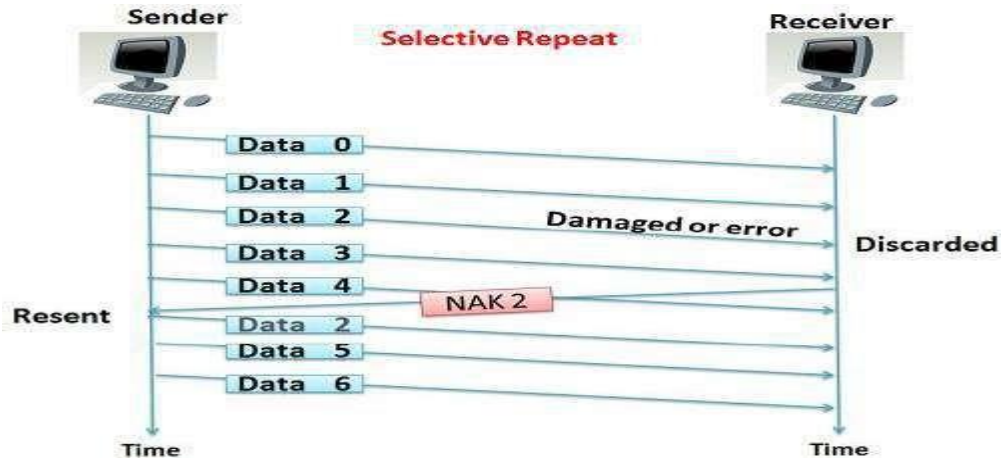


Fig. 2.14 Selective Repeat protocol

HYBRID ARQ

The HARQ is the use of conventional ARQ along with an Error Correction technique called 'Soft

Combining', which no longer discards the received bad data (with error).

With the 'Soft Combining' data packets that are not properly decoded are not discarded anymore. The received signal is stored in a 'buffer', and will be combined with next retransmission.

That is, two or more packets received each one with insufficient SNR to allow individual decoding can be combined in such a way that the total signal can be decoded!

The following image explains this procedure. The transmitter sends a package [1]. The package [1] arrives, and is 'OK'. If the package [1] is 'OK' then the receiver sends an 'ACK'.

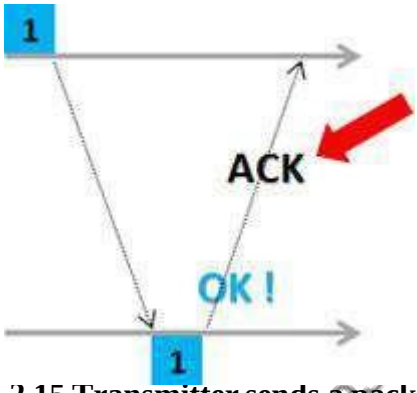


Fig. 2.15 Transmitter sends a packet-1

The transmission continues, and is sent a package [2]. The package [2] arrives, but let's consider now that it arrives with errors. If the package [2] arrives with errors, the receiver sends a 'NACK'.

Fig. 2.16 Transmitter sends a packet-2

Only now this package [2] (bad) is not thrown away, as it is done in conventional ARQ. Now it is stored in a 'buffer'.

Fig. 2.17 Receiver buffers a packet-2

Continuing, the transmitter sends another package [2.1] that also (let's consider) arrives with errors.

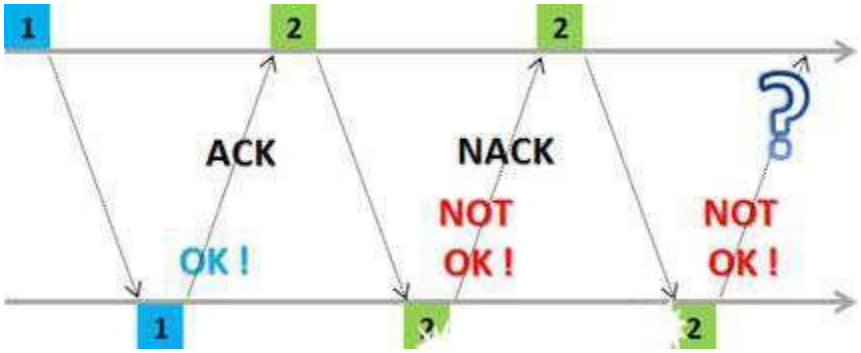


Fig. 2.18 Transmitter sends another packet-2

We have then in a buffer: bad package [2], and another package [2.1] which is also bad.

Does by adding (combining) these two packages ([2] + [2.1]) we have the complete information?

Yes. So, we send an 'ACK'.

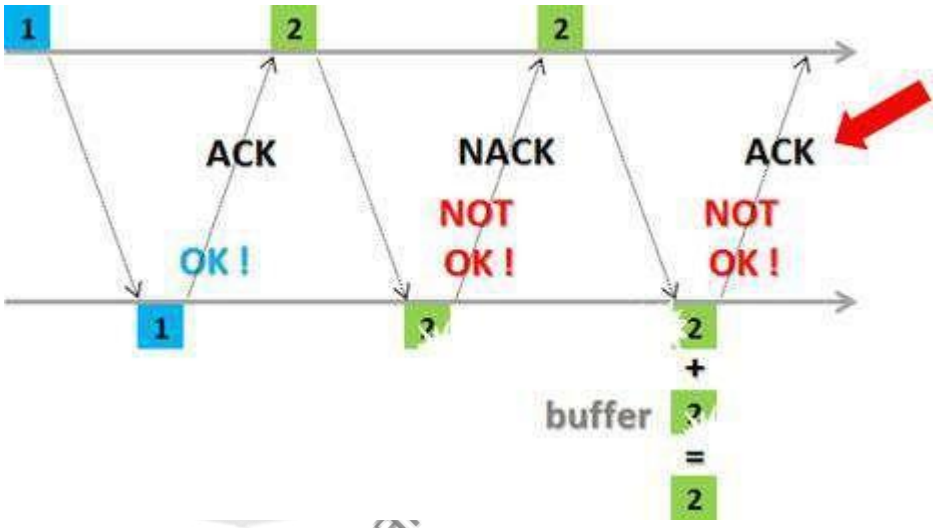


Fig. 2.19 Receiver combining buffers a packet-2 and another packet-2

But if the combination of these two packages still does not give us the complete information, the process must continue - and another 'NACK' is sent.

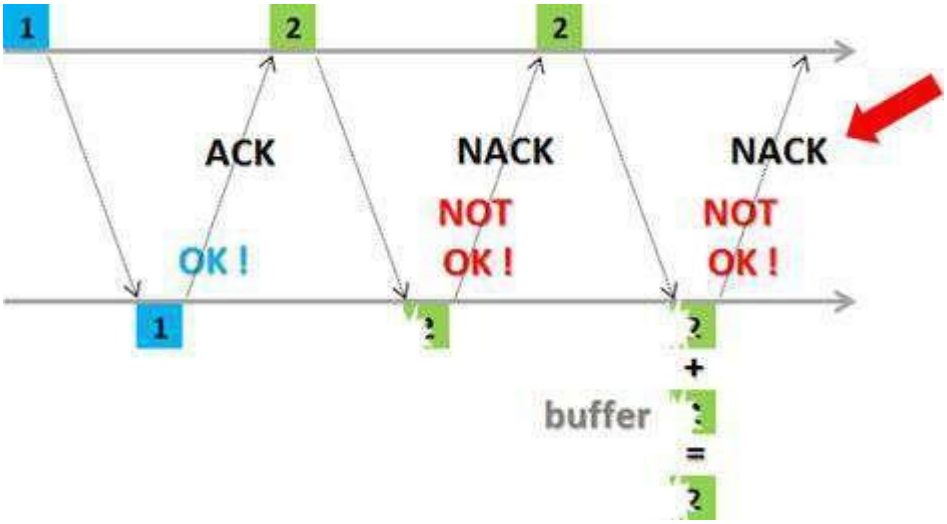


Fig. 2.20 Receiver sends NACK

And there we have another retransmission. Now the transmitter sends a third package [2.2].

Let's consider that now it is 'OK', and the receiver sends an 'ACK'.

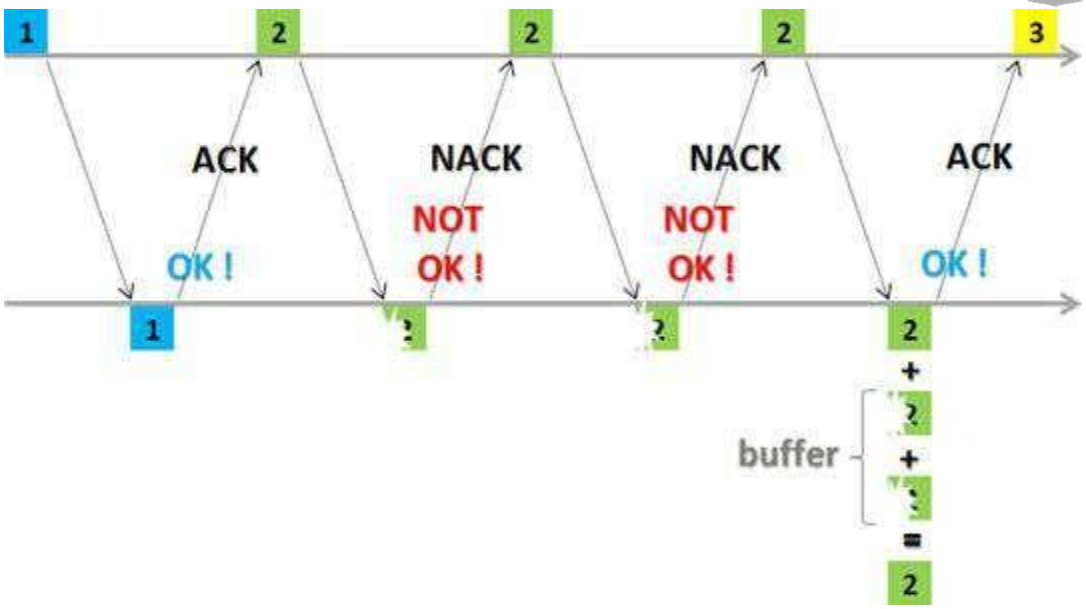


Fig. 2.21 Receiver sends ACK

Here we can see the following: along with the received package [2.2], the receiver also has packages [2] and [2.1] that have not been dropped and are stored in the buffer.

In our example, we see that the package arrived 2 times 'wrong'. And what is the limit of these retransmissions? Up to 4. IE, we can have up to 4 retransmissions in each process. This is the maximum number supported by 'buffer'.

BIT ORIENTED PROTOCOLS

A bit-oriented protocol is a communications protocol that sees the transmitted data as an opaque stream of bits with no semantics, or meaning. Control codes are defined in terms of bit sequences instead of characters. Bit oriented protocol can transfer data frames regardless of frame contents. It can also be stated as "bit stuffing" this technique allows the data frames to contain an arbitrary number of bits and allows character codes with arbitrary number of bits per character.

SDLC

Synchronous Data Link Control (SDLC) supports a variety of link types and topologies. It can be used with point-to-point and multipoint links, bounded and unbounded media, half-duplex and full-duplex transmission facilities, and circuit-switched and packet-switched networks.

SDLC identifies two types of network nodes: primary and secondary. Primary nodes control the operation of other stations, called secondary. The primary polls the secondary in a predetermined order and secondary can then transmit if they have outgoing data. The primary also sets up and tears down links and manages the link while it is operational. Secondary nodes are controlled by a primary, which means that secondary can send information to the primary only if the primary grants permission.

SDLC primaries and secondary can be connected in four basic configurations:

- Point-to-point---Involves only two nodes, one primary and one secondary.
- Multipoint---Involves one primary and multiple secondary.
- Loop---Involves a loop topology, with the primary connected to the first and last secondary. Intermediate secondary pass messages through one another as they respond to the requests of the

primary.

- Hub go-ahead---Involves an inbound and an outbound channel. The primary uses the outbound channel to communicate with the secondary. The secondary use the inbound channel to communicate with the primary. The inbound channel is daisy-chained back to the primary through each secondary.

SDLC Frame Format

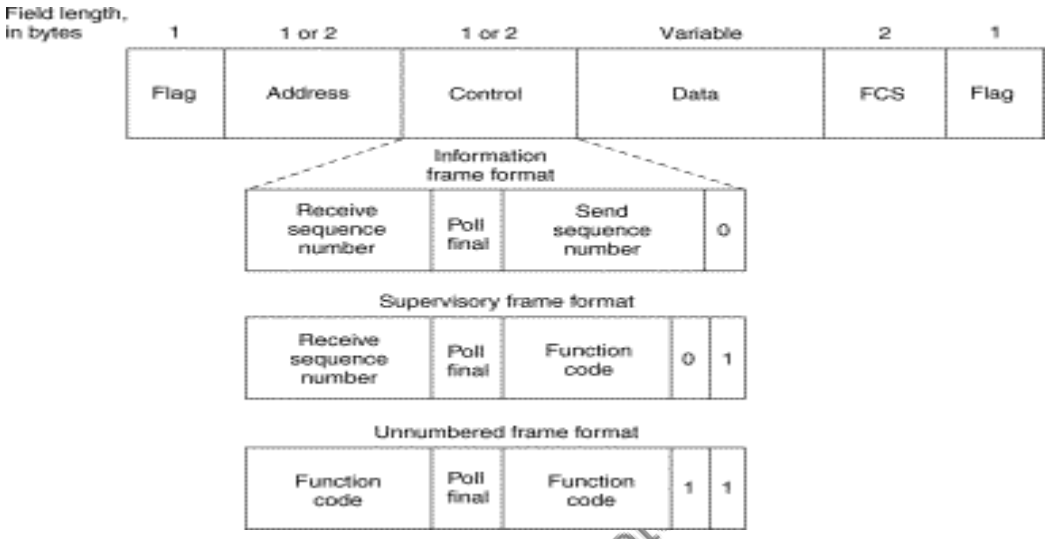


Fig. 2.22 SDLC Frame Format

- **Flag**---Initiates and terminates error checking.
- **Address**---Contains the SDLC address of the secondary station, which indicates whether the frame comes from the primary or secondary. This address can contain a specific address, a group address, or a broadcast address. A primary is either a communication source or a destination, which eliminates the need to include the address of the primary.
- **Control**---Employs three different formats, depending on the type of SDLC frame used:
  1. **Information (I) frame:** Carries upper-layer information and some control information. This frame sends and receives sequence numbers, and the poll final (P/F) bit performs flow and error control. The send-sequence number refers to the number of the frame to be sent next. The receive-sequence number provides the number of the frame to be received next. Both sender and receiver maintain send- and receive-sequence numbers.

     A primary station uses the P/F bit to tell the secondary whether it requires an immediate response. A secondary station uses the P/F bit to tell the primary whether the current frame is the last in its current response.
  2. **Supervisory (S) frame:** Provides control information. An S frame can request and suspend transmission, reports on status, and acknowledge receipt of I frames. S frames do not have an information field.
  3. **Unnumbered (U) frame:** Supports control purposes and is not sequenced. A U frame can be used to initialize secondary. Depending on the function of the U frame, its control field is 1 or 2 bytes. Some U frames have an information field.
- **Data**---Contains path information unit (PIU) or exchange identification (XID) information.
- **Frame Check Sequence (FCS)** ---Precedes the ending flag delimiter and is usually a cyclic

redundancy check (CRC) calculation remainder. The CRC calculation is redone in the receiver. If the result differs from the value in the original frame, an error is assumed.

Piggybacking and Protocol pipelining

In reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.

Communications are mostly full – duplex in nature, i.e. data transmission occurs in both directions. A method to achieve full – duplex communication is to consider both the communication as a pair of simplex communication. Each link comprises a forward channel for sending data and a reverse channel for sending acknowledgments.

However, in the above arrangement, traffic load doubles for each data unit that is transmitted. Half of all data transmission comprise of transmission of acknowledgments.

So, a solution that provides better utilization of bandwidth is piggybacking. Here, sending of acknowledgment is delayed until the next data frame is available for transmission. The acknowledgment is then hooked onto the outgoing data frame. The data frame consists of an *ack* field. The size of the *ack* field is only a few bits, while an acknowledgment frame comprises of several bytes. Thus, a substantial gain is obtained in reducing bandwidth requirement.

Working Principle of Piggybacking

Suppose that there are two communication stations X and Y. The data frames transmitted have an acknowledgment field, *ack* field that is of a few bits length. Additionally, there are frames for sending acknowledgments, ACK frames. The purpose is to minimize the ACK frames.

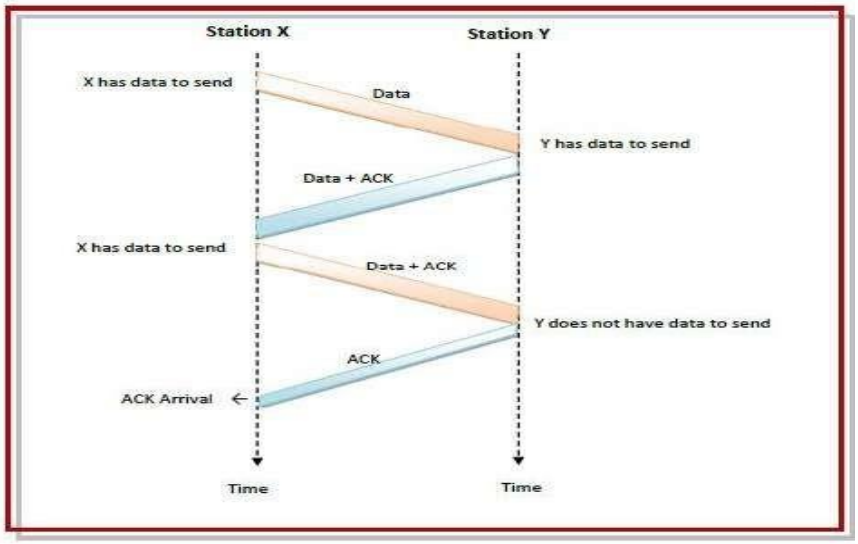


Fig. 1.23 Working Principle of Piggybacking

The three principles governing piggybacking when the station X wants to communicate with station Y are:

1. If station X has both data and acknowledgment to send, it sends a data frame with the *ack* field containing the sequence number of the frame to be acknowledged.
2. If station X has only an acknowledgment to send, it waits for a finite period of time to see whether a data frame is available to be sent. If a data frame becomes available, then it piggybacks the acknowledgment with it. Otherwise, it sends an ACK frame.
3. If station X has only a data frame to send, it adds the last acknowledgment with it. The station Y discards all duplicate acknowledgments. Alternatively, station X may send the data frame with the *ack* field containing a bit combination denoting no acknowledgment.

Protocol pipelining is a technique in which multiple requests are written out to a single socket without waiting for the corresponding responses. Pipelining can be used in various application layer network protocols, like HTTP/1.1, SMTP and FTP.

The pipelining of requests results in a dramatic improvement in protocol performance, especially over high latency connections (such as satellite Internet connections).Pipelining reduces waiting time of a process.

HDLC

High-Level Data Link Control (HDLC) is a bit-oriented code-transparent synchronous data link layer protocol. HDLC provides both connection-oriented and connectionless service. HDLC can be used for point to multipoint connections, but is now used almost exclusively to connect one device to another, using what is known as Asynchronous Balanced Mode (ABM). The original master-slave modes Normal Response Mode (NRM) and Asynchronous Response Mode (ARM) are rarely used.

FRAMING

HDLC frames can be transmitted over synchronous or asynchronous serial communication links. Those links have no mechanism to mark the beginning or end of a frame, so the beginning and end of each frame has to be identified. This is done by using a frame delimiter, or flag, which is a unique sequence of bits that is guaranteed not to be seen inside a frame. This sequence is '01111110', or, in hexadecimal notation, 0x7E. Each frame begins and ends with a frame delimiter. A frame delimiter at the end of a frame may also mark the start of the next frame. A sequence of 7 or more consecutive 1-bits within a frame will cause the frame to be aborted.

When no frames are being transmitted on a simplex or full-duplex synchronous link, a frame delimiter is continuously transmitted on the link. Using the standard NRZI encoding from bits to line levels (0 bit = transition, 1 bit = no transition), this generates one of two continuous waveforms, depending on the initial state:

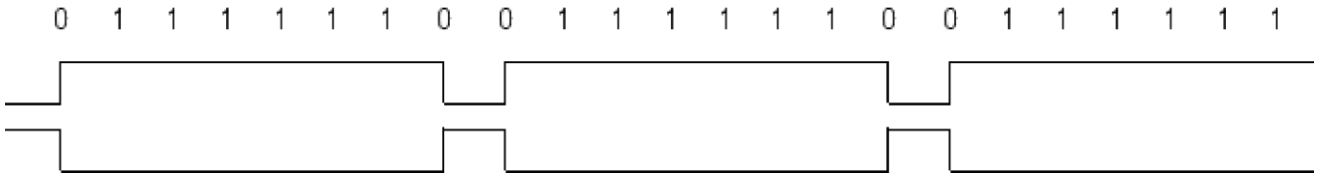


Fig. 2.24 HDLC Framing

This is used by modems to train and synchronize their clocks via phase-locked loops. Some protocols allow the 0-bit at the end of a frame delimiter to be shared with the start of the next frame delimiter, i.e.

'011111101111110'.

Frame structure

The contents of an HDLC frame are shown in the following table:

Flag	Address	Control	Information	FCS	Flag
8 bits	8 or more bits	8 or 16 bits	Variable length, 0 or more bits	16 or 32 bits	8 bits

Fig. 2.25 HDLC Frame structure

Note that the end flag of one frame may be (but does not have to be) the beginning (start) flag of the next frame.

Data is usually sent in multiples of 8 bits, but only some variants require this; others theoretically permit data alignments on other than 8-bit boundaries.

There are three fundamental types of HDLC frames.

- Information frames, or I-frames, transport user data from the network layer. In addition, they can also include flow and error control information piggybacked on data.
- Supervisory Frames, or S-frames, are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send. S-frames do not have information fields.
- Unnumbered frames, or U-frames, are used for various miscellaneous purposes, including link management. Some U-frames contain an information field, depending on the type.

LLC and MAC sub-layers of Data Link Layer

This post gives a brief overview of the two sub-layers of the data link layer, namely **LLC (Logical Link Control)** and **MAC (Media Access Control)**. The data link layer functionality is usually split it into logical sub-layers, the upper sub-layer, termed as LLC, that interacts with the network layer above and the lower sub-layer, termed as MAC, that interacts with the physical layer below, as shown in the diagram given below:

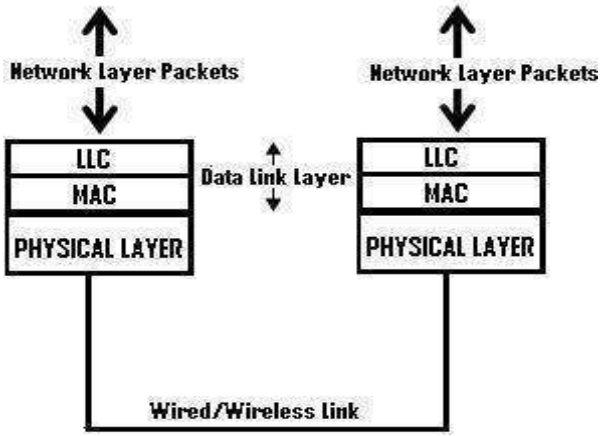


Fig .2.26 per and Lower sub-layers of Data Link Layer

While LLC is responsible for handling multiple Layer3 protocols (multiplexing/de-multiplexing) and link services like reliability and flow control, the MAC is responsible for framing and media access control for broadcast media. The functional overview of LLC and MAC sub-layers are given in the diagram below :

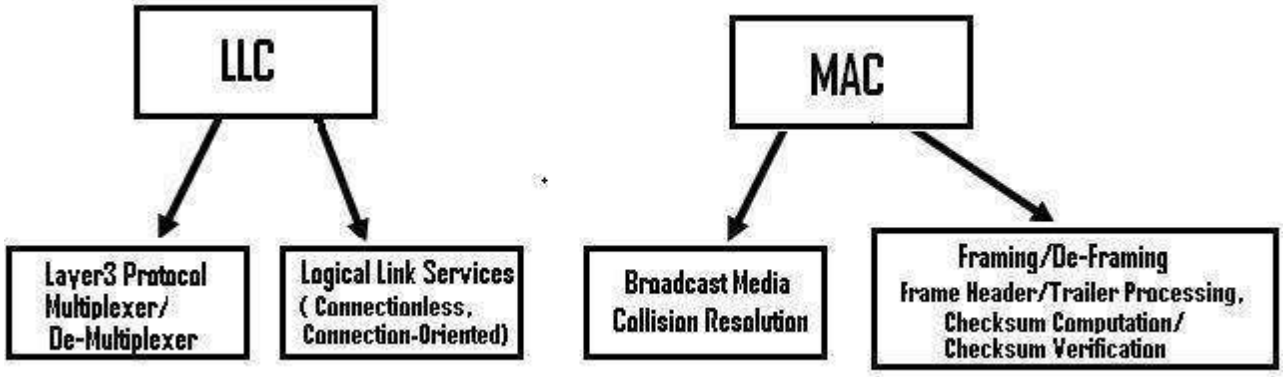


Fig .2.27 Role of LLC and MAC

LLC

The primary responsibilities of LLC are:

Network Layer protocol Multiplexing/De-Multiplexing

Interfacing with the Network (Layer3) above by doing L3 protocol multiplexing/de-multiplexing. On receiving a frame from the physical layer below, the LLC is responsible for looking at the L3 Protocol type and handing over the datagram to the correct L3 protocol (de-multiplexing) at the network layer above. On the sending side, LLC takes packets from different L3 protocols like IP, IPX, ARP etc., and hands it over to the MAC layer after filling the L3 protocol type in the LLC header portion of the frame (multiplexing).

Logical Link Services

LLC can optionally provide reliable frame transmission by the sending node numbering each transmitted frame (sequence number), the receiving node acknowledging each received frame (acknowledgment number) and the sending node retransmitting lost frames. It can also optionally provide flow control by allowing the receivers to control the sender's rate through control frames like RECEIVE READY and RECEIVE NOT READY etc.

Based on whether a logical connection is established between the layer 2 peers and based on whether frames are acknowledged by the peer, LLC can be classified to provide the following types of service modes:

a) **Connectionless Unacknowledged Service :** This is a best effort service like IP datagram service, with no connection establishment between L2 peers and also no acknowledgment for data frames from the peer. Whenever there is data to be transferred to the peer, it is sent directly, without any connection establishment.

Flow control may be optionally provided in this service. In Internet, since reliability, flow control and error control are provided at the transport layer by TCP, a simple connectionless unacknowledged service is enough at the data link layer, provided the link is of good quality with low error rates. Hence, this service mode is the most widely used mode in the Internet, where TCP/IP is the basic protocol stack. This mode is used on almost all high quality wired links like Ethernet and Optical.

b) **Connectionless Acknowledged Service:** In this mode, data is directly sent between Layer2 peers without any logical link establishment. But each frame is numbered using sequence numbers and the peer acknowledges each frame received using an Acknowledgment number field. This service mode is used in scenarios where the overhead of a connection establishment is costly due to the extra delay involved, but where data reliability is needed. The sender can track lost or damaged frames and retransmit such frames to achieve reliability. This type of service is used in wireless links, where the quality of link is not as good as wired links and so frequent link establishment and teardown are unnecessary overheads, as these control frames may themselves be corrupted or lost.

c) **Connection Oriented Service:** In this mode, procedures are laid out for logical link establishment and disconnection. Before data transfer, a logical connection is established between peers, before data transfer starts, through the exchange of control frames, known as **Supervisory Frames**. The logical connection is closed after the data exchange phase is over. Actual data transfer starts after the connection establishment phase and frames carrying higher layer data are known as **Information Frames**. A third category of frames, known as Unumbered Acknowledgment frames are used to acknowledge received Supervisory frames.

In this mode too, there are two variants that are used, namely one without acknowledgement and another with acknowledgement.

Connection oriented service Without Acknowledgment

Here, though a logical link is established before actual data transfer happens, there is no concept of frames being numbered and acknowledged through Sequence number and acknowledgment number fields. It is just a best effort service, with reliability left to the higher layer protocol. Many WAN protocols like HDLC, PPP, LAPB, LAPD etc. use this mode of service.

Connection oriented service with Acknowledgment

Here, apart from a logical link being established before data transfer happens, reliability and flow control services are also provided by the LLC. Reliability is provided through the use of sequence number, acknowledgment number and retransmission of lost frames using strategies like **Go Back N** or **Selective Repeat**. **Flow control** is provided by using a **sliding window mechanism**. This service mode is rarely used in the Internet, because Internet uses TCP, that supports reliability and flow control at the transport layer. This service mode is used in properietary protocols like Microsoft's NetBIOS.

Note that though connection establishment, reliability and flow control are optional services at the data link layer, error detection is still a basic service provided by the data link layer, through the use of CRC/checksums in the frame trailer, that is added by the MAC sub-layer framing functionality.

MAC

The MAC sub-layer interacts with the physical layer and is primarily responsible for framing/de-framing and collision resolution.

Framing/De-Framing and interaction with PHY: On the sending side, the MAC sub-layer is responsible for creation of frames from network layer packets, by adding the frame header and the frame trailer. While the frame header consists of layer2 addresses (known as MAC address) and a few other fields for control purposes, the frame trailer consists of the CRC/checksum of the whole frame. After creating a frame, the MAC layer is responsible for interacting with the physical layer processor (PHY) to transmit the frame.

On the receiving side, the MAC sub-layer receives frames from the PHY and is responsible for accepting each frame, by examining the frame header. It is also responsible for verifying the checksum to conclude whether the frame has come uncorrupted through the link without bit errors. Since checksum computation and verification are compute intensive tasks, the framing/de-framing functionality is done by **dedicated piece of hardware (e.g. NIC card on PCs)**.

Collision Resolution : On shared or broadcast links, where multiple end nodes are connected to the same link, there has to be a collision resolution protocol running on each node, so that the link is used cooperatively. The MAC sub-layer is responsible for this task and it is the MAC sub-block that implements standard collision resolution protocols like CSMA/CD, CSMA etc. For half-duplex links, it is the MAC sub-layer that makes sure that a node sends data on the link only during its turn. For full-duplex point-to-point links, the collision resolution functionality of MAC sub-layer is not required.

IEEE Standards 802 series & their variant

802.2 Logical Link Control

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc). Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware. The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

802.3 Ethernet

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.5 Token Ring

Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber. Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.11 Wireless Network Standards

802.11 is the collection of standards setup for wireless networking. You are probably familiar with the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

802.11a was one of the first wireless standards. 802.11a operates in the 5Ghz radio band and can achieve a maximum of 54Mbps. Wasn't as popular as the 802.11b standard due to higher prices and lower range.

802.11b operates in the 2.4Ghz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular.

802.11g is a standard in the 2.4Ghz band operating at 54Mbps. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band.

Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance. It has a "listen before talk" method of minimizing collisions on the wireless network. This results in less need for retransmitting data. Wireless standards operate within a wireless topology.

Data Services (ALOHA and Slotted ALOHA)

ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. The original system used for ground-based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. A scientest developed a protocol that would increase the capacity of aloha two-fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versions

Types of ALOHA:

(i) Pure ALOHA

(ii) Slotted ALOHA

(i) Pure ALOHA

- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

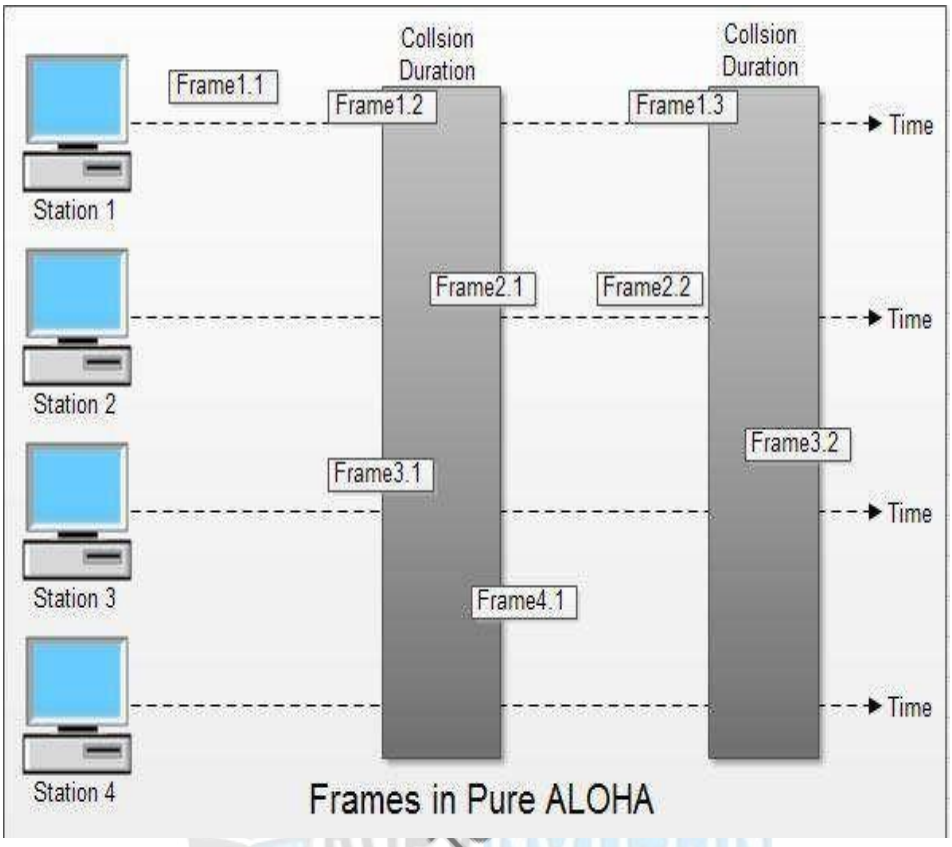


Fig 2.28 Pure ALOHA

(ii) Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

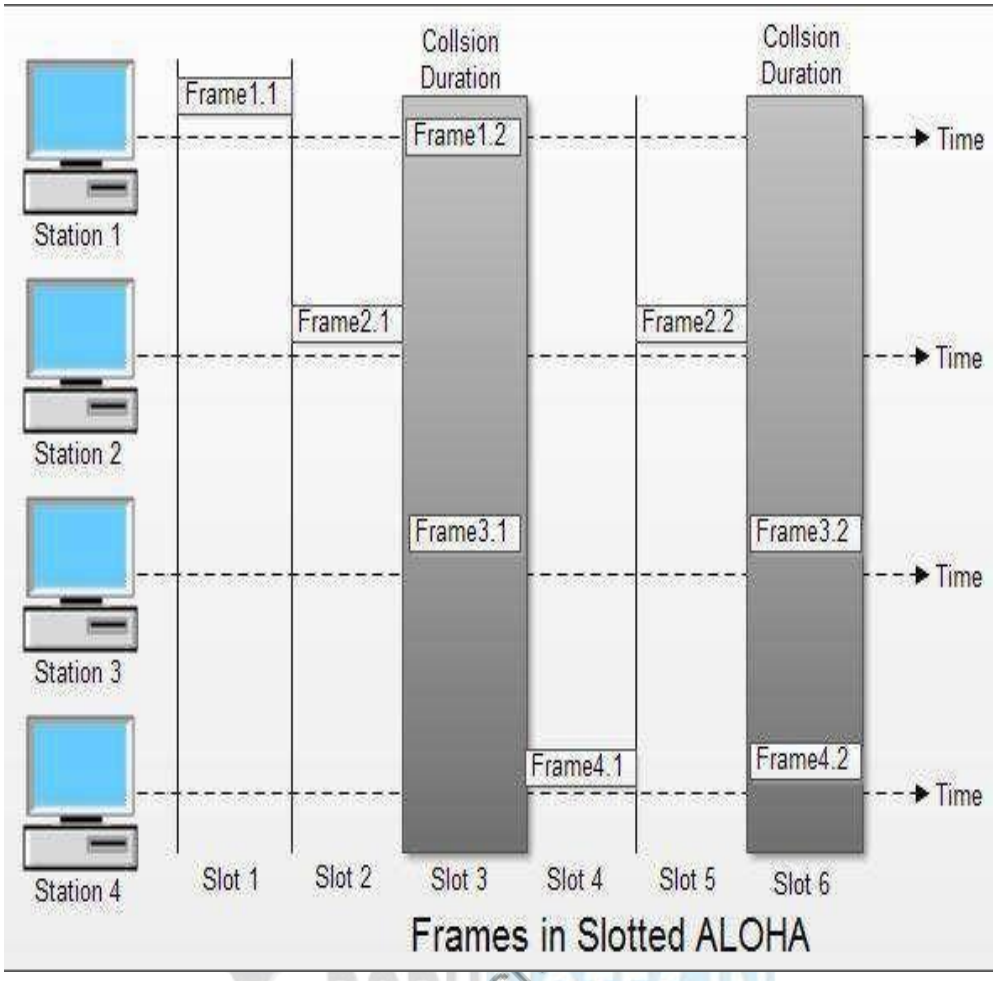


Fig 2.29 Slotted ALOHA

For Local-Area Networks (CSMA, CSMA/CD, CSMA/CA)

Carrier sense multiple access (CSMA) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

Carrier sense means that a transmitter uses feedback from a receiver to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier wave from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk".

Multiple access means that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations connected to the medium.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

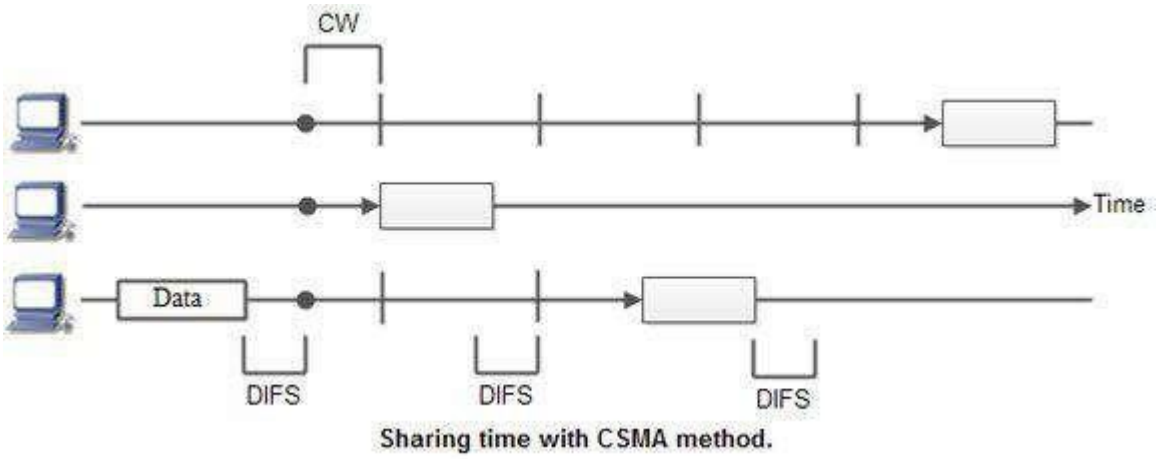


Fig 2.30 CSMA

There Are Three Different Type of CSMA Protocols

(I) 1-persistent CSMA

(ii) Non- Persistent CSMA

(iii) p-persistent CSMA

(i) 1-persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start allover again.

Drawback of I-persistent

The propagation delay time greatly affects this protocol. Let us suppose, just after the station 1 begins its transmission, station 2 also became ready to send its data and senses the channel. If the station 1 signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

Even if propagation delay time is zero, collision will still occur. If two stations became .ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

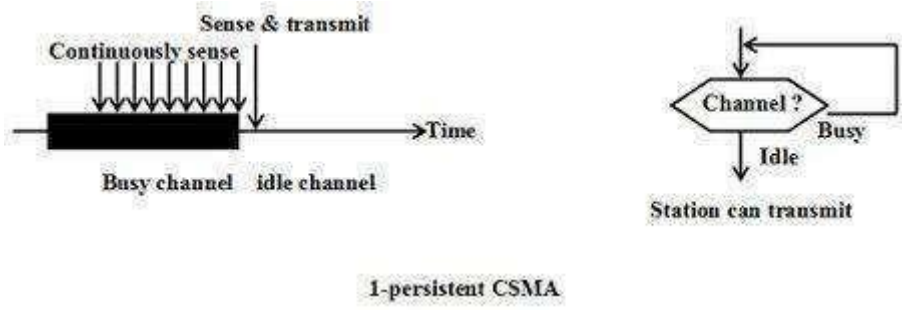


Fig 2.31-persistent CSMA

(ii) Non-persistent CSMA

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval oftime.
- After this time, it again checks the status of the channel and if the channel is.free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

- It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

- It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.

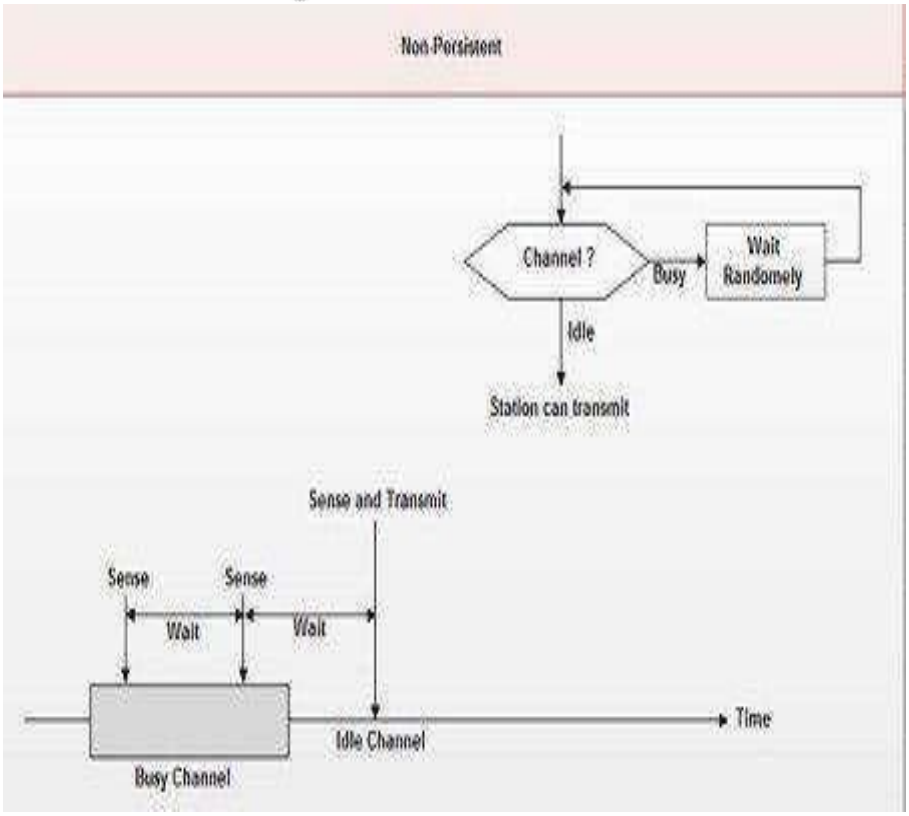


Fig 2.32 Non-persistent CSMA

(iii) p-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send, it senses the channel.
- If channel is busy, station waits until next slot.
- If channel is idle, it transmits with a probability p.
- With the probability q=1-p, the station then waits for the beginning of the next time slot.
- If the next slot is also idle, it either transmits or waits again with probabilities p and q.
- This process is repeated till either frame has been transmitted or another station has begun transmitting.

- In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

Advantage of p-persistent

- It reduces the chance of collision and improves the efficiency of the network.

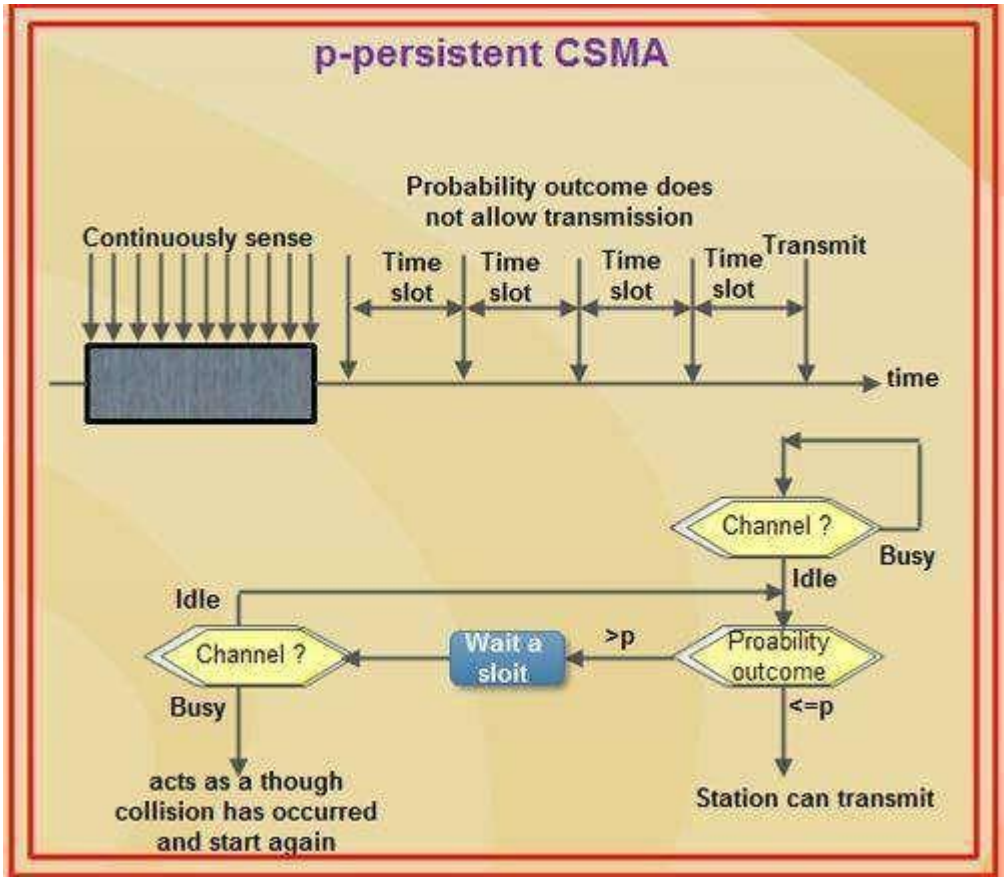


Fig 2.33 p-persistent CSMA

CSMA/CD - Carrier Sense Multiple Access / Collision Detection

To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD): CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits. it listens at the same time on communication media to ensure that there is no collision with a packet sent by another station. In a collision, the issuer immediately cancel the sending of the package. This allows to limit the duration of collisions: we do not waste time to send a packet complete if

it detects a collision. After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the "decline") exponential. In fact, the window collision is simply doubled (unless it has already reached a maximum). From a packet is transmitted successfully, the window will return to its original size.

Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again. If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

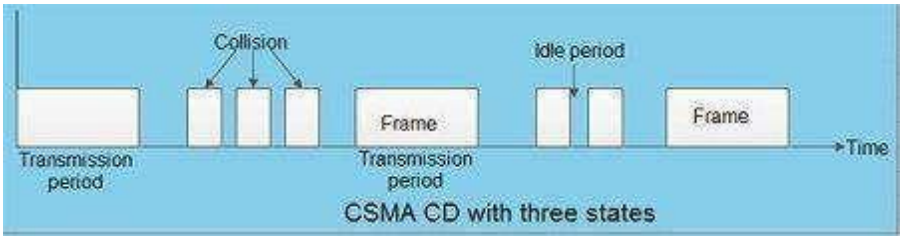


Fig 2.34 CSMA/CD

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.

• CSMA/CA avoids the collisions using three basic techniques.

(i) Interframe space

(ii) Contention window

(iii) Acknowledgements

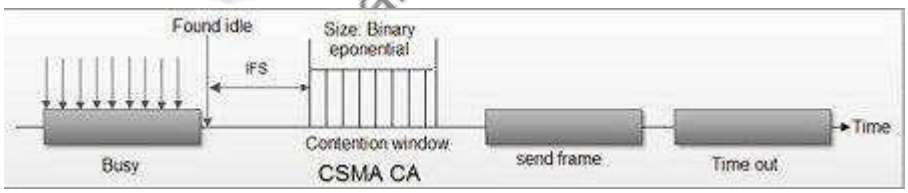


Fig 2.35 CSMA/CA

Comparision between all with an BAR Chart

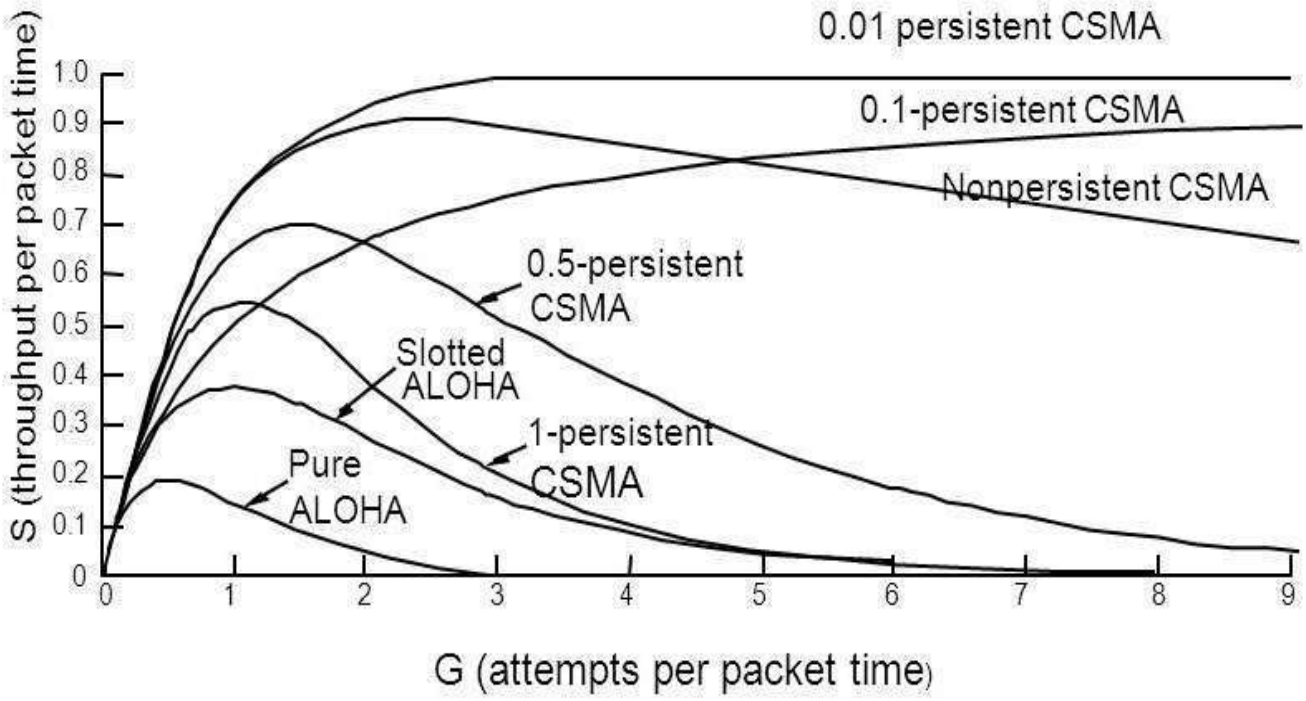


Fig 2.36 Comparision between all with an BAR Chart

1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

3. Acknowledgement

- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgment and the time-out timer can help guarantee that receiver has received the

frame.

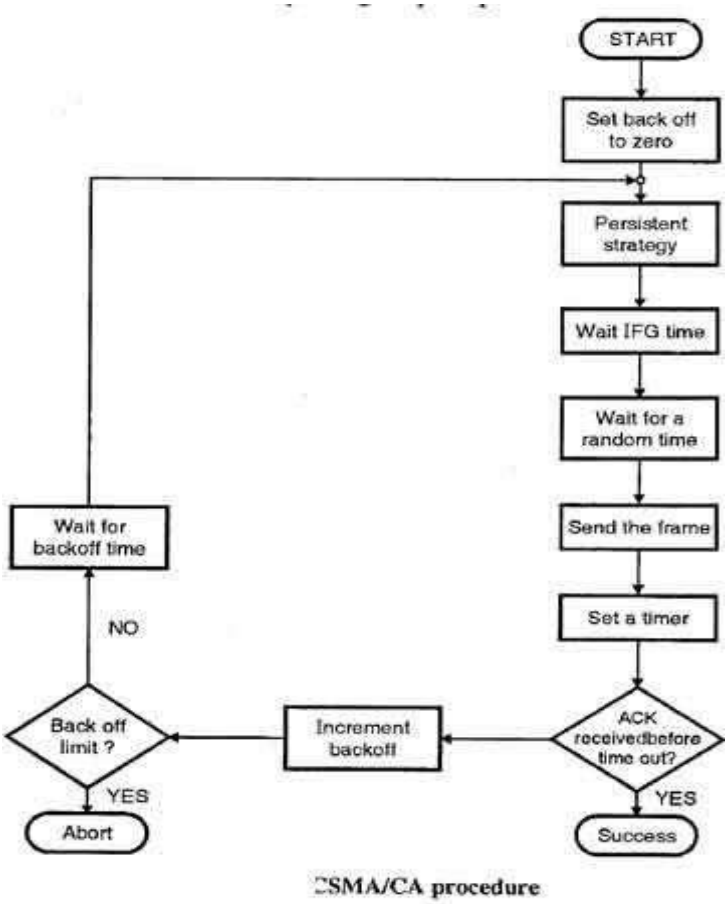


Fig 2.37 Flow Chart of CSMA/CA

Hidden Node Problem

In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B. The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".

Exposed Node Problem

If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C trnasmitting. Even if B would have transmitted to A, it would not have been a problem at A or D. CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel.

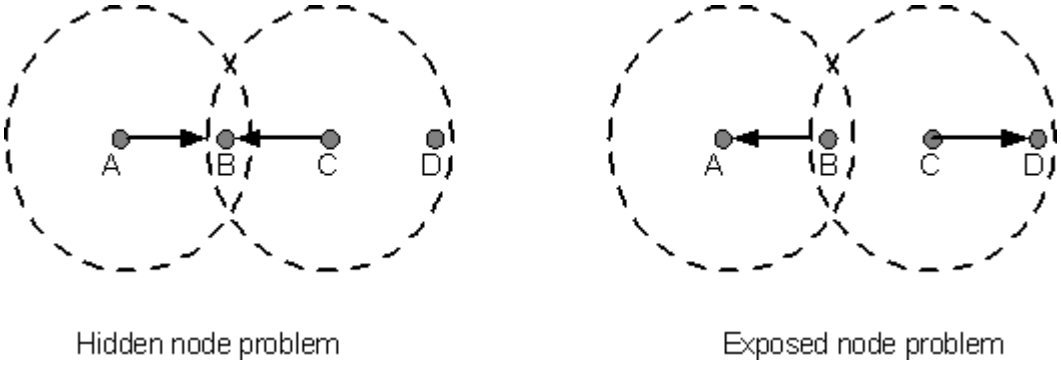


Fig 2.38 Hidden and Exposed Node Problem

Collision Free Protocols: Basic Bit Map, BRAP, Binary Count Down

Collision Free Protocols

A collision-free protocol for transmitting frames between stations connected over a shared transmission medium such as an IEEE 802.3 Ethernet LAN. A logical ring is formed and a token is circulated among the connected stations part of the logical ring (not all connected stations are required to be part of the logical ring). Transmitting from any one station, part of the logical ring, is permitted only while holding the token, therefore preventing collisions. A collision-free protocol, over a standard Ethernet infrastructure, becomes feasible, yet remains compatible with the standard collision protocol, thus improving performances.

Basic Bit Map

1. Assume N stations are numbered from 1 to N.
2. There is a contention period of N slots (bits).
3. Each station has one slot time during the contention period, numbered 1 to N.
4. Station J sends a 1-bit reservation during Jth slot time if it wants to transmit a frame.
5. Every station sees all the 1-bit reservation transmitted during the contention period, so each station knows which stations want to transmit.
6. After the contention period, each station that asserted its desire to transmit sends its frame in the order of station number.

BRAP

Backup Route Aware Routing Program (BRAP) is a protocol that provides interdomain routing. BRAP uses reverse paths and backup paths to ensure fast failure recovery in networking systems.

Binary Countdown

In this protocol, a node which wants to signal that it has a frame to send does so by writing its address into the header as a binary number. The arbitration is such that as soon as a node sees that a higher bit position that is 0 in its address has been overwritten with a 1, it gives up. The final result is the address of the node which is allowed to send. After the node has transmitted the whole process is repeated all over again. Given below is an example situation.

Nodes	Addresses
A	0010
B	0101
C	1010
D	1001

	1010

Node C having higher priority gets to transmit. The problem with this protocol is that the nodes with higher address always wins. Hence this creates a priority which is highly unfair and hence undesirable.

MLMA protocol

Multi-Level Multi-Access (MLMA): The problem with BRAP is the delay when the channel is lightly loaded. When there is no frame to be transmitted, the N-bit headers just go on and on until a station inserts a 1 into its mini slot. On average, the waiting time would be N=2. MLAM scheme 41 is nearly as efficient under high channel load, but has shorter delay under low channel load. In MLAM, a station wants to

transmit a frame sends its identification in a particular format. A group of 10 bits (called decade) is used to represent a digit of the station number 48.

Limited Contention Protocols: Adaptive Tree Walk

Contention based and Contention - free has their own problems. Under conditions of light load, contention is preferable due to its low delay. As the load increases, contention becomes increasingly less attractive, because the overload associated with channel arbitration becomes greater. Just the reverse is true for contention - free protocols. At low load, they have high delay, but as the load increases, the channel efficiency improves rather than getting worse as it does for contention protocols.

Obviously, it would be better if one could combine the best properties of the contention and contention - free protocols, that is, protocol which used contention at low loads to provide low delay, but used a contention-free technique at high load to provide good channel efficiency. Such protocols do exist and are called Limited contention protocols.

It is obvious that the probability of some station acquiring the channel could only be increased by decreasing the amount of competition. The limited contention protocols do exactly that. They first divide the stations up into (not necessarily disjoint) groups. Only the members of group 0 are permitted to compete for slot 0. The competition for acquiring the slot within a group is contention based. If one of the members of that group succeeds, it acquires the channel and transmits a frame. If there is collision or no node of a particular group wants to send then the members of the next group compete for the next slot. The probability of a particular node is set to a particular value (optimum).

Adaptive Tree Walk Protocol

Initially all the nodes are allowed to try to acquire the channel. If it is able to acquire the channel, it sends its frame. If there is collision then the nodes are divided into two equal groups and only one of these groups compete for slot 1. If one of its member acquires the channel then the next slot is reserved for the other group. On the other hand, if there is a collision then that group is again subdivided and the same process is followed. This can be better understood if the nodes are thought of as being organised in a binary tree.

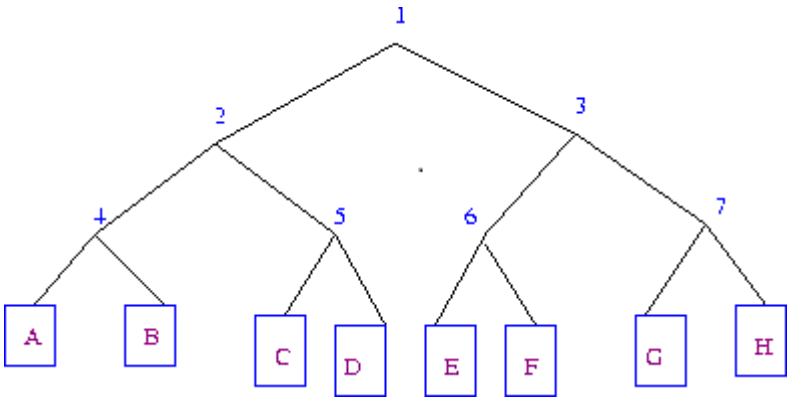


Fig 2.39 Adaptive Tree Walk

Many improvements could be made to the algorithm. For example, consider the case of nodes G and H being the only ones wanting to transmit. At slot 1 a collision will be detected and so 2 will be tried and it will be found to be idle. Hence it is pointless to probe 3 and one should directly go to 6,7.

URN Protocol

In computing, a uniform resource name (URN) is the historical name for a uniform resource identifier (URI) that uses the scheme. A URI is a string of characters used to identify a name of a web resource. Such identification enables interaction with representations of the web resource over a network, typically the World Wide Web, using specific protocols.

URNs were intended to serve as persistent, location-independent identifiers, allowing the simple mapping of namespaces into a single URN namespace. The existence of such a URI does not imply availability of the identified resource, but such URIs are required to remain globally unique and persistent, even when the resource ceases to exist or becomes unavailable.

(Uniform Resource Name) A name that identifies a resource on the Internet. Unlike URLs, which use network addresses (domain, directory path, file name), URNs use regular words that are protocol and location independent. Providing a higher level of abstraction, URNs are persistent (never change) and require a resolution service similar to the DNS system in order to convert names into real addresses. For the most part, URNs have evolved into XRI identifiers (see XDI). See URI and URL.

High Speed LAN: Fast Ethernet, Gigabit Ethernet

Name	IEEE Standards	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Fig 2.40 High Speed LAN: Fast Ethernet, Gigabit Ethernet

Key Differences between Fast Ethernet and Gigabit Ethernet

- Gigabit Ethernet is more advanced technology than Fast Ethernet having speed of 1000 Mbit/s, 10 times more than speed of Fast Ethernet, which is 100 Mbit/s.
- Due to more bit transfer speed and higher bandwidth, Gigabit Ethernet results in better performance than Fast Ethernet.
- Gigabit Ethernet is more expensive than Fast Ethernet. Upgrading of Fast Ethernet from Standard Ethernet is easy and cost effective while upgrading of Gigabit Ethernet from Fast Ethernet is complex and expensive.
- Configuration problems in Gigabit Ethernet are more complex than Fast Ethernet. Devices used in Gigabit Ethernet must have same configuration to function fully. While in Fast Ethernet, connected devices configure automatically with the system.
- Every network can support 100 Mbit/s but cannot support 1000 Mbit/s. So, specific network is required that can support the Gigabit Ethernet.

- Maximum length of 10 km network can be achieved in Fast Ethernet, if 100BASE-LX10 version is being used. While 70 km network length can be achieved in Gigabit Ethernet, if Single Mode Fiber (1,310 nm wavelength) is being used as a medium.
- Faster Ethernet runs on both optical fiber cable and unshielded twisted pair cable. Gigabit Ethernet runs on either 1000BASE-T twisted pair cable, 1000BASE-X optical fiber or 1000BASE-CX shielded balanced copper cable.
- Fast Ethernet is economical but provides the slow transfer speed as compared to the Gigabit Ethernet that provides the faster transfer rate but is very expensive. The ports of Gigabit Ethernet cost four times the price per port of Fast Ethernet.
- IEEE Standard for Gigabit Ethernet is IEEE 802.3-2008 and the IEEE Standards for Fast Ethernet are 802.3u-1995, 802.3u-1995 and 802.3u-1995.
- Upgrade from simple Ethernet to Fast Ethernet is relatively simple and economical as compared to the upgrade from Fast Ethernet to Gigabit Ethernet.
- Gigabit Ethernet requires specifically designed network devices that can support the standard 1000Mbps data rate. Fast Ethernet requires no specific network devices.
- Manual configuration is the must-have element in the setup of Gigabit Ethernet where most of the devices required prior configuration in order to be compatible with Gigabit Ethernet. While in Fast Ethernet there is no scene of configuration as connected devices automatically configured according to the requirement of Fast Ethernet.
- If you need the more bandwidth then Gigabit Ethernet will provide you the more bandwidth at the best possible frequency as compared to the Fast Ethernet.

IEEE Standards 802 series & their variant

802.2 Logical Link Control

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).

Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.

The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

802.3 Ethernet

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet. Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes. The most common topology for Ethernet is the star topology.

802.5 Token Ring

Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber. Token ring can be run over a star topology as well as the ring topology. There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber. Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.11 Wireless Network Standards

802.11 is the collection of standards setup for wireless networking. You are probably familiar with the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

802.11a was one of the first wireless standards. 802.11a operates in the 5Ghz radio band and can achieve a maximum of 54Mbps. Wasn't as popular as the 802.11b standard due to higher prices and lower range.

802.11b operates in the 2.4Ghz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular. 802.11g is a standard in the 2.4Ghz

band operating at 54Mbps. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band.

Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance. It has a "listen before talk" method of minimizing collisions on the wireless network. This results in less need for retransmitting data.

FDDI

The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper. It should be noted that relatively recently, a related copper specification, called Copper Distributed Data Interface (CDDI), has emerged to provide 100-Mbps service over copper. CDDI is the implementation of FDDI protocols over twisted-pair copper wire. This article focuses mainly on FDDI specifications and operations, but it also provides a high-level overview of CDDI.

FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. As will be discussed in detail later in this article, the primary purpose of the dual rings is to provide superior reliability and robustness.

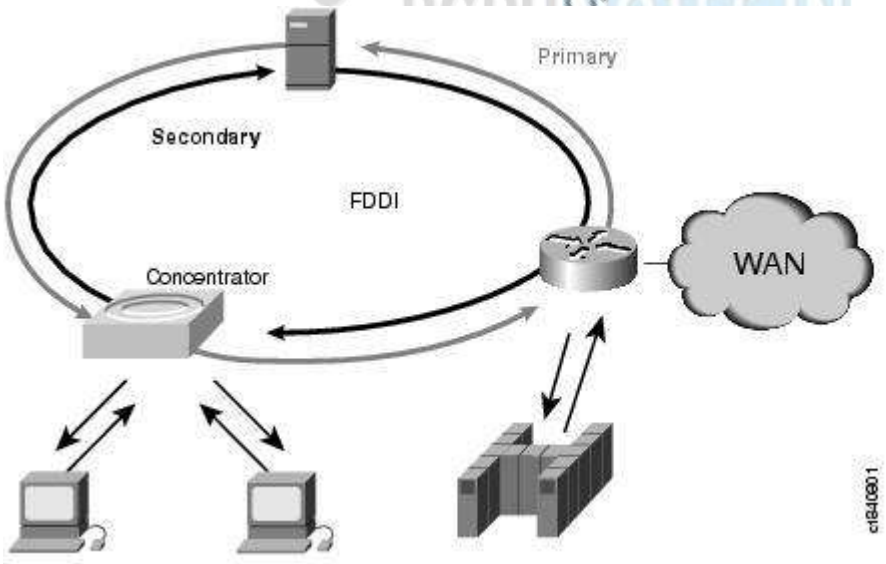


Fig 2.41 FDDI

FDDI Transmission Media

FDDI uses optical fiber as the primary transmission medium, but it also can run over copper cabling. As mentioned earlier, FDDI over copper is referred to as Copper-Distributed Data Interface (CDDI). Optical fiber has several advantages over copper media. In particular, security, reliability, and performance all are enhanced with optical fiber media because fiber does not emit electrical signals. A physical medium that does emit electrical signals (copper) can be tapped and therefore would permit unauthorized access to the data that is transiting the medium. In addition, fiber is immune to electrical interference from radio

frequency interference (RFI) and electromagnetic interference (EMI). Fiber historically has supported much higher bandwidth (throughput potential) than copper, although recent technological advances have made copper capable of transmitting at 100 Mbps. Finally, FDDI allows 2 km between stations using multimode fiber, and even longer distances using a single mode. FDDI defines two types of optical fiber: single-mode and multimode. A mode is a ray of light that enters the fiber at a particular angle. Multimode fiber uses LED as the light-generating device, while single-mode fiber generally uses lasers.

Multimode fiber allows multiple modes of light to propagate through the fiber. Because these modes of light enter the fiber at different angles, they will arrive at the end of the fiber at different times. This characteristic is known as modal dispersion. Modal dispersion limits the bandwidth and distances that can be accomplished using multimode fibers. For this reason, multimode fiber is generally used for connectivity within a building or a relatively geographically contained environment.

Single-mode fiber allows only one mode of light to propagate through the fiber. Because only a single mode of light is used, modal dispersion is not present with single-mode fiber. Therefore, single-mode fiber is capable of delivering considerably higher performance connectivity over much larger distances, which is why it generally is used for connectivity between buildings and within environments that are more geographically dispersed.

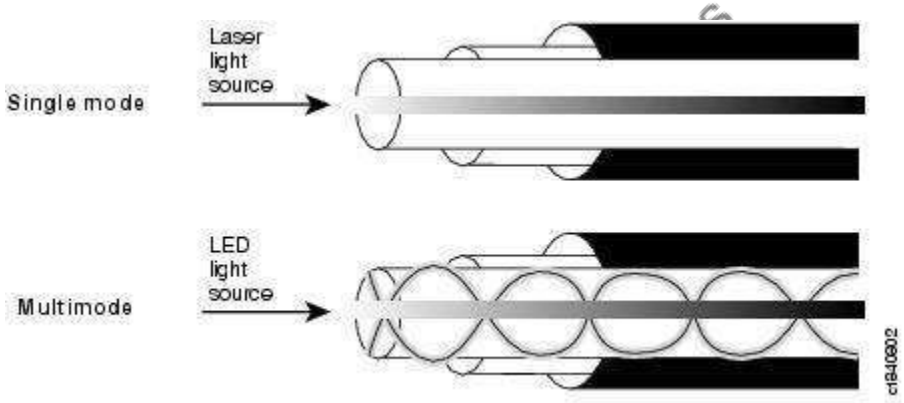


Fig 2.42 FDDI transmission medium

Performance Measuring Metrics

- **Latency:** It can take a long time for a packet to be delivered across intervening networks. In reliable protocols where a receiver acknowledges delivery of each chunk of data, it is possible to measure this as round-trip time.
- **Packet loss:** In some cases, intermediate devices in a network will lose packets. This may be due to errors, to overloading of the intermediate network, or to intentional discarding of traffic in order to enforce a particular service level.
- **Retransmission**: When packets are lost in a reliable network, they are retransmitted. This incurs two delays: First, the delay from re-sending the data; and second, the delay resulting from waiting until the data is received in the correct order before forwarding it up the protocol stack.
- **Throughput:** The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second. Throughput is analogous to the number of lanes on a highway, whereas latency is

analogous to its speed limit.

UNIT IV

Transport Layer

Transport layer services are conveyed to an application via a programming interface to the transport layer protocols. The services may include the following features:

- **Connection-oriented communication:** It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection-less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).
- **Same order delivery:** The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done using segment numbering, with the receiver passing them to the application in order. This can cause head-of-line blocking.
- **Reliability:** Packets may be lost during transport due to network congestion and errors. By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender. Automatic repeat request schemes may be used to retransmit lost or corrupted data.
- **Flow control:** The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun. This can also be used to improve efficiency by reducing buffer underrun.
- **Congestion avoidance:** Congestion control can control traffic entry into a telecommunications network, to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start. This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.
- **Multiplexing:** Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

TCP

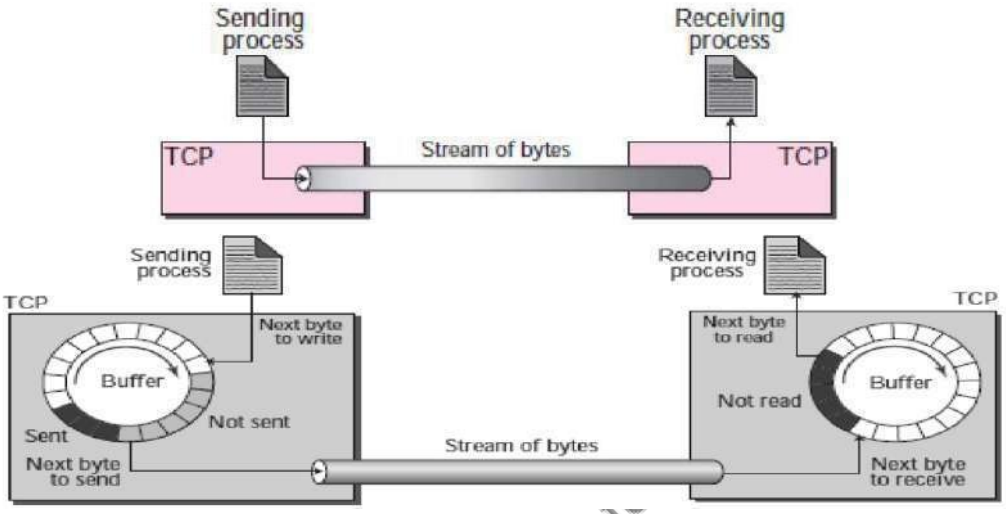
TCP lies between the application layer and the network layer and serves as the intermediary between the application programs and the network operations. Services offered by TCP to the processes at the application layer.

Well-known Ports used by TCP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day

Stream Delivery Service: - It allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their bytes across the Internet.

Sending and Receiving Buffers: - The sending and the receiving processes may not necessarily write or read data at the same rate, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction.



Segments

Although buffering handles the disparity between the speed of the producing and consuming processes, we need one more step before we can send data. The IP layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment. TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission.

Full-Duplex Communication

TCP offers full-duplex service, where data can flow in both directions at the same time. Each TCP endpoint then has its own sending and receiving buffer, and segments move in both directions.

Multiplexing and Demultiplexing

Like UDP, TCP performs multiplexing at the sender and demultiplexing at the receiver. However, since TCP is a connection-oriented protocol, a connection needs to be established for each pair of processes.

Connection-Oriented Service

TCP, unlike UDP, is a connection-oriented protocol. when a process at site A wants to send to and receive data from another process at site B, the following three phases occur:

1. The two TCPs establish a virtual connection between them.
2. Data are exchanged in both directions.
3. The connection is terminated.

Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent. Each may be routed over a

different path to reach the destination. There is no physical connection. TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site.

Reliable Service

TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data.

TCP FEATURES

Numbering System

Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header. Instead, there are two fields called the sequence number and the acknowledgment number. These two fields refer to a byte number and not a segment number.

Byte Number

TCP numbers all data bytes (octets) that are transmitted in a connection. Numbering is independent in each direction. When TCP receives bytes of data from a process, TCP stores them in the sending buffer and numbers them. The numbering does not necessarily start from 0. Instead, TCP chooses an arbitrary number between 0 and 232 − 1 for the number of the first byte.

Sequence Number

After the bytes have been numbered, TCP assigns a sequence number to each segment that is being sent.

Acknowledgment Number

As we discussed previously, communication in TCP is full duplex; when a connection is established, both parties can send and receive data at the same time. Each party numbers the bytes, usually with a different starting byte number.

Flow Control

TCP, unlike UDP, provides flow control. The sending TCP controls how much data can be accepted from the sending process, the receiving TCP controls how much data can to be sent by the sending TCP.

Error Control

To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented, as we will see later.

Congestion Control

TCP, unlike UDP, considers congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control) but is also determined by the level of congestion, if any, in the network.

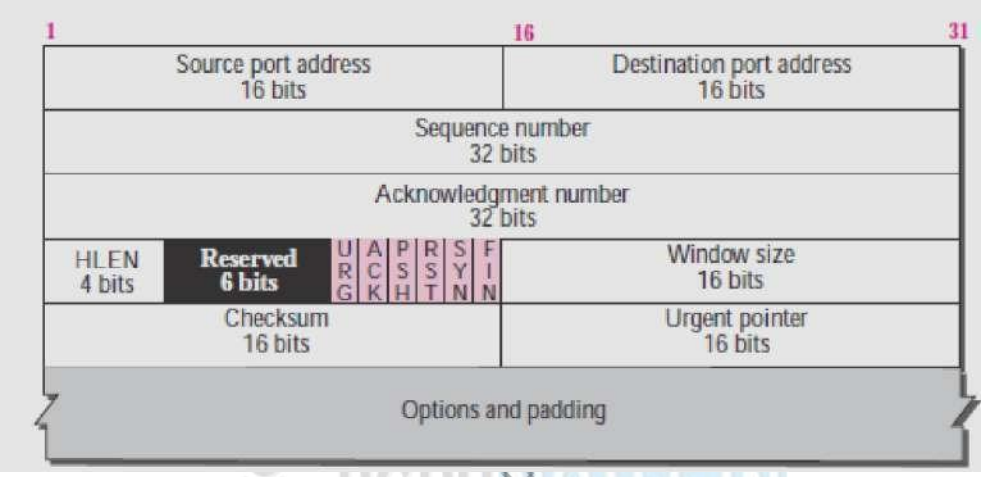
Addressing

TCP communication between two remote hosts is done by means of port numbers (T SAPs). Ports numbers can range from 0 – 65535 which are divided as:

System Ports (0 – 1023)
User Ports (1024 – 49151)
Private/Dynamic Ports (49152 – 65535)

SEGMENT

A packet in TCP is called a segment. The segment consists of a header of 20 to 60 bytes, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options. We will discuss some of the header fields in this section.



Source port address: This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.

Destination port address: This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.

Sequence number: This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered.

Acknowledgment number: This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party.

Header length: This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes.

Reserved: This is a 6-bit field reserved for future use.

Control: This field defines 6 different control bits or flags.

URG: Urgent pointer is valid			RST: Reset the connection		
ACK: Acknowledgment is valid			SYN: Synchronize sequence numbers		
PSH: Request for push			FIN: Terminate the connection		
URG	**ACK**	**PSH**	**RST**	**SYN**	**FIN**

6 Bits

Window size: This field defines the window size of the sending TCP in bytes. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes.

Checksum: This 16-bit field contains the checksum. The calculation of the checksum for TCP follows the same procedure as the one described for UDP.

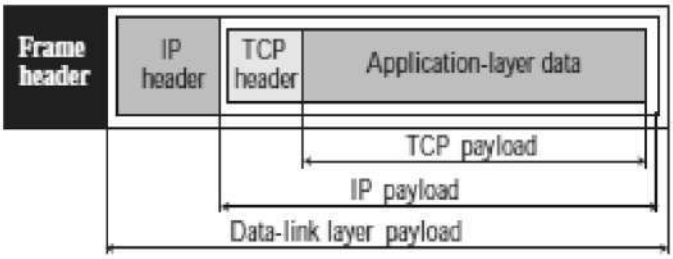
Windows Size: This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.

Checksum: This field contains the checksum of Header, Data and Pseudo Headers.

Urgent Pointer: It points to the urgent data byte if URG flag is set to 1.

Options: It facilitates additional options which are not covered by the regular header. Options field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach the 32-bit boundary.

Encapsulation: A TCP segment encapsulates the data received from the application layer. The TCP segment is encapsulated in an IP datagram, which in turn is encapsulated in a frame at the data-link layer.



Connection Management in TCP

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management. A connection-oriented transport protocol establishes a virtual path between the source and destination. All of the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames.

Connection Establishment

TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

Before the sending device and the receiving device start the exchange of data, both devices need to be synchronized. During the TCP initialization process, the sending device and the receiving device exchange a few control packets for synchronization purposes. This exchange is known as Three-way handshake.

The Three-way handshake begins with the initiator sending a TCP segment with the SYN control bit flag set.

TCP allows one side to establish a connection. The other side may either accept the connection or refuse it. If we consider this from application layer point of view, the side that is establishing the connection is the client and the side waiting for a connection is the server.

TCP identifies two types of OPEN calls:

Active Open: In an Active Open call, a device (client process) using TCP takes the active role and initiates the connection by sending a TCP SYN message to start the connection.

Passive Open: A passive OPEN can specify that the device (server process) is waiting for an active OPEN from a specific client. It does not generate any TCP message segment. The server processes listening for the clients are in Passive Open mode.

Three-way Handshaking:

Step 1. Device A (Client) sends a TCP segment with SYN = 1, ACK = 0, ISN (Initial Sequence Number) = 2000.

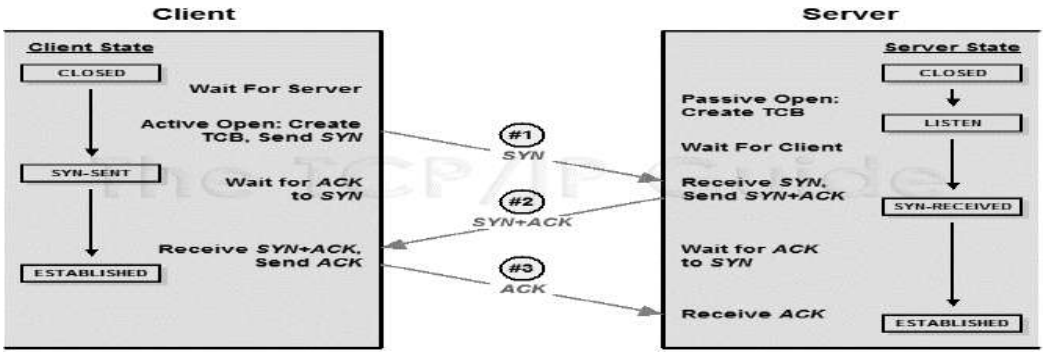
An Initial Sequence Number (ISN) is a random Sequence Number, allocated for the first packet in a new TCP connection.

The Active Open device (Device A) sends a segment with the SYN flag set to 1, ACK flag set to 0 and an Initial Sequence Number 2000 (For Example), which marks the beginning of the sequence numbers for data that device A will transmit. SYN is short for SYNchronize. SYN flag announces an attempt to open a connection.

Step 2. Device B (Server) receives Device A's TCP segment and returns a TCP segment with SYN = 1, ACK = 1, ISN = 5000 (Device B's Initial Sequence Number), Acknowledgment Number = 2001 (2000 + 1, the next sequence number Device B expecting from Device A).

Step 3. Device A sends a TCP segment to Device B that acknowledges receipt of Device B's ISN, with flags set as SYN = 0, ACK = 1, Sequence number = 2001, Acknowledgment number = 5001 (5000 + 1, the next sequence number Device A expecting from Device B)

This handshaking technique is referred to as TCP Three-way handshake or SYN, SYN-ACK, ACK.

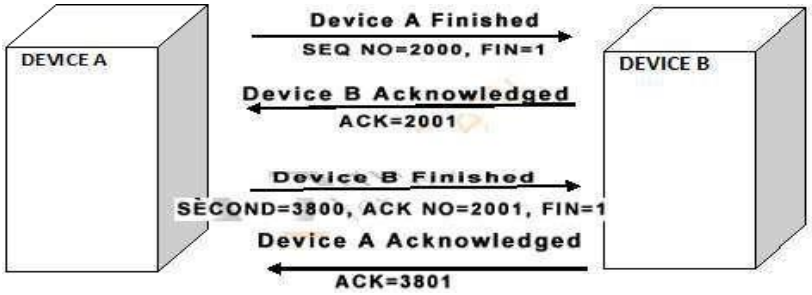


SYN Flooding Attack

The connection establishment procedure in TCP is susceptible to a serious security problem called SYN flooding attack. This happens when one or more malicious attackers send a large number of SYN segments to a server pretending that each of them is coming from a different client by faking the source IP addresses in the datagrams.

Transmission Control Protocol (TCP) Connection Termination

When the data transmission is complete and the device wants to terminate the connection, the device initiating the termination places a TCP segment (Segment is the name of the data packet at the transport layer, if the protocol is TCP) with the FIN flag set to one. The purpose of FIN bit is to enable TCP to gracefully terminate an established session. The application then enters in a state called the FIN-WAIT state. When at FIN-WAIT state, Device A continues to receive TCP segments from Device B and processes the segments already in the queue, but no additional data is accepted from the application.



Comparison between TCP & UDP

Characteristic / Description	UDP	TCP
General Description	Simple, high-speed, low-functionality "wrapper" that interfaces applications to the network layer and does little else.	A full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol Connection Setup	Connectionless; data is sent without setup.	Connection-oriented; connection must be established prior to transmission.
Data Interface To Application	Message-based; data is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure.
Reliability and Acknowledgments	Unreliable, best-effort delivery without acknowledgments.	Reliable delivery of messages; all data is acknowledged.
Retransmissions	Not performed. The application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage Flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms.
Overhead	Very low	Low, but higher than UDP
Transmission Speed	Very high	High, but not as high as UDP
Data Quantity	Small to moderate amounts of data (up to	Small to very large amounts of data (up

Suitability	a few hundred bytes)	to gigabytes)
Types of Applications That Use the Protocol	Applications where data delivery speed matters more than completeness, where small amounts of data are sent; or where multicast/broadcast are used.	Most protocols and applications sending data that must be received reliably, including most file and message transfer protocols.
Well-Known Applications and Protocols	Multimedia applications, DNS, BOOTP, DHCP, TFTP, SNMP, RIP, NFS (early versions)	FTP, Telnet, SMTP, DNS, HTTP, POP, NNTP, IMAP, BGP, IRC, NFS (later versions)

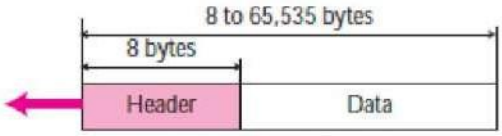
UDP

Requirement of UDP

A question may arise; why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgment packets share a significant amount of bandwidth along with the actual data. For example, in the case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain a huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features

- UDP is used when acknowledgment of data does not hold any significance.
- UDP is a good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is a suitable protocol for streaming applications such as VoIP, multimedia streaming.



a. UDP user datagram

b. Header format

Source port number. This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

Destination port number. This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.

Length. This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. How- ever, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes. The length field in a UDP user datagram is not necessary. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length.

UDP length = IP length – IP header's length

Checksum. This field is used to detect errors over the entire user datagram (header plus data). The checksum is discussed in the next section.

UDP SERVICES

Process-to-Process Communication

UDP provides process-to-process communication using sock- etc, a combination of IP addresses and port numbers. Several port numbers used by UDP.

Connectionless Services

As mentioned previously, UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program.

Flow Control

UDP is a very simple protocol. There is no flow control, and hence no window mechanism. The receiver may overflow with incoming messages. The lack of flow control means that the process using UDP should provide for this service if needed.

Error Control

There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded.

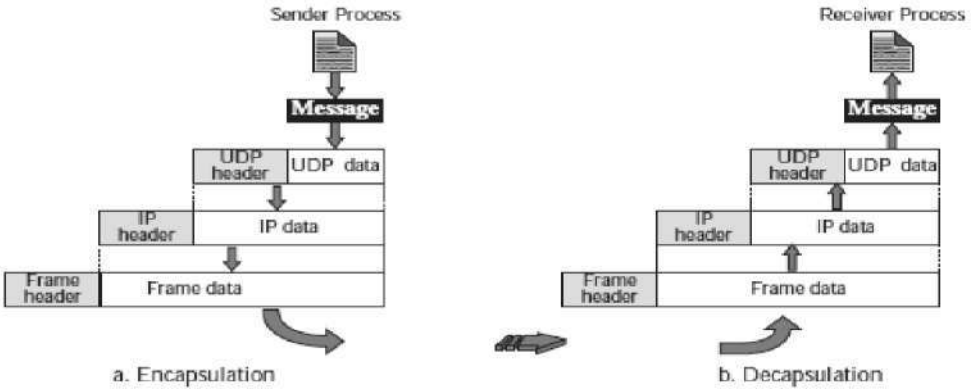
Checksum

UDP checksum calculation is different from the one for IP. Here the checksum includes three sections: a pseudo header, the UDP header, and the data coming from the application layer.

Congestion Control

Since UDP is a connectionless protocol, it does not provide congestion control. UDP assumes that the packets sent are small and sporadic, and cannot create congestion in the network. This assumption may or may not be true today when UDP is used for real-time transfer of audio and video.

Encapsulation and decapsulation



Encapsulation

When a process has a message to send through UDP, it passes the message to UDP along with a pair of socket addresses and the length of data. UDP receives the data and adds the UDP header. UDP then passes the user datagram to IP with the socket addresses. IP adds its own header, using the value 17 in the protocol field, indicating that the data has come from the UDP protocol.

Decapsulation

When the message arrives at the destination host, the physical layer decodes the signals into bits and passes it to the data link layer. The data link layer uses the header (and the trailer) to check the data. If there is no error, the header and trailer are dropped and the datagram is passed to IP. The IP software does its own checking. If there is no error, the header is dropped and the user datagram is passed to UDP with the sender and receiver IP addresses.

Integrated Services & Differentiated Services

INTEGRATED SERVICES

Two models have been designed to provide quality of service on the Internet:

- Integrated Services
- Differentiated Services

Both models emphasize the use of quality of service at the network layer (IP), although the model can also be used in other layers such as the data link layer. As we learned in Chapter 20, IP was originally designed for best-effort delivery. This means that every user receives the same level of services. This type of delivery does not guarantee the minimum of a service, such as bandwidth, to applications such as real-time audio and video. If such an application accidentally gets extra bandwidth, it may be detrimental to other applications, resulting in congestion. Integrated Services, sometimes called Int-Serv, is a flow-based QoS model, which means that a user needs to create a flow, a kind of virtual circuit, from the source to the destination and inform all routers of the resource requirement. Integrated Services is a flow based QoS model designed for IP.

Signaling

The reader may remember that IP is a connectionless, datagram, packet-switching protocol. How can we implement a flow-based model over a connectionless protocol? The solution is a signaling protocol to run over IP that provides the signaling mechanism for making a reservation. This protocol is called Resource Reservation Protocol (RSVP) and will be discussed shortly.

Flow Specification

When a source makes a reservation, it needs to define a flow specification. A flow specification has two parts:

- Rspec (resource specification)
- Tspec (traffic specification)

Rspec defines the resource that the flow needs to reserve (buffer, bandwidth, etc.). Tspec defines the traffic characterization of the flow.

Admission

After a router receives the flow specification from an application, it decides to admit or deny the service. The decision is based on the previous commitments of the router and the current availability of the resource.

Service Classes

Two classes of services have been defined for Integrated Services:

- Guaranteed service
- Controlled-load service

Guaranteed Service Class

This type of service is designed for real-time traffic that needs a guaranteed minimum end-to-end delay. The end-to-end delay is the sum of the delays in the routers, the propagation delay in the media, and the setup mechanism. Only the first, the sum of the delays in the routers, can be guaranteed by the router. This type of service guarantees that the packets will arrive within a certain delivery time and are not discarded if flow traffic stays within the boundary of Tspec. We can say that guaranteed services are quantitative services, in which the amount of end-to-end delay and the data rate must be defined by the application.

Controlled-Load Service Class

This type of service is designed for applications that can accept some delays but are sensitive to an overloaded network and to the danger of losing packets. Good examples of these types of applications are file transfer, e-mail, and Internet access. The controlled load service is a qualitative type of service in that the application requests the possibility of low-loss or no-loss packets.

RSVP (Resource reservation protocol)

In the Integrated Services model, an application program needs resource reservation. As we learned in the discussion of the Int-Serv model, the resource reservation is for a flow. This means that if we want to use Int-Serv at the IP level, we need to create a flow, a kind of virtual-circuit network, out of the IP, which was originally designed as a datagram packet-switched network. A virtual-circuit network needs a signaling system to set up the virtual circuit before data traffic can start. The Resource Reservation Protocol (RSVP) is a signaling protocol to help IP create a flow and consequently make a resource reservation. Before discussing RSVP, we need to mention that it is an independent protocol separate from the Integrated Services model. It may be used in other models in the future.

Multicast Trees

RSVP is different from some other signaling systems we have seen before in that it is a signaling system designed for multicasting. However, RSVP can be also used for unicasting because unicasting is just a special case of multicasting with only one member of the multicast group. The reason for this design is to enable RSVP to provide resource reservations for all kinds of traffic including multimedia which often uses multicasting.

Receiver-Based Reservation

In RSVP, the receivers, not the sender, make the reservation. This strategy matches the other multicasting protocols. For example, in multicast routing protocols, the receivers, not the sender, make a decision to join or leave a multicast group.

RSVP Messages

RSVP has several types of messages. However, for our purposes, we discuss only two of them:

- Path
- Resv

Path Messages Recall that the receivers in a flow make the reservation in RSVP. However, the receivers do not know the path traveled by packets before the reservation is made. The path is needed for the reservation. To solve the problem, RSVP uses Path messages. A Path message travels from the sender and reaches all receivers in the multicast path. On the way, a Path message stores the necessary information for the receivers. A Path message is sent in a multicast environment; a new message is created when the path diverges.

Resv Messages After a receiver has received a Path message, it sends a Resv message. The Resv message travels toward the sender (upstream) and makes a resource reservation on the routers that support RSVP. If a router does not support RSVP on the path, it routes the packet based on the best-effort delivery methods we discussed before.

Reservation Merging

In RSVP, the resources are not reserved for each receiver in a flow; the reservation is merged. Rc3 requests a 2-Mbps bandwidth while Rc2 requests an I-Mbps bandwidth. Router R3, which needs to make a bandwidth reservation, merges the two requests. The reservation is made for 2 Mbps, the larger of the two, because a 2-Mbps input reservation can handle both requests. The same situation is true for R2. The reader may ask why Rc2 and Rc3, both belonging to one single flow, request different amounts of bandwidth. The answer is that, in a multimedia environment, different receivers may handle different grades of quality. For example, Rc2 may be able' to receive video only at 1 Mbps (lower quality), while Rc3 may be able to receive video at 2 Mbps (higher quality).

Reservation Styles

When there is more than one flow, the router needs to make a reservation to accommodate all of them. RSVP defines three types of reservation styles.

Wild Card Filter Style In this style, the router creates a single reservation for all senders. The reservation is based on the largest request. This type of style is used when the flows from different senders do not occur at the same time. Fixed Filter Style In this style, the router creates a distinct reservation for each flow. This means that if there are n flows, n different reservations are made. This type of style is used when there is a high probability that flows from different senders will occur at the same time.

Shared Explicit Style In this style, the router creates a single reservation which can be shared by a set of flows.

Soft State

The reservation information (state) stored in every node for a flow needs to be refreshed periodically. This is referred to as a soft state as compared to the hard state used in other virtual circuit protocols such as ATM or Frame Relay, where the information about the flow is maintained until it is erased. The default interval for refreshing is currently 30 s.

Problems with Integrated Services

There are at least two problems with Integrated Services that may prevent its full implementation on the Internet:

- Scalability
- Service-type limitation

Scalability

The Integrated Services model requires that each router keeps information for each flow. As the Internet is growing every day, this is a serious problem.

Service-Type Limitation

The Integrated Services model provides only two types of services, guaranteed and control the load. Those opposing this model argue that applications may need more than these two types of services.

DIFFERENTIATED SERVICES

Differentiated Services (DS or Diffserv) was introduced by the IETF (Internet Engineering Task Force) to handle the shortcomings of Integrated Services. Two fundamental changes were made:

- The main processing was moved from the core of the network to the edge of the network. This solves the scalability problem. The routers do not have to store
- Information about flows. The applications, or hosts, define the type of service they need each time they send a packet.
- The per-flow service is changed to per-class service. The router routes the packet based on the class of service defined in the packet, not the flow. This solves the service-type limitation problem. We can define different types of classes based on the needs of applications.

INTERNETWORKING DEVICE

An internetworking device is a widely-used term for any hardware within networks that connect different network resources. Key devices that comprise a network are

- Routers
- Bridges
- Repeaters
- Gateways

Routers

Routers are highly intelligent network devices that are primarily used for large networks and provide the best data path for effective communication. Routers have memory chips which store large quantities of network addresses.

A router is a device that analyzes the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

Bridges

Bridges are used to connect two large networks by providing different network services.

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

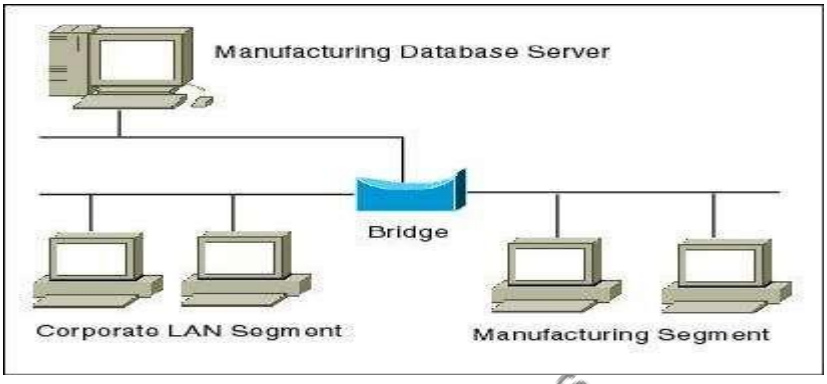
Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two

different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.

Bridges are also known as Layer 2 switches.

A bridge uses a database to ascertain where to pass, transmit or discard the data frame.

1. If the frame received by the bridge is meant for a segment that resides on the same host network, it will pass the frame to that node and the receiving bridge will then discard it.
2. If the bridge receives a frame whose node MAC address is of the connected network, it will forward the frame toward it.



Repeaters

Repeaters are used for signal and data regeneration and are primarily responsible for data amplification. The term "repeater" originated with telegraphy in the 19th century and referred to an electromechanical device used to regenerate telegraph signals. Use of the term has continued in telephony and data communications.

In telecommunication, the term repeater has the following standardized meanings:

1. An analog device that amplifies an input signal regardless of its nature (analog or digital).
2. A digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission. A repeater that includes the retiming function is also known as a regenerator.

In computer networking, because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the physical layer, the first layer of the OSI model.

Gateways

Gateways are internetworking devices used to convert formats and are the backbone of any network architecture. The term gateway has the following meaning:

- Gateway is a router or a proxy server that routes between networks
- Gateway Rule - Gateway should belong to the same subnet to which your
- PC belongs
- In a communications network, a network node equipped for interfacing with another network that uses different protocols.
- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.

- A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.
- Loosely, a computer or computer program configured to perform the tasks of a gateway. For a specific case, see default gateway.
- Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol.

Switch

A switch, in the context of networking, is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such, it can support all types of packet protocols.

Essentially, switches are the traffic cops of a simple local area network.

A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass through one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination.

Switches are similar to hubs, only smarter. A hub simply connects all the nodes on the network communication is essentially in a haphazard manner with any device trying to communicate at any time, resulting in many collisions. A switch, on the other hand, creates an electronic tunnel between the source and destination ports for a split second that no other traffic can enter. This results in communication without collisions.

Switches are similar to routers as well, but a router has the additional ability to forward packets between different networks, whereas a switch is limited to node-to-node communication on the same network.

Hub

A hub is the connection point in a computer device where data from many directions converge and are then sent out in many directions to respective devices. A hub may also act as a switch by preventing specific data packets from proceeding to a destination.

In addition to receiving and transmitting communication data, a hub may also serve as a switch. For example, an airport acts much like a hub in the sense that passengers converge there and head out in many different directions. Suppose that an airline passenger arrives at the airport hub and is then called back home unexpectedly, or receives instructions to change his or her destination. The same may occur with a computing hub when it acts as a switch by preventing specific data packets from proceeding to a destination while sending other data packets on a specific route. Where packets are sent depends on attributes (MAC addresses) within the data packets. A switch may also act as a hub.

Layered Communication

Network communication models are generally organized into layers. The OSI model specifically consists of seven layers, with each layer representing a specific networking function. These functions are controlled by protocols, which govern end-to-end communication between devices. As data is passed from the user application down the virtual layers of the OSI model, each of the lower layers adds a header (and sometimes a trailer) containing protocol information specific to that layer. These headers are called Protocol Data Units (PDUs), and the process of adding these headers is referred to as encapsulation.

The PDU of each lower layer is identified with a unique term:

Commonly, network devices are identified by the OSI layer they operate at (or, more specifically, what header or PDU the device processes). For example, switches are generally identified as Layer-2 devices, as switches process information stored in the Data-Link header of a frame (such as MAC addresses in Ethernet). Similarly, routers are identified as Layer-3 devices, as routers process logical addressing information in the Network header of a packet (such as IP addresses).